TUCS

Sanaz Rahimi Moosavi

Towards End-to-End Security in Internet of Things based Healthcare

Turku Centre *for* Computer Science

TUCS Dissertations
No 247, December 2019

Towards End-to-End Security in Internet of Things based Healthcare

Sanaz Rahimi Moosavi

To be presented, with the permission of the Faculty of Science and Engineering of the University of Turku, for public criticism in lecture hall X of Natura on Dec 5th, 2019, at 12 noon.

University of Turku
Department of Future Technologies
20014 TURUN YLIOPISTO, FINLAND

2019

Supervisors

Associate Professor Seppo Virtanen
Department of Future Technologies, University of Turku
Finland

Adjunct Professor Ethiopia Nigussie
Department of Future Technologies, University of Turku
Finland

Professor Jouni Isoaho
Department of Future Technologies, University of Turku
Finland

Reviewers

Professor Jari Nurmi
Department of Information Technology and Communication Sciences
Tampere University
Finland

Professor Gert Jervan
Department of Computer Systems
Tallinn University of Technology
Estonia

Opponent

Professor Ian G. Harris
Department of Computer Science
University of California, Irvine
USA

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin Originality Check service.

Painosalama Oy, Turku, Finland
ISBN 978-952-12-3883-3
ISSN 1239-1883

To my wonderful husband, Amir

Abstract

Healthcare IoT systems are distinguished in that they are designed to serve human beings, which primarily raises the requirements of security, privacy, and reliability. Such systems have to provide real-time notifications and responses concerning the status of patients. Physicians, patients, and other caregivers demand a reliable system in which the results are accurate and timely, and the service is reliable and secure. To guarantee these requirements, the smart components in the system require a secure and efficient end-to-end communication method between the end-points (e.g., patients, caregivers, and medical sensors) of a healthcare IoT system.

The main challenge faced by the existing security solutions is a lack of secure end-to-end communication. This thesis addresses this challenge by presenting a novel end-to-end security solution enabling end-points to securely and efficiently communicate with each other. The proposed solution meets the security requirements of a wide range of healthcare IoT systems while minimizing the overall hardware overhead of end-to-end communication. End-to-end communication is enabled by the holistic integration of the following contributions.

The first contribution is the implementation of two architectures for remote monitoring of bio-signals. The first architecture is based on a low power IEEE 802.15.4 protocol known as ZigBee. It consists of a set of sensor nodes to read data from various medical sensors, process the data, and send them wirelessly over ZigBee to a server node. The second architecture implements on an IP-based wireless sensor network, using IEEE 802.11 Wireless Local Area Network (WLAN). The system consists of a IEEE 802.11 based sensor module to access bio-signals from patients and send them over to a remote server. In both architectures, the server node collects the health data from several client nodes and updates a remote database. The remote webserver accesses the database and updates the webpage in real-time, which can be accessed remotely.

The second contribution is a novel secure mutual authentication scheme for Radio Frequency Identification (RFID) implant systems. The proposed scheme relies on the elliptic curve cryptography and the D-Quark lightweight hash design. The scheme consists of three main phases: (1) reader authentication and verification, (2) tag identification, and (3) tag verification. We show that among the existing public-key crypto-systems, elliptic curve is the optimal choice due to its small key size as well as its efficiency in computations. The D-Quark lightweight hash design has been tailored for resource-constrained devices.

The third contribution is proposing a low-latency and secure cryptographic keys generation approach based on Electrocardiogram (ECG) features. This is performed by taking advantage of the uniqueness and randomness properties of ECG's main features comprising of PR, RR, PP, QT, and ST intervals. This approach achieves low latency due to its reliance on reference-free ECG's main features that can be acquired in a short time. The approach is called Several ECG Features (SEF)-based cryptographic key generation.

The fourth contribution is devising a novel secure and efficient end-to-end security scheme for mobility enabled healthcare IoT. The proposed scheme consists of: (1) a secure and efficient end-user authentication and authorization architecture based on the certificate based Datagram Transport Layer Security (DTLS) handshake protocol, (2) a secure end-to-end communication method based on DTLS session resumption, and (3) support for robust mobility based on interconnected smart gateways in the fog layer.

Finally, the fifth and the last contribution is the analysis of the performance of the state-of-the-art end-to-end security solutions in healthcare IoT systems including our end-to-end security solution. In this regard, we first identify and present the essential requirements of robust security solutions for healthcare IoT systems. We then analyze the performance of the state-of-the-art end-to-end security solutions (including our scheme) by developing a prototype healthcare IoT system.

Tiivistelmä

Terveydenhuollon järjestelmät eroavat muista Esineiden Internet (Internet of Things, IoT) -järjestelmistä käyttökohteensa ja tietoturvavaatimustensa osalta. Kun järjestelmä on tarkoitettu ihmisten hoitamiseen ja ihmislähtöisen terveystiedon keräämiseen, analysointiin ja seurantaan, ovat järjestelmien luotettavuus, tietoturva ja yksityisyyden suoja keskeisiä vaatimuksia. Terveydenhuollon järjestelmät havainnoivat potilaan tilaa reaaliaikaisesti ja tarvittaessa antavat hälytyksen hoitohekilökunnalle. Lääkärit, potilaat ja hoitajat tarvitsevat järjestelmiä, jotka ovat luotettavia, tarkkoja, ja turvallisia käyttää. Jotta nämä vaatimukset voidaan täyttää, järjestelmät tarvitsevat luotettavan, päästä päähän salatun viestintäkanavan järjestelmän eri päätelaitteiden välille.

Nykyisten IoT-järjestelmien tietoturvaratkaisujen keskeinen haaste on päästä päähän salattujen yhteyksien puuttuminen. Tässä väitöskirjassa esitetään tähän ratkaisuna järjestelmä, joka mahdollistaa päätelaitteiden välisen tehokkaan viestinnän päästä päähän salatun yhteyden yli. Tämä järjestelmä vastaa terveydenhuollon IoT-laitteiden tietoturvavaatimuksiin samalla minimoiden laitteistotason resurssikulutuksen. Esitetty järjestelmä koostuu seuraaviin tieteellisissä julkaisuissa esitettyihin tutkimustuloksiin.

Ensimmäinen väitöskirjassa esitetty tutkimustulos on kahden eri arkkitehtuurin laitteistototeutus biosignaalien etätarkkailuun. Ensimmäinen toteutus perustuu matalavirrankulutuksiseen IEEE 802.15.4 Zigbee-protokollaan, jota käyttävät sensorit lukevat signaaleita erilaisista antureista, prosessoivat signaalit ja lähettävät ne palvelimelle. Toinen arkkitehtuuritoteutus käyttää IP-pohjaista langatonta sensoriverkkoa hyödyntäen langattoman lähiverkon IEEE 802.11 -standardia. Järjestelmä koostuu sensorimoduulista, joka lukee potilaasta tarvittavat biosignaalit ja lähettää ne etäpalvelimelle. Molemmissa arkkitehtuureissa palvelin kerää useiden potilaiden terveystietoja yhtä aikaa ja päivittää kerätyt tiedot tietokantaan. Terveystietoja voidaan tarkastella web-palvelimen, joka lukee tiedot reaaliajassa tietokannasta, avulla.

Toisena tuloksena esitetään uusi yhteisautentikointimenetelmä RFID-implanteille. Järjestelmän turvallisuus perustuu elliptisten käyrien kryptografiaan ja laskennallisesti kevyeen D-Quark -hajautusfunktioon.

Järjestelmän toiminta on kolmivaiheinen: (1) lukijan autentikointi ja verifiointi, (2) RFID-tagin tunnistus, ja (3) tagin verifiointi. Tutkimustuloksena esitetään, että elliptisiin käyriin perustuvat kryptojärjestelmät ovat muihin vastaaviin verrattuna optimaalinen valinta johtuen pienestä avaimen koosta ja laskennan tehokkuudesta. D-Quark -hajautusfunktio on vastaavasti räätälöity laskennallisesti rajoittuneille laitteille.

Kolmantena tuloksena esitetään elektrokardiogrammiin (EKG) perustuva nopea ja turvallinen kryptografisten avaimien generointimenetelmä. Tässä hyödynnetään EKG:a satunnaisuuden lähteenä sekä EKG:n PR-, RR-, RR-, PP-, QT- ja ST-välien yksilöllisyyttä. Koska nämä piirteet ovat nopeasti eroteltavissa EKG-signaalista, esitelty useisiin EKG-piirteisiin perustuva (Several ECG Features, SEF) kryptografisten avainten generointimenetelmä on nopea.

Neljäntenä tuloksena väitöskirjassa esitetään uusi turvallinen päästä päähän salattu ja käyttäjien mobiiliutta tukeva tietoturvakokonaisuusratkaisu IoT-pohjaisille terveydenhuollon diagnostiikka- ja analyysilaitteille. Ratkaisu koostuu (1) turvallisesta ja tehokkaasta loppukäyttäjän tunnistamisesta ja käyttöoikeuksien hallinta-arkkitehtuurista, joka hyödyntää Datagram Transport Layer Security (DTLS) -protokollan sertifikaatteja ja kättelyä, (2) turvallisesta DTLS-istunnon jatkamiseen perustuvasta päästä päähän salatusta viestintäkanavasta, ja (3) usvalaskentakerrokseen sijoittuvista keskenään verkottuneista älykkäistä porttilaitteista, jotka mahdollistavat päätelaitteiden liikkuvuuden.

Viidentenä ja viimeisenä tuloksena väitöskirjassa vertaillaan uusimpien päästä päähän salattujen terveydenhuollon järjestelmien tietoturvaratkaisujen suorituskykyä väitöskirjassa esitettyyn uuteen ratkaisuun. Vertailun aluksi tunnistetaan ja esitellään tämän kaltaisiin järjestelmiin kohdistuvat keskeiset vaatimukset. Tämän jälkeen kehitellään prototyyppi uudesta IoT-terveydenhuoltosovelluksesta, jonka avulla vertailtavien ratkaisujen suorituskykyä voidaan analysoida.

Acknowledgements

This work was carried out at the Department of Future Technologies, University of Turku, during January 2014 and June 2019. This dissertation would not have been possible without the guidance and the help of several individuals who in one way or another contributed and extended their valuable assistance in the accomplishment of this research work.

First and foremost, my utmost gratitude to my supervisors Adjunct Prof. Ethiopia Nigussie, Associate Prof. Seppo Virtanen, and Prof. Jouni Isoaho for their inspiration, guidance, and support. I attribute the level of my Ph.D. degree to their encouragement and effort and without them, this thesis, too, would not have been completed or written.

I also wish to thank Prof. Jari Nurmi from Tampere University and Prof. Gert Jervan from Tallinn University of Technology for their detailed reviews of this dissertation and for providing constructive comments and suggestions for improvement.

I have had an opportunity to do a research visit at the University of California Irvine, USA. I would like to acknowledge Associate Prof. Marco Levorato for his kind help and supervision.

The University of Turku Graduate School (UTUGS) is gratefully acknowledged for funding my doctoral studies. This research work was financially supported by the Finnish Foundation for Technology Promotion (TES), The Kaute Foundation (Tutkijat Maailmalle), the Nokia Foundation, the Ulla Tuominen Foundation, the Elisa (HPY) Telecommunications Foundation, and the Finnish Cultural Foundation. I would also like to express my gratitude to the MATTI doctoral programme for providing grants to support my conference and educational trips. Furthermore, I want to acknowledge the support of the technical and administrative personnel at the Department of Future Technologies, University of Turku and the Department of Computer Science, University of California, Irvine.

I would like to thank all my colleagues at the Communication Systems Lab. at the University of Turku Department of Future Technologies (previously Department of Information Technology): Antti Hakkala, Petri Sainio, Ali Farooq, and Nanda Kumar Thanigaivelan. I am grateful to everyone who has co-authored papers with me especially Anurag, Tuan Nguyen Gia, Amir

M. Rahmani, Tomi Westerlund, Guang Yang, Pasi Liljeberg, and Hannu Tenhunen for the insights they have shared.

I wish to thank my best friend, Parmida, for helping me get through the difficult times, and for all the emotional support, camaraderie, and caring she has provided. She is not just my best friend, she is my best sister.

I would like to express my deepest gratitude to my lovely parents for all the help during different stages of my life and studies. All the unconditional support they have provided me over the years was the greatest gift anyone has ever given me. My brother, Saman, also deserves thanks for his constant encouragement and support.

Last but not least, my warmest and heartfelt thanks go to my wonderful husband, Amir, who has been standing beside me throughout my study and writing this thesis. I am very grateful for his unconditional love and selfless patience when I was frustrated. These few words can not express my deepest appreciation and love for his endless support during these past years. He has been my inspiration and motivation for continuing to improve my knowledge and move my research forward. He is everything to me.

Irvine, June 2019

Sanaz Rahimi Moosavi

List of original publications

The work discussed in this dissertation is based on the original publications listed below:

Publications included in the thesis

1. Publication I
   Anurag, **Sanaz Rahimi Moosavi**, Amir M. Rahmani, Tomi Westerlund, Guang Yang, Pasi Liljeberg, Hannu Tenhunen, "Pervasive Health Monitoring Based on Internet of Things: Two Case Studies," in IEEE International Conference on Wireless Mobile Communication and Healthcare (ICST-2014), pp. 275-278, Greece, 2014.

2. Publication II
   Sanaz Rahimi Moosavi, Ethiopia Nigussie, Seppo Virtanen, Jouni Isoaho, "An Elliptic Curve-based Mutual Authentication Scheme for RFID Implant Systems," in Elsevier International Conference on International Conference on Ambient Systems, Networks and Technologies (ANT-2014), pp. 198-206, Belgium, 2014.

3. Publication III
   Sanaz Rahimi Moosavi, Ethiopia Nigussie, Marco Levorato, Seppo Virtanen, Jouni Isoaho, "Low-latency Approach for Secure ECG Feature Based Cryptographic Key Generation," in IEEE Access, pp. 428-442, 2017.

4. Publication IV
   Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Ethiopia Nigussie, Amir M. Rahmani, Seppo Virtanen, Hannu Tenhunen, Jouni Isoaho, "End-to-End Security Scheme for Mobility Enabled healthcare Internet of Things," in Elsevier Future Generation Computer Systems (FGCS-2016), pp. 108-124, 2016.

5. Publication V
   Sanaz Rahimi Moosavi, Ethiopia Nigussie, Marco Levorato, Seppo

Virtanen, Jouni Isoaho, "Performance Analysis of End-to-End Security Schemes in Healthcare IoT," in Elsevier International Conference on Ambient Systems, Networks and Technologies (ANT-2018), pp. 432-439, Portugal, 2018.

Publications not included in the thesis

This thesis is composed of 5 original publications, which are included in Part II of this dissertation. However, The following articles were also published as a result of collaborations in the field of IoT security during this dissertation.

6. Publication VI
Sanaz Rahimi Moosavi, Antti Hakkala, Johanna Isoaho, Seppo Virtanen, and Jouni Isoaho, "Specification Analysis for Secure RFID Implant Systems," in International Journal of Computer Theory and Engineering (IJCTE-2014), pp. 177-188, 2014.

7. Publication VII
Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Amir-Mohammad Rahmani, Ethiopia Nigussie, Seppo Virtanen, Jouni Isoaho, and Hannu Tenhunen, "SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways," in Proc. of 6th International Conference on Ambient Systems, Networks and Technologies (ANT-2015), pp. 452-459, UK, 2015.

8. Publication VIII
Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Ethiopia Nigussie, Amir-Mohammad Rahmani, Seppo Virtanen, Jouni Isoaho, and Hannu Tenhunen, "Session Resumption-Based End-to-End Security for Healthcare Internet-of-Things," in Proc. of IEEE International Conference on Computer and Information Technology (CIT-2015), pp. 581-588, UK, 2015.

9. Publication IX
Antti Vikström, **Sanaz Rahimi Moosavi**, Hans Moen, Tapio Salakoski, Sanna Salanterä, "Factors Affecting the Availability of Electronic Patient Records for Secondary Purposes – A Case Study," in Proc. of Springer International Conference on Well-Being in the Information Society (WIS-2016), pp. 47-56, Finland, 2016.

10. Publication X
Moreno Ambrosin, Arman Anzanpour, Mauro Conti, Tooska Dargahi, **Sanaz Rahimi Moosavi**, Amir M. Rahmani, Pasi Liljeberg, "On

the Feasibility of Attribute-Based Encryption on Internet of Things Devices", in IEEE Micro, pp. 25-35, 2016.

11. Publication XI
Sanaz Rahimi Moosavi, Ethiopia Nigussie, Seppo Virtanen, Jouni Isoaho, "Cryptographic key generation using ECG signal," in Proc. of 14th IEEE Annual Consumer Communications and Networking Conference (CCNC-2017), pp. 1024-1031, USA, 2017.

12. Publication XII
Antti Vikström, Hans Moen, **Sanaz Rahimi Moosavi**, Tapio Salakoski, Sanna Salanterä, "Secondary use of electronic health records: Availability aspects in two Nordic countries", in Health Information Management Journal (HIMJ-2018), pp. 1-8, 2018.

Abbreviations

6LBR	6LoWPAN Border Router
6LoWPAN	IPv6 over Low-power Wireless Personal Area Network
AES	Advanced Encryption Standard
AFE	Analog Front-End
AP	Access Points
API	Application Programming Interface
BAN	Body Area Network
BLE	Bluetooth Low Energy
BSN	Body Sensor Network
CCM	Cipher Block Chaining Message
CPU	Central Processing Unit
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CVD	Cardiovascular Diseases
DB	Database
DH	Diffie-Hellman
DNA	Deoxyribonucleic Acid
DoS	Denial of Service
DSP	Digital Signal Processing
DTLS	Datagram Transport Layer Security
ECC	Elliptic Curve Cryptography

ECDH	Elliptic Curve Diffie Hellman
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ECG	Electrocardiogram
EEG	Electroencephalography
EMG	Electromyography
EOG	Electrooculography
FFT	Fast Fourier transform
ID	Identity Document
IEEE	Institute of Electrical and Electronics
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IoT	Internet of Things
IP	Internet Protocol
IPI	Interpulse Interval
IPv6	Internet Protocol version 6
KBS	Knowledge Base System
LFSR	Linear Feedback Shift Register
LLNs	Low power and Lossy Networks
MAC	Medium Access Control
MCU	Micro Controller Unit
MITM	Man-In-the-Middle
MPU	Microprocessor Unit
MSN	Medical Sensor Network
MTU	Maximum Transmission Unit
NIST	National Institute of Standards and Technology

OS	Operating System
PDA	Personal Digital Assistant
PHP	Hypertext Preprocessor
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PPG	Photoplethysmogram
PRF	Pseudorandom Function
PRNG	Pseudo-random Number Generator
PSK	Pre-shared key
QoS	Quality of Service
RAM	Random Access Memory
RFID	Radio Frequency Identification
ROM	Read Only Memory
RQ	Research Question
RSA	Rivest–Shamir–Adleman
RSS	Received Signal Strength
SCVP	Server-based Certificate Validation Protocol
SNAP	Sensor Network for Assessment of Patients
SNEP	Secure Network Encryption Protocol
SoC	System-on-chip
SPI	Serial Peripheral Interface
SpO2	Blood Oxygen Saturation
SQL	Structured Query Language
SSL	Secure Sockets Layer
TI	Texas Instruments
TLS	Transport Layer Security

TPM	Trusted Platform Module
UDP	User Datagram Protocol
WIoT	Wearable Internet of Things
WLAN	Wireless Local Area Network
WSN	Wireless Sensor Network

Contents

I Research Summary xxi

1 Introduction 1
1.1 Objectives and Research Questions 4
1.2 Research Contributions 6
1.3 Research Methodology 10
1.4 Thesis Organization 13

2 Background and Related Work 15
2.1 Resource-Constrained Network Environments 15
2.2 IoT: Definition, Applications, and IP Adaptation 17
2.3 IoT in Healthcare Environments 19
2.4 Healthcare IoT Communication Architecture 22
2.4.1 Pervasive Health Monitoring Based on the IoT 22
2.4.2 Healthcare IoT Authentication and Authorization Approaches 23
2.4.3 Cryptographic Keys and Constrained Health IoT Devices 28
2.4.4 End-to-End Communication of Healthcare IoT Systems 30
2.4.5 Healthcare IoT Mobility Management 32

3 Contributions of the Thesis 35
3.1 Pervasive Health Monitoring Based on IoT 37
3.2 Authentication Scheme for RFID Implant Systems 40
3.3 ECG Feature Based Cryptographic Key Generation 42
3.4 End-to-End Security for Healthcare IoT 46
3.5 End-to-End Security Scheme Performance Analysis 51

4 Overview of Original Publications 53
4.1 Overview of Original Publications 53
4.1.1 Publication I: Pervasive Health Monitoring Based on Internet of Things: Two Case Studies 53
4.1.2 Publication II: An Elliptic Curve-based Mutual Authentication Scheme for RFID Implant Systems 54

4.1.3 Publication III: Low-latency Approach for Secure ECG Feature Based Cryptographic Key Generation . 55
4.1.4 Publication IV: End-to-End Security Scheme for Mobility Enabled Healthcare Internet of Things 56
4.1.5 Publication V: Performance Analysis of End-to-End Security Schemes in Healthcare IoT 57

5 Conclusions 59
5.1 Future Work 62

Bibliography 65

II Original Publications 77

Part I

Research Summary

Chapter 1

Introduction

Recent advances in information and communication technologies have given rise to a new technology: the Internet of Things (IoT) [1, 2, 3]. IoT enables people and objects in the physical world, as well as data and virtual environments to interact with each other, hence realizing smart environments such as smart transport systems, smart cities, smart healthcare, and smart energy. The concept of IoT provides a solid framework for interconnecting edge computing devices, sensors, smartphones, and cloud computing platforms for seamless interactions. IoT is on the revolutionary road, remodeling the healthcare sector along the way in terms of social benefits and penetration as well as economics. Enabled by ubiquitous computing and communication, all the healthcare system entities, such as individuals, appliances, and medicine, can be monitored and managed continuously. The IoT's connectivity provides a new way to monitor, store, and utilize health and wellbeing related data (that is, diagnosis, treatment, recovery, medication, finance, and even daily activity) on a 24/7 basis. The rising cost of healthcare and the prevalence of chronic diseases around the world urgently demand the transformation of healthcare from a hospital-centered system to a person-centered environment, with a focus on citizens' disease management as well as their well-being [4]. It has been predicted that in the following decades, the way healthcare is currently provided will be transformed from hospital-centered, first to hospital-home-balanced in the 2020s, and then ultimately to home-centered in the 2030s [5]. This essential transformation necessitates the fact that the convergence and overlap of the IoT architectures and technologies for smart spaces and healthcare domains should be more actively considered [4, 6, 7, 8].

Healthcare IoT systems are distinct in that they are built to serve human beings, which inherently raises the requirements of safety, security, and reliability. In such systems, improving a patient's quality of life is important to mitigate the negative effects of being hospitalized. Providing patients with the possibility to walk around the medical environments and knowing that the monitoring of their health conditions is not interrupted is an important feature. Moreover, healthcare IoT systems have to provide real-time notifications and responses regarding the status of patients. The development of personal mobile devices, such as smartphones and tablets, is helping to establish a model of mobile health that can facilitate a continuum of person-centered care. The care can be done by relying on these mobile devices as a medium of sensing, interaction, and communication. Smartphones are embedded with an array of sensors that can track a user's motion, location, activity, and so forth. However, these devices still cannot collect detailed information for a user's bodily health. A wide array of wearable devices has recently been developed to extend the capabilities of mobile devices, especially in the area of body and behavior sensing. Wearable devices encompass a variety of functions, including data collection from on-body sensors, preprocessing of data, temporary data storage, and data transfer to internet-connected immediate neighbors. These devices also offer significant advantages to healthcare by automating remote healthcare interventions that include diagnostic monitoring, treatments, and interoperability between patients and physicians.

Healthcare IoT systems raise important questions and introduce new challenges for the security of systems and processes and the privacy of individuals. One of the main problems in IoT systems is the significant number of devices that are getting connected to the Internet. Connecting more devices causes the available resources, such as bandwidth and computing power, to be shared by more nodes leading to quality and performance degradation. However, this degraded infrastructure is unacceptable because of the critical application domain. Also, a large portion of these devices are resource constrained. This shortage of resources adds more design limitations to the architecture design. To guarantee these requirements, the smart components in the healthcare IoT system require a reliable communication architecture. Wearable IoT (WIoT) is defined as technological infrastructure. WIoT interconnects wearable sensors to enable monitoring human factors, including health, wellness, and behaviors to enhance individuals' everyday quality of life. Wearable sensors offer significant advantages to healthcare by automating remote healthcare interventions that include diagnostic monitoring, treatments, and interoperability between patients and physicians. In a typical WIoT system, the system has to ensure the safety of patients by monitoring patients' activities and vital signs. Also, physicians, patients, and other caregivers demand a reliable system in which the results are accurate and timely, and the service is secure and dependable.

Due to the direct involvement of humans in WIoT, providing robust and secure communication among medical sensors, actuators, and caregivers is crucial. Although collected from innocuous wearable sensors, such data is vulnerable to top privacy concerns [9, 10, 11, 12]. For example, some wearable devices collect sensitive information, such as the user's absolute location and movement activities. If this information is not safeguarded during the process of storage or communication, the patient's privacy may be compromised. Misuse or privacy concerns may restrict people benefiting from WIoT technology. There may also be a possibility of severe social unrest due to the fear that government or private organizations are using such devices for monitoring and tracking individuals [13]. Internet Protocol (IP) enabled sensors in a Medical Sensor Network (MSN) can transmit medical data of patients to remote healthcare services.In such scenarios, the conveyed medical data may be routed through an untrusted network infrastructure, such as the Internet. Misuse or privacy concerns restrict societies from utilizing IoT-based healthcare applications. Robust techniques and methodologies are needed to control and limit attacks against these networks.

Although there is a rich body of literature in the field of communication security for healthcare IoT systems, a significant gap in this area still exist. The main challenge encountered by the existing security solutions is how to provide *End-to-End* security in a way that end-points in these systems would be able to securely and efficiently communicate with each other beyond the local network boundaries. End-to-end security philosophy takes a holistic, start-to-finish approach to security design. The idea is to secure all communication from the preliminary source to the end destination using relevant security schemes/protocols to eliminate all potential for third party intrusion. To achieve this, security should be built in where applicable, and enhanced via additional layers of security that start protecting communications upon initial establishment. Taking an end-to-end security approach to healthcare IoT security can help solve common problems with healthcare IoT including data tampering, snooping, and device take-over attacks that often occur in healthcare IoT environments.

In the paradigms of healthcare IoT, not only data can be collected by smart devices (medical sensors) and transmitted to end-users (caregivers), but end-users can also access, control, and manage medical sensors through the Internet. Since patients' health data is the basis for enabling applications and services in healthcare IoT, it becomes imperative to provide secure end-to-end communication between end-users, medical sensors, and health caregivers to protect the exchange of health data. To enable the secure end-to-end communication, mutual authentication and authorization of end-users and healthcare IoT devices/services is a crucial task. This is to block eavesdropping on sensitive medical data as well as malicious activities at the entrance to the healthcare IoT. Medical sensors rely on cryptography to secure their end-to-end communications. Proper application of cryptography requires the use of secure keys and key generation methods. Cryptographic Key generations relying on physiological features/parameters of individuals' body are proper solutions for tiny medical sensors as those solutions are lightweight and require low resources. Cryptographic keys can be generated within the network on the fly via the usage of information collected by medical sensors when and as needed. The generated keys can be employed in end-to-end communications to securely encrypt/decrypt messages (e.g., patients' medical data) transmitted between medical sensors and health caregivers. The keys can also be used for authentication and authorization of peers in healthcare IoT systems. Mobility support is also one of the most important issues in healthcare IoT systems. Enabling mobility for healthcare IoT systems offers a high quality of medical service, as it allows patients to move around freely within the premises. Patients do not need to be worried about moving around because the system can enable mobility while continuously monitoring vital signs. The mobility support can be provided to the healthcare IoT ubiquitously without compromising the end-to-end security.

For these reasons, this thesis focuses on proposing an end-to-end security solution for healthcare IoT systems through specifying and developing a novel distributed architecture considering resource constraints, as well as security levels of IoT devices and services, supports mobility of individuals, and offers a low-latency solution for personalized unique cryptographic key generation. The proposed solution is not just limited to a specific healthcare environment, it can be applied to any environment of healthcare IoT that requires a secure end-to-end communication.

1.1 Objectives and Research Questions

In this thesis, we explore, identify, examine, and provide research-based solutions and suggestions for the challenges concerning the security of the healthcare IoT systems. In summary, the following objectives and research questions have been delineated.

- Creating an efficient standards-based communication architecture for healthcare IoT systems. The architecture ensures security and seamless availability of medical IoT devices and services, as well as ubiquitous mobility.

- Creating the building blocks of secure end-to-end communication for healthcare IoT systems. The created blocks offer peer authentication and authorization to highly resource constrained IoT devices. The authentication and authorization of the healthcare IoT peers are done using personalized unique cryptographic keys.

The following research questions (RQs) are addressed to achieve the objectives of end-to-end security in healthcare IoT systems.

- RQ1: How to design a reliable and robust communication architecture that considers the constrained nature of healthcare IoT devices?

  The architecture of a system provides information about the components, the organization of the parts, and the interactions. It is one of the critical elements for achieving graceful scaling and performance. Among the non-functional requirements that constrain the system architecture design, few of these are scalability, usability, and performance. In most healthcare IoT applications, especially in smart homes and hospitals, there exists a bridging point, which is a gateway between a sensor network and the Internet that often performs essential functions such as translating between the protocols utilized in the Internet and sensor networks [14, 15].

- RQ2: How to design a secure healthcare IoT architecture such a way that it ensures seamless availability of IoT devices/services and ubiquitous mobility?

  Healthcare IoT services are supposed to be offered to patients in a seamlessly and continuously way when the patients are moving. An essential feature is giving patients the ability to walk around the hospital wards knowing their health condition is being monitored without interruption. In a case that a moving sensor loses its connection with one of the smart gateways, health caregivers will stop monitoring the patients. This condition is not favorable in situations where real-time and continuous monitoring is necessary. Distributed smart e-health gateways can provide seamless availability and ubiquitous mobility of healthcare IoT systems. By exploiting smart e-health gateways in a distributed fashion, the tasks of a centralized gateway can be broke down to be handled by distributed smart gateways.

- RQ3: How unauthorized access and intrusion attempts can be prevented in healthcare IoT systems?

  In a healthcare IoT system, security and privacy of patients are among significant areas of concern, as most devices and their communications are wireless. Performing mutual authentication and authorization, trustworthy communication of healthcare IoT devices and services can barricade unauthorized access and intrusion attempts. With mutual authentication and authorization, trustworthy communication can occur when one device trusts the other devices. Therefore, eavesdropping on sensitive medical data or malicious triggering of specific tasks can be prevented, and any malicious activity can be blocked before entering a medical constrained domain.

- RQ4: How to enable the end-points of a healthcare IoT system to communicate beyond the independent network securely?

End-to-end security is one of the significant requirements in healthcare IoT systems. This feature enables the end-points of a healthcare IoT system to communicate securely. Designing a handshake delegation architecture using a session resumption technique can efficiently achieve a secure end-to-end communication. The main idea to employ session resumption is to perform heavy-weight operations only once, during an initial handshake connection phase. Thus, the peers need to keep a minimal session state, even after the session is terminated. The session resumption enables the peers to resume the secure connection without the need for running expensive operations and transmitting long certificates.

- RQ5: How to exploit the human body as the authentication identity and the means of generating and managing cryptographic keys to secure Body Area Networks (BANs)?

  Given the constrained nature of medical sensors used in BSNs, conventional key generation approaches may potentially involve reasonable computations, as well as latency during network or any subsequent adjustments, due to their need for pre-deployment. Biometrics are generally regarded as the only solution that is lightweight, requires low resources, and, indeed, can identify authorized subjects in BANs [16, 17, 18, 19]. The choice of a biometric to be used for generating cryptographic keys relies on the capability of medical sensor nodes on extracting an individual's relevant biometric information. It has been found that the next generation of biometrics (also known as physiological or bio-signals) are the best candidates to be employed for the authentication and generating cryptographic keys. Because cryptographic keys generated using humans' physiological signals have the following specifications. First, they are different for different subjects at any time. Second, they are different for the same person at different time intervals. Third, they are cryptographically random to provide security. Finally, they are measurable from each subject.

1.2 Research Contributions

This thesis comprised of five main contributions. These contributions are presented in detail in the original publications in Part II of the thesis. A brief overview of the main contributions is presented in the following:

1. Pervasive Health Monitoring Based on Internet of Things: The IoT-based pervasive healthcare system has the potential to offer an error-free alerting system, as well as medical data, in critical conditions with continuous monitoring. Such a system minimizes the need for dedicated medical personnel for patient monitoring and helps the patient lead a normal life in addition to providing high-quality medical service. In this thesis, our first contribution is to provide the implementation of IoT-based architectures for remote health monitoring based on two popular wireless technologies, the Institute of Electrical and Electronics Engineers (IEEE) 802.11 Wireless Local Area Network (WLAN) and IEEE 802.15.4 (ZigBee). We present a health monitoring wireless sensor network architecture and assess the usability of two wireless communication technologies in the presented context. The aim is to identify the advantages and shortcomings of these architectures and find application domains in which these architectures can be properly utilized. ZigBee exploits mesh topology, which has different advantages over point to point networks in terms of scalability, reliability, and addressing interference issues by the structure. IEEE 802.11 WLAN offers all the benefits of IP standards such as compatibility, heterogeneity, flexibility, speed, efficiency, security, and accuracy. To provide a proof of concept, the experimental setup to compare both architectures was developed. The scenario was comprised of a hospital room with 20 patient nodes reading patient's medical data from different sensors. The sensors are two-lead Electrocardiogram (ECG), Blood Oxygen Saturation (SpO2), Blood Pressure, Heart Rate, Temperature, Respiration, and Glucose level. We observed that the power consumption in the ZigBee based network was less than the IEEE 802.11 WLAN based network for the same experimental setup. The IEEE 802.11 WLAN based network consumed more power than ZigBee for lower data-rate. While, with an increase in data rate, power consumption in ZigBee increased rapidly when compared to IEEE 802.11 WLAN. In the case of a star topology, the network can support up to 18 nodes. Whereas in the case of mesh topology using multi-hopping, each node can route data of up to 17 other nodes apart from transmitting the data acquired, thus increasing the scalability to a higher number. At the present data rate, scalability is not an issue in the case of IEEE 802.11 WLAN and the system can be scaled to a large number of nodes using a single access-point.

2. Mutual Authentication Scheme for RFID Implant Systems: The IoT is emerging as an attractive future networking paradigm. The IoT consists of smart objects and low-power networks, such as Radio Frequency Identification (RFID) networks, Wireless Sensor Networks (WSNs), BANs, and actuators. The second contribution of this thesis is a novel secure mutual authentication scheme for RFID implant systems. An insecure communication channel between a tag and a reader makes the RFID implant system vulnerable to attacks and endangers the user's safety and privacy. The proposed scheme relies on elliptic curve cryptography and the D-Quark lightweight hash design. The D-Quark lightweight hash design is tailored for resource- constrained pervasive devices, cost, and performance. The proposed scheme consists of three phases: (1) the reader authentication and verification phase, (2) the tag identification phase, and (3) the tag verification phase. In the proposed scheme, we suppose the communication between the reader and the back-end database server is done through a secure channel while communication between the RFID implant tag and the reader is not secure. We proved that the proposed scheme is secure against the relevant attacks and also ensures a higher security level than related work found in the literature. Also, we carried out a computational performance analysis of the proposed scheme. The analysis results show that the elliptic curve-based mutual authentication scheme has less communication overhead than similar available schemes. It also requires less total memory compared to existing schemes.

3. Low latency approach for ECG feature-based cryptographic key generation: The third contribution of this thesis is a novel ECG feature based cryptographic key generation approach that has a low-latency key generation time and offers a high-security level [20]. The approach uses Several ECG Features (SEF) in addition to the Interpulse Interval (IPI) feature of an ECG signal. SEF consists of (1) detecting the arrival time of the ECG's fiducial points using a Daubechies wavelet transform to compute the ECG's main features accordingly; (2) using a dynamic technique to specify the optimum number of bits that can be extracted from each main ECG feature; (3) generating cryptographic keys by exploiting the above-mentioned ECG features; and (4) consolidating and strengthening the SEF approach with a cryptographically secure Pseudo-random Number Generator (PRNG). Fibonacci Linear Feedback Shift Register (LFSR) and Advanced Encryption Standard (AES) algorithms are implemented as the PRNG to enhance the security level of the generated cryptographic keys. We mainly investigated the property of randomness of the main ECG features, including PR, PP, QT, and ST intervals. The investigation was done to ensure that they can be used along with IPI for generating cryptographic keys. The approach was applied to normal and abnormal ECG signals. The main contributions of this work are comprised of four main phases. The approach was applied to the ECG signals of 239 subjects; the signals were comprised of Normal Sinus Rhythm, Arrhythmia, Atrial Fibrillation, and Myocardial Infarction. We investigated the security of the generated keys in terms of distinctiveness, a test of randomness, temporal variance, as well as using the National Institute of Standards and Technology (NIST) benchmark. We also investigated the efficiency of the approach in terms of key generation execution latency.

4. End-to-end security for mobility-enabled healthcare IoT: The fourth contribution of this thesis is a novel secure end-to-end communication scheme for the healthcare IoT system, which significantly alleviates some burden of medical sensors. The proposed scheme consists of (1) a secure and efficient peer authentication and authorization architecture based on the certificate based DTLS handshake, (2) secure end-to-end communication based on session resumption, and (3) robust mobility based on interconnected smart gateways. In [21], we presented a secure and efficient authentication and authorization architecture for the healthcare IoT system using smart e-health gateways called *SEA*. In [22], we introduced a comprehensive end-to-end security scheme for healthcare IoT systems using the session resumption technique. The architecture relies on the certificate-based DTLS handshake protocol as it is the primary transport layer security solution for IoT systems. The proposed end-to-end security scheme enables end-users and medical sensors to communicate without need to perform heavy computations. To provide end-to-end security, the DTLS session resumption technique without the server-side state is used. This form of session resumption offloads the encrypted session states of DTLS toward non-resource-constrained end-users for the subsequent communication utilized. The main motivation to employ the DTLS session resumption was to mitigate the overhead on resource-constrained sensors.

We exploited the concept of Fog Computing in IoT for realizing efficient and seamless mobility since fog extends the cloud paradigm to the edge of the network [23, 24, 25]. Mobility support can be ubiquitously provided to the medical sensors from the fog layer. Thus, no more reconfiguration is needed in the resource-constrained device layer. To enable seamless transitions of medical sensors, we provided an efficient and robust data handover mechanism among smart gateways, considering the limitations of sensors. The mobility scenario comprises of three main phases. The first phase includes message exchange in the patient's base MSN. This phase presents the initial state of the medical sensors, where each sensor is connected to its base MSN via smart e-health gateway and exchanges the required messages. The second phase is when a patient moves out of his or her base MSN to a new medical subnetwork. In this case, the sensor detects if the quality of the connection with the associated smart gateway is reduced below a predefined threshold. We propose to provide mobility support to the sensors from the fog layer to alleviate the processing and computation burden of the sensors. To enable mobility for healthcare IoT systems, neighbor solicitation and data handover functions are performed in the fog layer between smart gateways. The third phase is when the patient returns back to his or her base network. In this case, the medical sensor sends a reassociation request to inform the smart gateway regarding its new location.

We evaluated our end-to-end security scheme in terms of security and energy performance analysis. We also proved that the work fulfills the requirements of full end-to-end security and ensures a higher security level compared to the existing solutions. The analysis of the implementation revealed that the handover latency caused by mobility is low. Also, the handover process does not incur any processing or communication overhead on the sensors.

5. Performance Analysis of End-to-End Security in Healthcare IoT: The fifth contribution of this thesis is to analyze the performance of the state-of-the-art end-to-end security schemes in healthcare IoT systems. We identified that the essential requirements of robust security solutions for healthcare IoT systems comprised of (1) a low-latency secure key generation approach using patients' ECG signals, (2) secure and efficient authentication and authorization for healthcare IoT devices based on the certificate-based DTLS, and (3) robust and secure mobility-enabled end-to-end communication based on DTLS session resumption. The performance of the state-of-the-art security solutions, including the end-to-end security scheme, was tested by developing a prototype healthcare IoT system. We found out that our solution had the most extensive set of performance features in comparison to related approaches found in the literature. The performance evaluation results show that the proposed cryptographic key generation approach was faster than existing key generation approaches while being more energy-efficient. In addition, the scheme reduced the communication overhead and the communication latency between smart gateways and end users. The scheme is also faster than certificate based and faster that symmetric key-based DTLS. On the other hand, the Read Only Memory (ROM) and Random Access Memory (RAM) requirements of our scheme were almost as low as those in symmetric key-based DTLS.

1.3 Research Methodology

The research methodologies in this thesis are summarized below:

- Design a pervasive health monitoring wireless sensor network architecture and assess the usability of two wireless communication technologies in the presented context. For the health monitoring platform, we used IEEE 802.11 WLAN and ZigBee wireless technologies. The experimental setup to compare both architectures consisted of a hospital room with 20 patient nodes reading a patient's medical data from various sensors. The employed sensors were a two-lead ECG, SpO2, Blood Pressure, Heart Rate, Temperature, Respiration, and Glucose level. There was one sink node for the ZigBee based architecture or an IEEE 802.11 WLAN access point for the IEEE 802.11 WLAN based architecture to collect data from all the patient nodes in the respective setup. The distance between the adjacent patient nodes in the same column was two meters, and the distance between the adjacent patient nodes in the different columns was six meters. Every patient node transmitted approximately 8.7 kbits of data per second.

- Evaluate the proposed secure elliptic curve-based mutual authentication scheme for RFID implant systems that are used in healthcare IoT applications. In this work, we mainly focused on the performance analysis of implantable tags because RFID readers are known to be robust devices [26]. As a common cryptographic primitive, we exploited standardized 163-bit elliptic curve domain parameters recommended by NIST. The parameters were defined over the binary finite field $\mathrm{F}(2^{163})$. We utilized the Elliptic Curve Digital Signature Algorithm (ECDSA) algorithm having the coordinate (x, y). As a reminder, the elliptic curve domain parameters over $\mathrm{F}(2^m)$ were specified by the tuple $T = (m, f(x), a, b, G, n, h)$, where $m = 163$ and the representation of $\mathrm{F}(2^{163})$ is defined by $f(x) = x^{163} + x^7 + x^6 + x^3 + 1$ [27]. As an environment to measure the computational time for the mentioned cryptography algorithms, we used an Intel Core2 CPU T5500 1.66 GHz having 1GB RAM. In the proposed scheme, we outlined the storage requirement by considering the tag's memory, including its public key and private key. The private key is denoted as the tag's secret keys s_1 and s_2 and the public key is the tag's public key ID_t. In the proposed scheme, the required memory consists of (ID_t,s_1,s_2).

- Evaluate the security level and performance of the proposed ECG-based cryptographic key generation approaches in terms of distinctiveness, a test of randomness, temporal variance, and key generation execution time. We conducted the experiments on both normal and abnormal ECG signals obtained from the publicly available and widely used database, that is, Physiobank [28]. PhysioBank is comprised of databases of multi-parameter neural, cardiopulmonary, and other biomedical signals from patients and healthy subjects with a variety of conditions. Subject conditions may include sudden cardiac death, irregular heartbeat (arrhythmia), congestive heart failure, sleep apnea, and epilepsy. The experiments were carried out on both normal and abnormal. ECG signals which, were obtained from 239 subjects studied by the Beth Israel Hospital Laboratory in Boston and the National Metrology Institute of Germany (Physikalisch-Technische Bundesanstalt (PTB)).

  The employed ECG signals included: (1) ECG signals of 18 subjects (five men, aged 26 to 45; 13 women, aged 20 to 50) with Normal Sinus Rhythm. The recordings were digitized at 128 samples per second with a 11-bit resolution over a 10 mV range. (2) ECG signals of 48 subjects with Arrhythmia (22 women aged 23 to 89; 26 men aged 32 to 89) were recorded using two-channel ambulatory ECG system.

The recordings are digitized at 360 samples per second with an 11-bit resolution over a 10 mV range per patient. (3) ECG signals of 25 men with Atrial Fibrillation were recorded for 10 hours and contained two ECG signals, each digitized at 250 samples per second with 12-bit resolution over a range of 10 mV. (4) ECG signals of 148 subjects with Myocardial Infarction (89 men aged 17 to 87; 59 women aged 19 to 83). Each signal was digitized at 1000 samples per second, with 16-bit resolution over a range of 16 mV. We captured 100 different samples of 5-minute long ECG data for each subject and evaluated the efficiency of the approach. The collected ECG signals were filtered using a low-pass filter with a 30 Hz threshold frequency. Such a filter reduces environmental noise and provides a smoother signal for further analysis. For the experiment, we generated 128-bit cryptographic keys using the approaches mentioned above. We implemented and analyzed the key generation approaches utilizing MATLAB [29].

- The system architecture of distributed end-to-end communication supporting mobility was implemented for experimental evaluation. To Implement the architecture, we set up a platform that consisted of medical sensors, UT-GATE smart e-health gateways, a remote server, and end-users. A UT-GATE was constructed from the combination of a PandaBoard [30] and a Texas Instruments (TI) SmartRF06 board that was integrated with a CC2538 module [31]. The PandaBoard is a low-power and low-cost single-board computer development platform based on the TI OMAP4430 System-on-chip (SoC) following the OMAP architecture and fabricated using 45 nm technology. The OMAP4430 processor is composed of a Cortex-A9 Microprocessor Unit (MPU) subsystem including dual-core ARM cores with symmetric multiprocessing at up to 1.2 GHz each. In the configuration, UT-GATE used 8GB of external memory and was powered by Ubuntu OS, which allowed for controlling devices and services, such as local storage and notification. To investigate the feasibility of the proposed architecture, the *Wismote* [32] platform, which is a common resource-limited sensor, was utilized in Contiki's network simulation tool Cooja [33].

  Wismote is equipped with a 16MHz MSP430 micro-controller, an IEEE 802.15.4 radio transceiver, 128KB of ROM, 16KB of RAM, and supports 20-bit addressing. For the evaluation, we used the open source tool *OpenSSL* version 1.0.1.j to create elliptic curve public and private keys from the NIST P-256 (prime256v1) and X.509 certificates. The prevailing form of certificates are X.509 and are employed in the certificate-based mode of DTLS [34]. The server association to the end-user was created using Open Secure Sockets Layer (SSL) Application Programming Interface (API). It provided all necessary functions related to end-users, including configuration, certificate, handshake, session state, and cipher suites to support session resumption. *TinyDTLS* [35] was used as the code-base of the proposed scheme, in this work. TinyDTLS is an open-source implementation of DTLS in symmetric key-based mode. We extended it with support for the certificate-based DTLS as well as session resumption. For the public-key functions, we utilized the *Relic-toolkit* [36] that is an open source cryptography library tailored for specific security levels with an emphasis on efficiency and flexibility. The My Structured Query Language (SQL) database was set up for static and non-static records. Static records that are managed by system administrators include white tables, essential data required by the DTLS handshake, and an end-user authentication mechanism. Non-static records store up-to-date biosignals that are synchronized between the PandaBoard database and a cloud server database. The cloud server database was processed using xSQL Lite, which is a third party tool for data synchronization. Concerning the cryptographic primitives and to make a fair comparison, we followed similar cipher suites as employed in the most recently proposed authentication and authorization architecture for IP-based IoT [36]. In this regard, we utilized elliptic curve NIST-256 for public-key operations, $AES\_128\_CCM\_8$ (with an IV of 8 bytes) for symmetric-key, and SHA256 for hashing operations.

1.4 Thesis Organization

The thesis consists of two main parts. Part I provides a research summary, while Part II presents the original publications. Part I consists of the following chapters:

- Chapter 1 introduces the motivation for this work and presents the research questions and a brief overview of the research contributions.

- Chapter 2 provides the background and discusses important topics related to the works.

- Chapter 3 presents a summary of the main contributions while focusing on the challenges that they address.

- Chapter 4 provides a description and organization of the original publications and provides a mapping between the publications and the RQs.

- Chapter 5 presents conclusions, future research directions, and our approach to validate the research work.

Chapter 2

Background and Related Work

In this chapter, we first provide a brief overview of the necessary background concepts and technologies on which this thesis is based. These include IoT, healthcare (medical) IoT, and healthcare IoT communication architectures. Then, we present the most important related works on authentication and authorization, end-to-end security, mobility management, and cryptography and constrained devices in healthcare IoT systems.

2.1 Resource-Constrained Network Environments

Resource-constrained networks comprise of constrained devices that are equipped with confined memory, power resources, and CPU. These devices can enable physical world objects to become smart via communication, sensing, and actuating functionalities. Exemplary application scenarios include collecting sensing information about automated monitoring or management of factories, natural ecosystems, healthcare monitoring, and home automation. We briefly present the specifications of such devices and the networks in which they operate.

Constrained Nodes: Resource-constrained devices can be everyday ”dumb” objects that are capable of network communication and they can interact with the physical world. The communication with the physical world is, for instance, feasible via sensors and actuators. This can be done by attaching a Micro Controller Unit (MCU) to a dumb object or using tiny sensors or actuators as standalone devices. Constrained devices have low-power Central Processing Units (CPUs) with few kilobytes of memory for code and data. In addition, the devices may be battery-powered, which makes energy efficiency an essential requirement. These devices are mostly communicated wirelessly, whereas border routers and Gateways (GWs) connect a WSN to another network, like the Internet, are communicated over wire [37]. A prevalent link-layer technology for WSNs is IEEE 802.15.4 [38]. The platforms for evaluation and implementation objectives rely on IEEE 802.15.4. There are also other low-power radio technologies available, like Low-Power IEEE 802.11 [39] and Bluetooth Low Energy (BLE) [40].

The Internet Engineering Task Force (IETF) proposes a classification of constrained sensor nodes considered the capabilities of these devices, as well as memory limitations [33]. This classification comprises of three classes of constrained sensor devices. *Class 0*, these devices are highly resource-constrained and have memory sizes of below 10 (i.e., data memory e.g., RAM) to 100 (i.e., program memory e.g., Flash) kbyte. These devices perform sensing functionality, but they cannot communicate directly with the Internet nodes. *Class 1*, these devices are more powerful and offer memory resources within the order of 10 (i.e., data memory) to 100 (i.e., program memory) kbyte. Such devices present a tailored IP stack and can participate in Internet communication. Compared to class 0 sensor devices, class 1 devices are capable of establishing secure end-to-end communications. *Class 2*, these devices offer memory resources within the order of 50 (i.e., data memory) to 250 (i.e., program memory) kbyte. These sensor devices do not need modified stacks and are tailored for efficiency purposes. This thesis mainly focuses on class 1 devices, while dividing these devices further into two sub-classes. (1) The highly resource-constrained class 1 devices cannot perform Public Key Cryptography (PKC) operations, due to expensive computations and high memory requirements. (2) The less resource-constrained class 1 devices can at least meet memory requirements for PKC primitives.

Constrained Node Networks: Resource-constrained devices generally operate in low-power IP networks. This is due to the constrained nature of these embedded devices with limited resources. The limited resources account for smaller packet queueing possibilities in a resource-constrained sensor node that originates the "lossy" nature of Low power and Lossy Networks (LLNs). In addition, the prices of sensor nodes should be kept as low as possible due to economies of scales. Using cheap radio chips in constrained networks has the drawback that they cause high bit error probabilities as well as high packet loss rates. As a result, links among sensor nodes in these constrained network environments are not reliable and cause packet losses. Moreover, radio communication in constrained networks is more energy consuming than in-node computations. It is basically due to the mentioned network characteristics and the higher current draw of the radio chip. Thus, alleviating conveyed bytes via in-node computation is a common measure to make constrained network applications more energy efficient [41]. The IEEE 802.15.4 communication standard defines the Medium Access Control (MAC) and Physical layers for these resource-constrained networks [38]. The data rate in constrained networks is quite low, that is, 250 kbit/s for IEEE 802.15.4-based networks. In addition, for link layer frames in the IEEE 802.15.4 standard, the Maximum Transmission Unit (MTU) is 127 bytes. This reduces the probability of collisions and interference and offers the transmission of full frames in short period of times. Further significant features offered by the standard are collision avoidance through integrated security support and Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA).

2.2 IoT: Definition, Applications, and IP Adaptation

The IoT is the network of physical devices embedded with actuators, sensors, electronics, software, and connectivity which, enables these objects to connect and exchange data. Each device is uniquely noticeable through its embedded computing system but can interoperate within the current Internet infrastructure. IoT realizes the interconnection of resource-constrained devices with the Internet. IoT builds an infrastructure that expedites the realization of future technologies. The vision of the IoT brings the connectivity of all "*things*" to the Internet. One of the provocative forces of rendering IoT devices IP-enabled is the connectivity prerequisite. IP-enabled IoT networks are more effective with respect to maintenance. This is due to the broad experience of IP networks. The utilization of a popular protocol stack, for example IP, also offers the interoperability of heterogeneous devices from various producers.

Shelby *et al.* [42] presented definition for the IoT: *"As the Internet of routers, servers and personal computers have been maturing, another Internet revolution has been going on- The Internet of Things. The vision behind the Internet of Things is that embedded devices, also called smart objects, are universally becoming IP enabled, and an integral part of the Internet. Examples of embedded devices and systems using IP today range from mobile phones, personal health devices and home automation, to industrial automation, smart metering, and environmental monitoring systems. The scale of the Internet of Things is already estimated to be immense, with the potential of trillions of devices becoming IP-enabled. The impact of the Internet of Things will be significant, with the promise of better environmental monitoring, energy savings, smart grids, more efficient factories, logistics, healthcare, and smart homes."*

Constrained IoT networks are becoming IP-enabled and therefore moving away from isolated WSNs into interoperable and interconnected networks. This necessitates an IP adaptation layer that adapts IP packets in such a way that they can be routed in constrained networks, for example, IEEE 802.15.4-based networks. This adaptation layer for IEEE 802.15.4-

based networks is called IPv6 over Low-power Wireless Personal Area Network (6LoWPAN) [43, 44]. It is located between the *Data Link Layer* and the Network Layer. 6LoWPAN is relevant to this thesis, as its performance affects the connectivity and, therefore, the secure end-to-end communication. IEEE 802.15.4 offers an MTU of 127 bytes. Subtracting the maximum MAC protocol overhead from the MTU leaves 102 bytes available for the upper layers. If link layer security using AES-Cipher Block Chaining-Message Authentication Code (CCM)-128 is enabled, then just 81 bytes are left. After subtracting the 40 bytes of Internet Protocol version 6 (IPv6) header, just 41 bytes are left, from which the transport-layer protocol header needs to be deducted. In the case of User Datagram Protocol (UDP), 8 bytes that causes a very short payload length for the actual application-layer data, while IPv6 needs the support of a maximum MTU of 1280 bytes which signifies IPv6 packets with maximum MTU length cannot be conveyed over IEEE 802.15.4-based networks without fragmentation. These overheads and requirements are coped with the 6LoWPAN adaptation layer.

The 6LoWPAN offers the functionality of mapping between IEEE 802.15.4-based networks and the traditional IP networks through (1) encapsulation of IP packets into IEEE 802.15.4 frames and vice versa, (2) fragmentation mechanism because of the adaptation of the packet sizes, (3) header compression mechanisms to reduce the overhead caused by large IPv6 headers [45]. The 6LoWPAN header compression systems [46, 47] reduce the UDP and IPv6 header sizes. The 6LoWPAN encodes the IPv6 header in the best case in only 2 bytes, which represents the whole information from the header in a compressed way. Based on the above definition, the IoT is creating new revenue models, driving a new industrial revolution, and unprecedented levels of innovation. Today's challenge is not only to deliver massive, secure connectivity for the IoT but to ensure new technology experiences and business opportunities. The ability to network embedded devices with limited power resources and memory means that the IoT finds applications in nearly every field. The applications for internet connected devices are very extensive. From building automation, smart cities, smart factories, smart energy to smart healthcare, the IoT touches every facet of our lives. While these applications are limitless, several key vertical markets are emerging as areas where it is likely to scale. These foundational IoT markets serve as proving grounds where companies, research organizations, and individual developers can explore the possibilities of what the IoT can deliver.

2.3 IoT in Healthcare Environments

Healthcare represents one of the most remarkable application areas for the IoT. *Medical IoT*, sometimes called *Healthcare IoT*, refers to a rising number of IoT exploits in the medical industry. These produce a wide range of IoT devices and applications specifically designed for healthcare environments, such as sensors and apps for consultation, remote healthcare monitoring, and delivery. The IoT has the potential to give rise to many medical applications such as remote health monitoring, chronic diseases, fitness programs, and elderly care. It also offers life-changing improvements to traditional medical devices, for example the smart inhaler for people with asthma. Compliance with medication and treatment at home by healthcare providers is another important application. Hence, medical devices, sensors, and imaging and diagnostic devices can be viewed as smart devices or objects constituting a core part of the healthcare IoT.

IoT-based healthcare services are expected to reduce the costs of healthcare, increase the quality of life, and enrich individuals' experiences. Ease of cost-effective interactions through seamless and secure connectivity across individual patients, clinics, homes, and healthcare organizations is an important trend. From the perspective of healthcare providers, the IoT has the potential to reduce device downtime through remote provision. This can precisely identify optimum times for replenishing supplies for medical devices for their smooth and continuous operation. Up-to-date healthcare systems driven by IoT technology are expected to support early diagnoses, real-time monitoring, chronic diseases, and medical emergencies. Medical servers, smart gateways, and health databases play crucial roles in creating health records and delivering on-demand health services to authorized health caregivers. Personalized healthcare is based on an individual's exclusive biological, behavioral, and social characteristics. This leads to premiere outcomes by making healthcare cost-effective. High quality healthcare service focuses on home care and early disease detection, rather than the exclusive clinical one.

IoT and healthcare can bring each other a lot of profit. The IoT enables handling of the care personalization services as well as preserving a digital identification for every individual. Various equipment are employed in healthcare, to communicate, and to make the omnipresent system-of-system. Thus, an efficient categorization of the IoT based on personalized healthcare systems includes remote monitoring, and clinical care systems as follows: (1) *Remote Monitoring System:* this system allows access to health monitoring by using wireless solutions that are connected using IoT technology in order to monitor patients. Various algorithms and IoT devices are employed for data analysis and then share this information remotely with the medical professionals through wireless connectivity. (2) *Hospitalized Care System:*

this system uses both invasive and non-invasive monitoring IoT systems for the hospitalized subjects. This clinical care system employs medical sensors for collecting physiological information that is stored in the cloud for further analysis. This improves the quality of healthcrae with lower cost. The general framework for the IoT includes different architectures for the health monitoring system. (3) *Wearables:* there are a lot of devices that patients can wear every day, for example blood pressure, fitness bands, and heart rate monitoring cuffs, etc. These gadgets monitor not only the user's daily activity but also collect data about taken steps, burnt calories, etc. These devices change the patients' lives, especially elderly people as they allow constantly tracking their health conditions. Wearables can send notifications to the family members about changes in the routine activities or any other condition variation of the user. (4) *Medication Management:* to produce and manage medicines, a lot of money are spent. In this regard, IoT devices can provide an opportunity to follow all safety standards of the pharmaceutical market. One of the best examples is the smart vaccine fridge. It is able to prevent vaccines from spoiling and monitor their conditions 24/7.

The common features of the IoT-based health monitoring system include health data that are collected from sensors using MSNs, user displays and interfaces, and network connectivity to access infrastructure services. In such a system, patient health-related information is recorded by body-worn or implanted sensors, with which the patient is equipped for personal monitoring of multiple parameters. This data can also be supplemented with context information such as, date, time, location, and temperature. This feature enables to identify unusual patterns and make more precise inferences about the situation. Followings are some advantages of Healthcare IoT. (1) *Lower Expenses:* there are many gadgets that can track health condition which enable medical employees to monitor patients' health in real-time mode. People do not need to visit doctors regularly which leads to fewer expenses. Also, people can stay at home, if they are not critically ill and doctors will see every change using telemedicine. (2) *Better Treatment Results:* These technologies as Fog/Cloud computing and medical devices connectivity enable doctors to see real-time data about patients using the healthcare IoT monitoring system. Therefore, doctors are able to analyze the symptoms faster and give proper treatment which leads to better care results. (3) *Better disease control:* receiving new data every day, doctors are able to find out disease earlier and start a proper treatment faster. (4) *Maintenance of Medical Devices:* medical devices are high-priced and any medical equipment requires a suitable maintenance to function normally. IoT plays a key role here as this technology can calculate all possible issues with any device. (5) *Fewer Mistakes:* These automated processes as data segmentation, data receiving, and data-driven decisions can decrease diagnosis errors.

The system architecture includes the following components:

1. MSNs: Enabled by the ubiquitous identification, sensing, and communication capacity, biomedical, and context signals are captured from the body or room which is used for treatment and diagnosis of medical states. The signal is then transmitted to the gateway via wireless or wired communication protocols such as Serial, Serial Peripheral Interface (SPI), Bluetooth Low Energy, IEEE 802.11 WLAN, or IEEE 802.15.4.

2. Gateway: The gateway supports different communication protocols, acts as a touching point between the MSN and the local switch/Internet. It receives data from different sub-networks, performs protocol conversion, and provides other higher level services such as data aggregation, filtering, and dimensionality reduction [4].

3. Back-End System: The back-end of the system consists of the remaining components, a local switch (in in-hospital domains), a cloud computing platform that includes broadcasting, data warehouse and big data analytic servers, and hospital local Database (DB) that periodically performs data synchronization with the remote healthcare DB server at the cloud to continuously synchronize patients' health data over time. In the cloud computing platform accessibility to patient-related health data is classified as public data such as, a patient's Identity Document (ID) or blood type, and private, data such as Deoxyribonucleic Acid (DNA), based on the relevance.

4. Web Clients: These clients are considered the graphical user interface for final visualization and apprehension. The collected health and context information represents a vital source of big data for the statistical and epidemiological medical research such as, detecting approaching diseases. The evolution in medical devices, electronics, and computer science has led to significant technological progress in the form of IoT realization. Nowadays, multiple sensor nodes can be connected to the Internet from in-home monitoring devices to hospital-based imaging. Thus, IoT-based healthcare systems offer enhanced care by systematizing the processes to securely facilitate the collaboration of the transferred information.

Intelligent systems provide physicians with efficient and easy access to health information to improve the patient experience. The followings are a few examples of applications of the IoT for healthcare. (1) *Heart Rate Monitoring*: In such a system, the biometrics of each subject are independently monitored using specific threshold settings. Such a monitoring system records the ECG Heart rate variability and reliability, the activity level of the heart, and respiration rate. In addition, supplementary devices used in conjunction can also monitor other vital signs, such as blood pressure. Generally, the heart rate monitoring system reports the rhythm to realize the cardiac role of impenetrable symptoms. (2) *Elderly Monitoring*: In such a system, IoT-based elderly monitoring is employed as a personalized home care solution for tracking and locating individuals' activities. Emergency calls can be managed in an actual cost system for wide area communication interface. This system comprises of wearable sensors that can be programmed in order to send reports to healthcare professionals.

2.4 Healthcare IoT Communication Architecture

For the discussion of healthcare IoT communication architecture, we recognize five main research directions: (1) pervasive health monitoring, (2) authentication and authorization of healthcare IoT components, (3) cryptographic keys and constrained IoT medical devices, (4) secure end-to-end communication of healthcare IoT systems, and (5) mobility management. The state-of-the-art related approaches for healthcare IoT communication architecture are discussed in the following section.

2.4.1 Pervasive Health Monitoring Based on the IoT

The IoT offers enormous opportunities to revolutionize healthcare in the near future. It can play a vital role in a wide range of healthcare devices that, for example, enable remote vital sign monitoring in hospitals and more importantly, at home. Indeed, remote monitoring offers tremendous possibilities to decrease the costs of healthcare, and, at the same time, to increase healthcare quality by identifying and preventing diseases. In many cases, health care is becoming increasingly costly, as patients are required to stay in the hospital for the entire duration of their treatments due to the lack of devices with the capability of remotely providing patients' health information to authorized health professionals. Using the IoT, gathering patient's health information and transferring it in real time to healthcare professionals will not only reduce the cost of healthcare services but also enable the treatment of health issues before they become critical. It is predicted that the number of devices with Internet capability will be around 50 billion by 2020 [48].

There have been many efforts in the field of IoT based remote patient monitoring systems. Piccini *et al.* [49] discuss wireless systems based on Bluetooth for acquiring bio-medical signals, such as ECG, Electromyography (EMG), Electroencephalography (EEG) and Electrooculography (EOG). The architecture consists of two operational units: one to acquire single-lead ECG signal and the other a Digital Signal Processing (DSP) system to clean the acquired signal from the first unit. More research is required for integrating the associated sensors with a hardware board and miniaturizing the system to make it wearable. She *et al.* [50] presented a wireless sensor network architecture based on the ZigBee and 3G networks for healthcare applications for home or hospital. The system reads signals, including ECG, EMG, EEG and EOG, heart rate, breathing, and blood pressure; processes it; and sends it to a remote server or displays it on an LCD screen. The system implements priority scheduling and data compression, which reduces the transmission delays of critical signals and saves bandwidth and power. Lo *et al.* [51] explained the BSN based on the IEEE 802.15.4 standard which not only monitors and processes medical data such as ECG and SpO2 but also implements context-aware sensing with the help of context sensors (for example, temperature, accelerometer, and humidity). The BSN is power efficient requiring only 0.01 mA in active mode and 1.3 mA for computations such as Fast Fourier Transform (FFT). A flash BSN card displays the collected and processed data for Personal Digital Assistants (PDAs). A PDA also works as an access point to send the processed data to a central server. Istepanian *et al.* [52] proposed the m-IoT (Internet of M-Health Things), an IP based wireless sensor network architecture based on 6LoWPAN, which is used to measure medical data, such as the glucose level in blood and blood pressure. A central access point collects data from the sensor nodes and sends to IP based medical server, from where it can be accessed and analyzed. Our motivation is to compare the implementation of health monitoring wireless sensor network architectures based on two popular wireless technologies, which are IEEE 802.11 WLAN and ZigBee, and analyze the suitability of these technologies for different medical applications.

2.4.2 Healthcare IoT Authentication and Authorization Approaches

This section deals with related research approaches for authentication and authorization of peers to be used for secure end-to-end communication in Wireless Sensor Networks (WSNs), the healthcare IoT. The authentication and authorization of peers are a critical requirement for a secure end-to-end communication as eavesdropping on sensitive medical data or malicious triggering of specific tasks can be prevented. We identify four main research directions: (1) Elliptic Curve Cryptography (ECC) based approaches, (2) centralized approaches, (3) delegation-based approaches, and (4) alternative delegation solutions that require special purpose hardware modules. In the following, we discuss important works of each of these directions in more detail.

1. Elliptic Curve-based Authentication and Authorization Approaches: In 2006, Tuyls *et al.* [53] proposed an ECC-based RFID identification scheme using the Schnorr identification protocol. They claimed that their scheme was resistant against tag counterfeiting. However, in 2008 Lee *et al.* [54] presented that this scheme suffered from a location tracking attack, as well as forward security. In such a scheme when an adversary can compute the public key $X(= -t.P)$ of a tag, it can benefit from X in order to get access to other information related to the tag. Lack of scalability is another problem of Tuyls *et al.*'s scheme because, at each time a tag needs to be identified, the reader should fetch the tag's public key from the database server to verify it. This means that the reader requires to perform a linear search to identify each tag. By doing so, a considerable computational cost will be imposed on the whole system.

In 2007, Batina *et al.* [55] proposed an ECC-based RFID identification scheme based on Okamoto's authentication algorithm. Although they claimed that their scheme was resisant against active attacks, Lee *et al.* [56] asserted in 2008 that this scheme suffers from tracking as well as a forward secrecy problem. In 2010, Lee *et al.* [54], proposed an ECC-based RFID authentication scheme in order to address the existing tracking problems [53, 55]. Nevertheless, in the mentioned schemes, the authors merely considered tag to reader identification, excluding the reader to tag authentication [26]. This causes tags to reply to any malicious query being sent by an adversary. The major reason is that tags are not capable of confirming to whom they are talking to. In 2011, Zhang *et al.* [57] proposed an ECC-based randomized key scheme in order to improve the schemes by Tuyls *et al.* and Lee *et al.* Although their scheme is secure against relevant attacks concerning the RFID systems, it still not capable of performing mutual authentication. In 2013, Liao *et al.* [26] proposed a secure ECC-based authentication scheme integrated with the ID-verifier transfer protocol. Similar to Zhang *et al.*'s work, Lial *et al.*'s scheme achieved the required security level of RFID systems. However, their tag identification scheme lacked performance efficiency in terms of the tag's computation time and its memory requirement.

2. Centralized Authentication and Authorization Approaches: Symmetric key-based authentication and authorization approaches are considered suitable and efficient solutions for constrained networks. However, a common issue hereby is the scalability of these approaches. A constrained node must be pre-configured with shared keys of all entities before deployment. To counter this scalability issue, several approaches have been introduced. A centralized server or a certificate authority serves as the key distributor and constrained nodes are pre-configured with a shared key for secure communication. This requires trusting the server or the certificate authority, which is applicable for small domains. In the intra-domain communication however, it is challenging to establish trust between the servers of different domains. This requires further non-trivial infrastructure, for example, by means of Public Key Infrastructure (PKI), between the servers. Perrig *et al.* presented SPINS [58], a centralized architecture for securing unicast and multicast communication in constrained networks. SPINS is comprised of two security protocols, the Micro Timed Efficient Stream Loss-tolerant Authentication (μTESLA) and the Secure Network Encryption Protocol (SNEP). The μTESLA provides authenticated broadcast for constrained environments, whereas SNEP provides data confidentiality and with integrity of the unicast communication. In the bootstrapping phase, each constrained device acquires a master secret from the domain manager that could be the sink node or the Gateway (GW). Encryption keys between peers are derived from this master secret using the Pseudorandom Function (PRF). The μTESLA relies on the concept of delayed key disclosure, where the key is employed to authenticate the message m_i along with the message m_i+1. The receiver can verify the accuracy of each key by performing a hash function. The μTESLA needs time-synchronization in the constrained network because keys are bound to time. Garcia-Morchon *et. al.* [59] presented a polynomial-based approach as an alternative to public key-based primitives in DTLS to provide secure authentication and authorization in the IoT.

Polynomial-based schemes aim at simplifying the key agreement process in sensor networks. The principal idea in the polynomial scheme is to allocate every node n a polynomial share $F(n, y)$ derived from a secret symmetric bi-variate polynomial $F(x, y)$. This enables any possible pair of nodes with a polynomial share to establish a common secret [60]. The procedure of using polynomial schemes in the DTLS handshake is presented in the following. While assuming every sensor node is pre-configured with a Pre-shared Key (PSK), the sensor nodes authenticate themselves to the domain manager upon joining a network. During this phase, sensor nodes retrieve their polynomial share from the bi-variate polynomial. Afterward, any two nodes N_1 and N_2 can perform an extended version of the DTLS handshake in the PSK mode, during which they exchange their identifiers ID_1 and ID_2 in the $ClientHello$ and $ServerHello$ messages. This approach offers an alternative to PKC-based modes in DTLS. In this approach, the domain manager is a central entity that distributes polynomial shares in a domain. To allow secure communication across two domains, supporting inter-domain communication needs non-trivial coordination among two administrative domains. In contrast, we focus on enabling public key-based authentication and authorization for the healthcare IoT systems which does not need a central entity for the authentication and authorization process and instead, relies on public keys.

3. Delegation-based Authentication and Authorization Approaches: Delegation-based authentication and authorization approaches introduce solutions to delegate computationally expensive tasks, such as public key-based operations involved in session establishments, to more powerful devices. One such delegation-based approach is the Server-based Certificate Validation Protocol (SCVP) [61]. SCVP enables a client to delegate the complex task of certificate path construction or certificate validation to a trusted server. By offloading certificate validation, clients do not need to perform specific tasks for certificate validation and can consequently have a simplified logic. Nevertheless, this requires that the SCVP server be as much trusted as the reliable local software. In the case of untrusted SCVP servers, the client can delegate less critical tasks, for instance, fetching revocation information. SCVP needs integrity protection of the queries and responses through a digital signature or MAC. The key utilized to generate the MAC is derived from a key agreement protocol, such as Diffie-Hellman (DH). This means that clients are still required to perform expensive public key-based operations. In addition, this approach increases the per-handshake communication overhead within constrained networks, specifically considering the length of certificates which causes the highest transmission overhead during a handshake.

Another delegation approach with regards to the IoT is presented by Bonetto *et. al.* [62]. The authors proposed an approach to delegate the public key-based operations to a more powerful device, such as the GW. They explain the process for the Internet Key Exchange (IKE) session establishment, where the GW intercepts session establishment and pretends to be the end-point. After the calculation of the session key, this key is handed over to the constrained sensor node. Afterward, both peers can directly communicate and protect their communication using the session key. This approach necessitates a strong trust in the GW. Then, the GW, as an on-path entity in possession of the session key, has access to the communication in plaintext. Hence, GW can modify messages unnoticed. This, however, breaks the end-to-end security. An alternative delegation-based architecture is Tiny 3 Transport Layer Security (TLS) that requires a strong trust level between the GW and the constrained device [63]. Tiny 3-TLS offloads expensive public key-based operations to the GW. The constrained device trusts the GW and the non-constrained device authenticates itself to the GW and hence, the GW trusts the non-constrained device.

As a result, Tiny 3-TLS assumes that by using a transitive trust, the constrained device could trust the non-constrained device. Tiny 3-TLS distinguishes between fully and partially trusted GWs. In the fully trusted scenario, the non-constrained client performs a server-side certificate-based authentication and authorization with the GW. After a successful handshake, the GW conveys the session keys to the constrained device. The partially trusted GW performs all PKI-based tasks, except the key agreement. For the key agreement task, the constrained device offers its Elliptic Curve Diffie Hellman (ECDH) public key to the GW. Hence, both end-points derive a shared key that remains unknown to the GW. Similar to the previous approach, in Tiny 3-TLS, a strong trust-level needs to exist between the constrained device and the GW. This is because a malicious GW can launch a Man-In-the-Middle (MITM) attack by replacing the ECDH public keys.

Sizzle [64] implements an SSL-secured HTTP web server for constrained devices with support for ECC-based authentication and authorization. Compared to the previous delegation-based architectures, this approach delegates only the task of adapting the underlying transport layer protocol. This is performed by terminating the incoming TCP connection at the GW and sending the payload through a UDP-based reliable protocol to the constrained device. Sizzle only performs certificate-based authentication and authorization towards non-resource constrained clients and does not perform certificate handling for constrained devices. While the authors give remarkable insights into certificate transmission in constrained networks, they do not consider the impact of the DH key agreement and the certificate verification in constrained networks. In addition, with DTLS a UPD-based variant of SSL-TLS has been introduced, therefore, the need for a UDP-TCP proxy has become obsolete [65]. Hummen *et al.* [33] presented an implementation of a delegation architecture based on an off-path delegation server. Their proposed delegation-based architecture relied on a centralized delegation server. However, their proposed architecture lacks scalability and reliability. More precisely, their architecture cannot be extended to be employed for multi-domain infrastructures, such as large in-home or hospital domains. Also, their proposed architecture suffers from a considerable network transmission overhead resulting in a long transmission latency. Moreover, if an adversary performs a DoS attack or compromises the delegation server, a large quantity of stored security context of a constrained domain can be retrieved. More precisely, in multi-domain networks, a DoS attack can disrupt all the available constrained medical domains as the functionality of the IoT-based healthcare still depends on the centralized delegation server.

4. Hardware-based Authentication and Authorization Approaches: A class of security solutions relies on hardware security modules, such as Trusted Platform Module (TPM). A TPM is tamper-proof hardware that offers support for cryptographic computations, more specifically for public key-based cryptographic primitives. TPM have the possibility to hold private keys, such as Rivest–Shamir–Adleman (RSA) private keys in a protected memory area. Moreover, the cryptographic accelerator of TPMs can compute the cryptographic computations with higher performance. TPMs are finding their ways into commodity hardware, including desktops and notebooks. This allows for a better performing disk encryption, remote attestation of various software modules, and key protection [66]. Hence, researchers in the area of WSNs have currently studying the feasibility and applicability of TPMs on constrained devices [67]. Kothmayr *et al.* [68] presented a TPM-enabled architecture with support for RSA-based cipher suites of DTLS. They implemented their approach in Tiny Operation System (OS) with a memory footprint of approximately 63 kbyte of ROM and

18 kbyte of RAM. The evaluation of the mutual DTLS handshake with 2048-bit RSA keys and the cipher suit $TLS\_RSA\_with\_AES\_128\_CBC\_SHA$ provides suitable handshake times of a few seconds. The use of this special purpose hardware may be reasonable in some sensitive application scenarios. Nevertheless, the IoT vision comprises of highly resource-constrained devices, where specific purpose hardware modules including the TPM, are neither feasible nor economical. In addition, RSA keys and RSA-based certificates impose a high transmission overhead. This is crucial in resource-constrained environments due to expensive radio communication and lossy links with respects to energy consumption, while ECC offers a similar security level with considerably smaller footprint. Thus, ECC is recommended and preferred for constrained environments. One of the main purposes of this thesis is to allow highly resource-constrained IoT devices that have no special purpose hardware, to participate in secure end-to-end communication.

2.4.3 Cryptographic Keys and Constrained Health IoT Devices

One of the main objectives of secure communication in the healthcare IoT system is to generate robust cryptographic keys for medical sensors. This enables medical sensors to encrypt and decrypt messages that need to be conveyed between the sensors and health caregivers. This section is organized as follows. First, an overview of biometric-based cryptographic keys in healthcare IoT systems is presented. Then, we present the most well-known approaches proposed regarding the generation of cryptographic keys for constrained IoT devices.

Biometrics are generally regarded as the only solution that is lightweight, requires low resources, and indeed can identify authorized subjects in BANs [16, 17, 18, 19]. Key generation techniques relying on humans' biometric systems are best suited for resource-constrained medical sensors as those solutions are lightweight and require low resources [19], and medical sensors rely on cryptography to secure their communications [17]. The proper application of cryptography requires the use of secure keys and key generation methods. Key generation approaches that are proposed for generic wireless sensors are not directly applicable to tiny sensors used in BANs as they are highly resource-constrained and demand a higher security level [69]. Key generation in sensor networks generally requires some form of pre-deployment. Nevertheless, given the constrained nature of medical sensors used in BSNs, conventional key generation approaches may potentially involve reasonable computations as well as latency during network or any subsequent adjustments, due to their need for pre-deployment.

In [70, 71, 72, 73, 74], fuzzy vault-based bio-cryptographic key generation protocols are proposed for BANs. In each of these protocols, frequency domain characteristics of PPG and ECG signals are used as the physiological parameters. Bao *et al.* [75] presented an entity authentication protocol and a fuzzy commitment-based key distribution protocol, in which the IPI values generated from the Photoplethysmogram (PPG) signals are employed as the physiological parameters. In their work, adaptive segmentation was used to divide the value range of the IPI into segments. The main drawback of the above-mentioned approaches is that they are not applicable enough to be used for generating cryptographic keys for medical sensors. This is due to the required heavy-weight computations. Poon *et al.* [17] and Zhang *et al.* [18] further evaluated the performance of Bao *et al.*'s [75] approach using both PPG and ECG signals with respect to their error rates. In another study by Bao *et al.* [76], seperate solution is proposed for which physiological parameter generation is utilized in a bio-cryptographic security protocol. The authors claimed that the physiological parameters which are generated utilizing the individual and multi-level IPI sequences have comparable distinctiveness and randomness. Nevertheless, the latency of these approaches is very high as 256 IPIs are required in order to generate a 64-bit cryptographic key. In a cryptographic security infrastructure designed for BANs, for the cryptographic keys to be generated from the captured bio-signals in real-time, the delay of the key generation process should be kept as minimum as possible. Altop *et al.* [69] and Xu *at al.* [77] proposed key generation approaches in which the IPI values generated from ECG signals are utilized.

In both of these works, the authors employed Gray encoding to map each IPI value to a 4-bit binary number using a uniform quantization method. According to the authors, the generated physiological parameters pass the randomness measurement tests presented by the NIST test benchmark [78]. They also stated that the generated physiological parameters pass both temporal variance and distinctiveness tests. However, in [69] and [77], no related numerical information for experimental performance evaluation in terms of key generation execution time is provided. In addition, compared to the approach in this study, these works have failed to provide as high a security level in terms of distinctiveness, the test of randomness, and temporal variance. Zhang *et al.* [18], Poon *et al.* [17] and Bao *et al.* [76] evaluated the performance of the physiological parameter generation, utilizing both PPG and ECG signals. The authors developed physiological parameter generation techniques that can be utilized in bio-cryptographic key generation approaches. In their work, these authors claimed that physiological parameters generated utilizing IPI sequences offer promising features to be exploited for cryptographic key generation approaches.

Zheng *et al.* [79] proposed a time-domain physiological parameter generation method. They used the time distances between the R peaks as the ”Reference Points” and other peak values of an ECG signal from one heartbeat cycle. The authors claimed that their solution was faster than the conventional IPI-based methods and it ensures the property of randomness. However, their proposed approach lacks reliability as it was only applicable to ECG records collected from subjects with normal ECG rhythm or subjects with no severe cardiovascular diseases. In healthcare systems, subjects often suffer from Cardiovascular Diseases (CVDs) such as Cardiac Arrhythmia, Poor R-wave Progression, Myocardial infarction and Anterior Wall MI in which the R peaks are not easily detectable, or might be even missing within one heartbeat cycle. Choosing the R peak as the reference for calculation of all the other features is not always reliable enough to be used for the binary sequence generation. In addition, as the main focus of the approach present in [79] is on rapid key generation, distinctiveness and temporal variance properties were not analyzed and reported in their approach. In this context, we claim that a robust ECG-based cryptographic key generation approach needs to cover both healthy and unhealthy human subjects. This necessitates ECG features selection to becoming independent of any reference point.

2.4.4 End-to-End Communication of Healthcare IoT Systems

Over the past few years, researchers have conducted several studies toward designing secure and efficient end-to-end communication for IoT systems. However, many of the existing studies proposing the secure end-to-end communication system are still based on centralized architecture and do not provide comprehensive end-to-end security. Instead, their solutions are considered semi end-to-end security. In this section, we first provide a broad overview of secure end-to-end communication in IoT systems. We then discuss the well-known approaches proposed for end-to-end security and the challenges associated with each of them. Secure end-to-end communication between constrained devices and Internet hosts with the goal of providing confidentiality, integrity, and authenticity is an important requirement of a secure IoT. Existing end-to-end communication approaches are focused on PSKs on both ends, ,that is, client and server. In addition, certificate-based approaches is generally considered infeasible for constrained IoT devices. DTLS is the demanded and de facto favorable security solution to perform secure end-to-end communication [80]. To this end, this thesis focuses on DTLS as the main transport layer security to provide secure end-to-end communication.

Implementation is needed to quantify overheads and the required resources for end-to-end communication approaches using DTLS. This implementation must be as lightweight as possible, to fit the available resources of constrained IoT devices. When developing such an implementation, overheads can be detected and efficient solutions to reduce them can be designed. As described in the previous section, highly constrained devices cannot provide enough resources to deploy expensive public key-based operations; hence they require a delegation architecture. A delegation-based architecture allows constrained IoT devices that cannot cope with expensive public key-based operations to efficiently perform secure end-to-end communication. This allows one to take advantage of public key-based operations, such as key agreement without prior knowledge as well as key revocation. More importantly, authentication and authorization of IoT components based on certificates can be performed in such a way that the heavy public key-based operations are delegated to a more powerful off-path entity that fulfills the minimum required level of trust. CodeBlue is one of the most popular healthcare research projects developed at the Harvard sensor network Lab [81]. In this approach, several medical sensors are placed on a patient's body. The authors of CodeBlue admit the necessity of end-to-end security for IoT-based medical applications. However, the security aspects of CodeBlue are still left as the future work.

Lorincz *et al.* [82] suggest that elliptic curve cryptography [27] and TinySec [83] are efficient solutions to be used for key generation and symmetric encryption in the CodeBlue project, respectively. Kambourakis *et al.* discuss some attack models and security threats concerning the CodeBlue project: denial-of-service attack, snooping attack, grey-hole attack, Sybil attack, and masquerading attacks [84]. Johns Hopkins University developed an in-hospital patient monitoring system called MEDiSN [85]. It consists of multiple physiological motes that are battery powered and equipped with medical sensors in order to collect patients' medical and physiological health information. The MEDiSN architecture focuses on reliable communication, routing, data rate, and Quality of Service (QoS) [85]. In their proposed architecture, the authors of MEDiSN acknowledged the necessity of having encryption for the physiological monitors. However, they did not mention which cryptosystems have been used for data confidentiality and integrity. Although the authors claim that security is provided by the MEDiSN architecture, their study did not reveal much information regarding security implementation.

An architecture called Sensor Network for Assessment of Patients (SNAP) [13] has been proposed to address the security challenges concerning the wireless health monitoring systems. However, the main problem of the aforementioned architecture is that it does not authenticate users when providing medical data. Furthermore, the data collected from medical sensors are conveyed to a controller in a plaintext format. Hence, the medical data of the patients can be modified or intercepted by a malicious user. In [86], the researchers proposed a lightweight identity-based cryptography solution called IBE-Lite. The basic idea of IBE-Lite is to balance security and privacy with availability. Nevertheless, security and privacy issues, as well as efficiency problems, are recognized in IBE-Lite. First, in their work, Tan *et al.* do not consider sensor to the base station and end-user data authentication. Therefore, falsified medical information can be introduced or treated as authentic due to the lack of authentication schemes. Second, IBE-Lite cannot resist replication attacks. Consequently, an adversary can insert malicious medical sensors into the network.

To establish interoperable network security between end-peers from independent network domains, researchers have recently proposed variants of conventional end-to-end security protocols, among which DTLS is one of the most relevant protocols [80]. In this regard, Hummen *et al.* [33] presented an implementation of a delegation architecture based on an off-path delegation server. Their proposed delegation-based architecture relies on a centralized delegation server. Due to this, their proposed architecture lacks scalability and reliability. More precisely, their architecture cannot be extended to be employed for multi-domain infrastructures, such as large in-home or hospital domains. Also, their proposed architecture suffers from a considerable network transmission overhead resulting in a long transmission latency. Moreover, if an adversary performs a DoS attack or compromises the delegation server, a large quantity of the stored security context of a constrained domain can be retrieved.

Hummen *et al.* [33], Granjal *et al.* [87], and Kang *et al.* [88] presented the state-of-the-art end-to-end security approaches proposed for IoT. However, we distinguish the following major advantages offered by our scheme compared to their approaches. We believe that the approaches presented by Granjal *et al.* [87] and Kang *et al.* [88] do not provide comprehensive end-to-end security. Rather, they can be considered *semi end-to-end* security. The main reason is that in these works, the 6LoWPAN Border Router (6LBR) acts as an intermediary node located between the sensor and the end-user. Every time these two end-points try to communicate with each other, all the secret information related to the communication needs to pass through the 6LBR. However, the smart gateway utilized in our work is only used during the initialization phase and then, both end-points directly communicate with each other through a channel secured by the DTLS session resumption. Therefore, *end-to-end* security is guaranteed in our work.

2.4.5 Healthcare IoT Mobility Management

Mobility support is one of the most important issues in healthcare IoT systems. In such systems, improving patients' quality of life is essential.It is essential to provide patients with the possibility of walking around the hospital wards with the knowledge that the monitoring of their health condition is not interrupted. Researchers have completed several studies over the past few years to design efficient mobility management approaches. In this section, we first give a broad overview of mobility management in healthcare IoT systems. Then, we present the most important related works on for mobility management. Using a portable patient monitoring system offers a high quality of medical service by providing patients with a freedom of movement. Mobility enables patients to go for a walk around the medical domains while they are monitored. In addition, mobility allows the patients to move from their base MSN to other rooms for medical tests without losing the continuous monitoring. This scenario can also be extended to other environments, such as a nursing house or in-home patient monitoring. The main goal of the continuous monitoring in the healthcare IoT systems is to achieve a knowledge base from the patient and this enables the remote server and the Knowledge Base System (KBS) to detect symptoms, predict, and manage the illnesses.

Mobility can be categorized into two main topics denoted as macro-mobility and micro-mobility. The movement of medical sensors between various medical network domains distinguishes the macro-mobility. Micro-mobility assumes that medical sensors move between different MSNs within the same domain. To achieve a continuous monitoring of patients considering the mobility support, it is essential to develop self-configuration or handover mechanisms that are capable of handling secure and efficient data transfers among different MSNs. A data handover mechanism is defined as the process of changing or updating the registration of a mobile sensor from its associated base MSN to the visited MSN, for example, when moving across the hospital's wards. Data handover solutions should enable ubiquity when they need to work autonomously without human intervention. The handover mechanism should also offer medical sensors continuous connectivity if several gateways existin the hospital or nursing environments.

Valenzuela *et al.* proposed a solution to support mobility for in-home health monitoring systems using wearable sensors [89]. This approach utilizes a coordinator sensor attached to the patients' bodies that is responsible for all communications between wearable sensors and network Access Points (APs). Jara *et al.* proposed a solution to support the mobility of sensors employed to monitor patients in hospital environments [90, 91, 92]. This approach supports micro-mobility exploiting elements such as sink nodes and gateways in their proposed architecture. This proposal supposes that each mobile node has a base network and can move into other networks. Fotouhi *et al.* [93] presented a handover approach for mobility support in WSN that can be easily employed for BSN [94, 95]. In their work, different parameters are utilized to specify the time for handover, but the most important ones are the Received Signal Strength (RSS) and the sensor velocity. If the RSS connection with the current AP is under the pre-defined threshold, the handover mechanism begins. To acknowledge the received signal strength between the sensor and the access point, the sensor periodically sends probe queries. To verify the quality of the link, as well as to decide on the handover mechanism, this solution requires a continuous exchange of probe or acknowledge messages between the sensor and the corresponding access point. However, this continuous message exchange weakens the network in terms of transmission overhead, memory, and energy consumption.

Chapter 3

Contributions of the Thesis

In healthcare IoT systems, improving patients' quality of life is important to mitigate the negative effects of being hospitalized. It is crucial to provide patients with the possibility of walking around the medical environments with the knowledge that the monitoring of their health condition is not interrupted [4, 5, 6, 7, 8]. Patients do not need to be worried about moving around, as the system can enable mobility while continuously monitoring their vital signs. In IoT-based healthcare applications, security and privacy are among major areas of concern, as most devices and their communications are wireless in nature [9, 10, 11, 12, 13]. An IP-enabled sensor in a healthcare IoT, can transmit patients' medical data to remote healthcare service. However, in such scenarios, the conveyed medical data may be routed through an untrusted network infrastructure, which is the Internet. Misuse or privacy concerns may restrict people utilizing IoT-based healthcare applications. In this regard, the authentication and authorization of healthcare IoT components, robust cryptographic key generation, and secure end-to-end communication are critical requirements as eavesdropping on sensitive medical data or malicious triggering of specific tasks can be prevented [33]. Medical sensor nodes rely on cryptographic keys to secure their communications.

Due to the constrained nature of these sensors, establishing or maintaining the security of exchanged medical data is not a trivial task. There are significant cryptographic key generation solutions for generic wireless sensors that are not directly applicable to medical sensors. This is because medical sensors are highly resource-constrained and demand a higher security level. Key generation solutions relying on humans' biometric systems are best suited for tiny medical sensors as those solutions are lightweight and require a low resource [19]. By developing a robust and efficient key generation using biometric systems, the security of medical sensors can be offered in a plug-n-play manner where neither a network establishment nor a key pre-distribution mechanism is required. In this thesis, we investigate the challenge of designing, implementing, and evaluating a scalable architecture for secure end-to-end communication in healthcare IoT systems. We did this to identify the advantages and shortcomings of the designed architecture and to find application domains in which this architecture can be properly utilized. For the presented healthcare IoT architecture, we propose a novel secure and efficient authentication and authorization approach, as well as a session resumption-based end-to-end communication scheme [21, 22]. Our proposed architecture exploits the smart gateways' advantageous property of being non-resource constrained for outsourcing the heavy-weight processing burdens from tiny medical sensors. In [21], the main focus was on the analysis and development of authentication and authorization between peers rather than end-to-end security. In [22], we proposed a session resumption-based end-to-end security scheme for healthcare IoT systems to securely and efficiently manage the communication between medical sensors and remote healthcare centers/caregivers. To provide end-to-end security, the session resumption technique without a server-side state is utilized. To improve the mobility of the proposed architecture, we carried out a further study in which we developed an end-to-end security scheme for mobility enabled healthcare IoT [96].

We present two different ECG-based cryptographic key generation approaches for which the IPI feature of ECG underlays both of the proposed approaches. We also propose a new approach, called Several ECG Feature (SEF) based cryptographic key generation. The SEF approach alleviates the key generation execution overhead of the existing and our previous approaches [96], while preserving the achieved high-security levels. We applied the proposed approach to both normal and abnormal ECG signals. The generated keys are employed in end-to-end communications to securely encrypt/decrypt patients' medical data transmitted between medical sensors and health caregivers. Also, we used the keys in mutual authentication and authorization of peers in our healthcare IoT architecture. Finally, we extended our previous works by analyzing the performance of the state-of-the-art security solutions including the holistic integration of our recent works [20, 22, 96, 97, 98] in terms of energy-performance on a prototype of a healthcare IoT system through the simulation and hardware/software prototype. We present the contribution of this thesis in detail in the original publications in Part II of the thesis. This chapter presents a summary of the main contributions while also providing a brief overview of some of the most important challenges that they addressed.

3.1 Pervasive Health Monitoring Based on IoT

Our first contribution in this thesis is to discuss the implementation of two architectures for remote monitoring of biomedical signals. We present wireless systems for remote monitoring of biomedical signals to alleviate issues in traditional health monitoring systems and to improve the quality of medical care. Medical applications have a certain nature and requirements that usually have life or death consequences when data are not successfully transferred. However, requirements and concerns are mostly financial in other applications. The IEEE 1073 group defined these requirements, such as data rate and delay. In the case of a 3-lead ECG system, a patient node generates 2.4 kbps of data. In the implementations, the sensors used to collect medical data include Blood Pressure, Heart Rate, Temperature, Respiration, Glucose, SpO2, and ECG. We implemented two variants of the wireless health monitoring architectures to remotely monitor patients: (1) The first architecture is a wireless sensor network based on a low power ZigBee that consists of a set of sensor nodes to read data from various medical sensors, process them, and send them wirelessly over ZigBee to a server node. (2) The other architecture implements an IP-based wireless sensor network using IEEE 802.11 WLAN.

1. **ZigBee-Based Architecture:** In the implementation, ZigBee is based on a low-rate IEEE 802.15.4 standard, designed for supporting low-power, low-cost, and low-data rate applications. The ZigBee-based architecture consists of several patient nodes and a sink node. The system is implemented with ZigduinoR2 [11] hardware platform, which is an Arduino compatible microcontroller platform. The Contiki operating system is used to implement WSN. The ZigBee-based architecture is divided into four sections; sensor interface, WSN implementation, database application, and webserver application. (1) *Sensor interface:* The sensor interface is implemented using an Arduino-compatible E-health shield on top of the Zigduino hardware. The E-health shield is a gateway between the medical sensors and the Zigduino board. The Zigduino collects data measured from various sensors via the E-health shield. (2) *WSN implementation:* The Zigduino's microcontroller contains an on-chip 2.4 GHz IEEE 802.15.4 radio. The implemented WSN consists of several patient nodes and a sink node. Patient nodes collect data from various sensors and send them wirelessly over ZigBee to the sink node. (3) *Database application:* The sink node is connected to a local PC (Personal computer) where a Python code is executed to collect data from the serial terminal and save it into a remote database. (4) *Webserver Application:* Web-server application written with

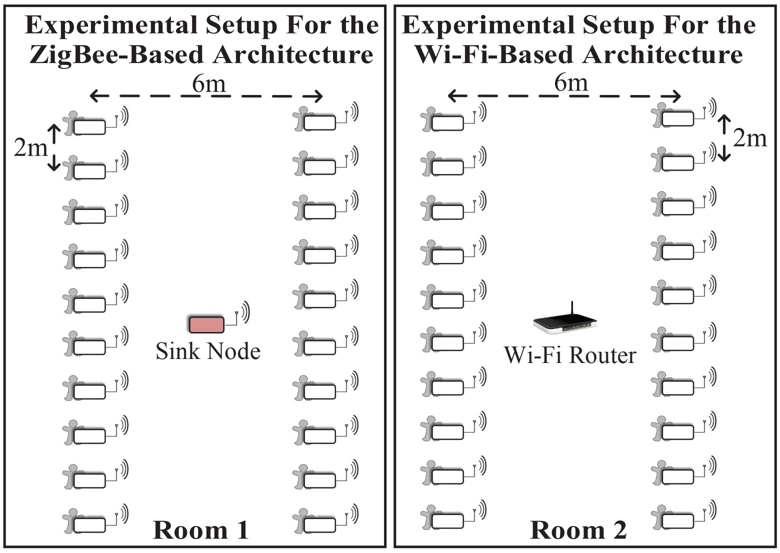

Experimental Setup For the ZigBee-Based Architecture
6m
2m
Sink Node
Room 1
Experimental Setup For the Wi-Fi-Based Architecture
6m
2m
Wi-Fi Router
Room 2

Figure 3.1: Experimental setup to compare the architectures [99]

a Hypertext Preprocessor (PHP) that accesses the database and updates the web page in real time. The data from the webpage can be accessed remotely by the patient's caregivers through their laptops or smartphones using any browser.

2. **IEEE 802.11 WLAN-Based Architecture:** The IEEE 802.11 WLAN based architecture consists of IEEE 802.11 WLAN enabled sensor nodes to access patients' medical data and IEEE 802.11 WLAN access point. The sensor nodes are designed using an Analog Front-End (AFE) and IEEE 802.11 WLAN module (RTX4140). The RTX module is provided with a proprietary operating system. The architecture is divided into four sections; sensor interface, WSN implementation, database application, and webserver application. (1) *Sensor interface:* The sensor interface is implemented using the AFE to read data from the medical sensors and to perform analog to digital conversion. The digital data from the output of AFE are read by RTX4140 through SPI. (2) *WSN implementation:* A UDP client application running on the RTX4140 sends the UDP data packet to a remote server through IEEE 802.11 WLAN once the connection to the IEEE 802.11 WLAN access point is established. (3) *Database application:* A UDP server application (running on a remote system), written in python, continuously listens to the UDP port, collects the incoming data and updates a remote database. (4) *Webserver application:* Webserver application is the same as that of the ZigBee-based architecture.

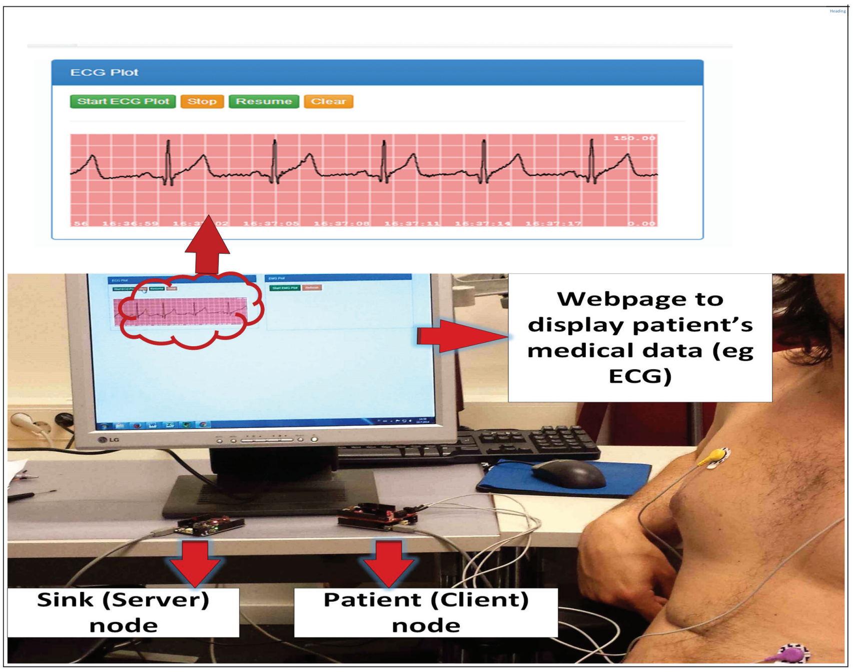


Figure 3.2: Implementation of WSN [99]

Figure 3.1 shows the experimental setup to compare both architectures. The scenario consists of a hospital room with twenty patient nodes reading patients' medical data from various sensors. There is one sink node to collect data from all the patient nodes in their respective setup. The distance between the adjacent patient nodes in the same column is two meters, and the distance between the adjacent patient nodes in the different columns is six meters. Every patient node transmits about 8.7 kilobits of data per second. Results show that the power consumption in the ZigBee based network is almost six to seven times less (seven times for 802.11g and six times for 802.11b/n) when compared with the IEEE 802.11 WLAN based network for the same experimental setup. The IEEE 802.11 WLAN based network consumes more power than ZigBee for a lower data-rate. Nevertheless, with an increase in data rate, power consumption in ZigBee increases rapidly when compared to IEEE 802.11 WLAN. In practice, the maximum data-rate achieved for transmitting sensor data with ZigBee using Contiki OS is 160 kbps, when the nodes are placed at a distance of around 10 meters. In the case of a star topology, the network can support up to 18 nodes. However, in the case of a mesh topology using multi-hopping, each node can route data of up to 17 other nodes apart from transmitting the data acquired, thus increasing the scalability to a higher number.

3.2 Authentication Scheme for RFID Implant Systems

This section presents an ECC-based mutual authentication scheme that satisfies the security requirements in an RFID implant system. The proposed scheme consists of three phases: (1) the reader authentication and verification phase, (2) the tag identification phase, and (3) the tag verification phase. In the proposed scheme, we suppose that the communication between the reader and the back-end database server is done through a secure channel, while communication between the RFID implant tag and the reader is not secure. Our scheme will provide a secure channel between the tag and the reader in such a way that they can communicate with each other securely and efficiently. Before describing the three mentioned phases, we first introduce parameters and notations used in our proposed scheme.

- G: a group of order q on an elliptic curve having the order n,
- P: a primitive element or the base point of G,
- s_1, s_2: each tag keeps two secret points s_1, $s_2 \in \mathrm{E}(F_g)$, which will change over time. These secret points will vary each time the tag is successfully identified, item ID_t: the tag's identification number or ID,
- s_3: each reader keeps a secret point $s_3 \in Z_n$, which will change over time. This secret point will vary each time the reader is successfully authenticated,
- $ID_r = s_3.P$: the reader's public key,
- r_s, i_1, i_2: random numbers in Z_n,
- h: a lightweight hash function,
- (d, c): a signature generated by the tag in its identification phase.

1. **Reader Authentication and Verification (Phase 1):** The reader authentication and verification phase of our proposed scheme relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP) [27]. In this phase, the reader chooses a random number $r_1 \in Z_n$ and computes $R_1 = r_1.P$ as its public key. Next, it initializes its counter value i_1 to one and sends both R_1 and i_1 to the tag. It then increments the value i_1 by r_1. Upon receiving the message, the tag checks whether i_2 (which is initialized to zero) is greater than i_1. If the condition holds, it replaces i_2 by i_1 and selects a random number $r_2 \in Z_n$.

Then, the tag computes $r_3 = X(r_2.P) * Y(R_1)$ where * is a non-algebraic operation over the abscissa of $(r_2.P)$ and the ordinate of R_1 and it sends the value r_3 to the reader. After receiving r_3, the reader computes $R_2 = r_1.ID_t + r_3.s_3$ and sends the value R_2 to the tag. Finally, the tag checks whether $(R_2 - r_1.ID_t)r_3^{-1}.P = ID_r$ holds. Then, the tag verifies that the reader is authentic.

2. **Tag Identification (Phase 2):** In the tag identification phase of the proposed scheme, the tag's initial secret point is $s_1 \in E(F_g)$ from which the next secret point s_2 and ID_t will be computed. To generate the second secret point, the tag computes $s_2 = f(X(s_1)).P$. For the sake of efficiency, the function f should be selected in a manner that avoids large Hamming weights for s_2, assuring that the computation of $s_2.P$ will be fast without compromising security [100]. Once the generation of the second secret point s_2 is done, the tag selects a random integer $k \in Z_g$ and computes a curve point $(x, y) = k.G$. In order to send its digital signed message (d, c) to the reader, the tag computes $d = x \bmod n$. If $d = 0$, the tag starts to select another random number $k \in Z_g$ and computes the next curve point. The tag computes its $ID_t = Mb(X(s_1)) * Mb(X(s_2)).P$ where Mb will output some middle bits of the input values. The operand * is a non-algebraic operation $\in F_g$ done over the abscissa of the first and the second secret points. Then, the tag computes $c = k(hash(ID_t) + X(s_1).d)$. Here again, if the computed $c = 0$, the tag will start the algorithm by selecting another random integer k. Finally, the tag sends the computed values (d, c) and (ID_t) to the reader.

3. **Tag Verification (Phase 3):** In this phase, to verify the tag is authentic, the reader selects a random integer $r_s \in Z_n$ and it computes its public key $p_r = r_s.P$. For $j \in [1, n-1]$, the reader checks whether $d, c \in Z_n$. If the result is valid, the reader calculates $h = Hash(ID_t)$, where Hash is the same Quark lightweight hash function that is used in the previous phase to generate the tag's signature. Once the hash value of (ID_t) is computed, the reader selects the leftmost bit of h and denotes it as z. Then, the reader calculates the values w, u_1, u_2. Based on the calculated values, the reader computes the curve point $(x, y) = u_1.P + p_r$. Finally, the reader will accept the tag's signature as a valid one if the equation $r = x \bmod n$ holds.

To the best of our knowledge, the previously proposed elliptic curve-based authentication schemes, concerning RFID systems in general, cannot fully fulfill the essential security and performance requirements of RFID implant systems. Most of the earlier proposed solutions were not secure against the most relevant attacks of the RFID systems. Also, they were not capable

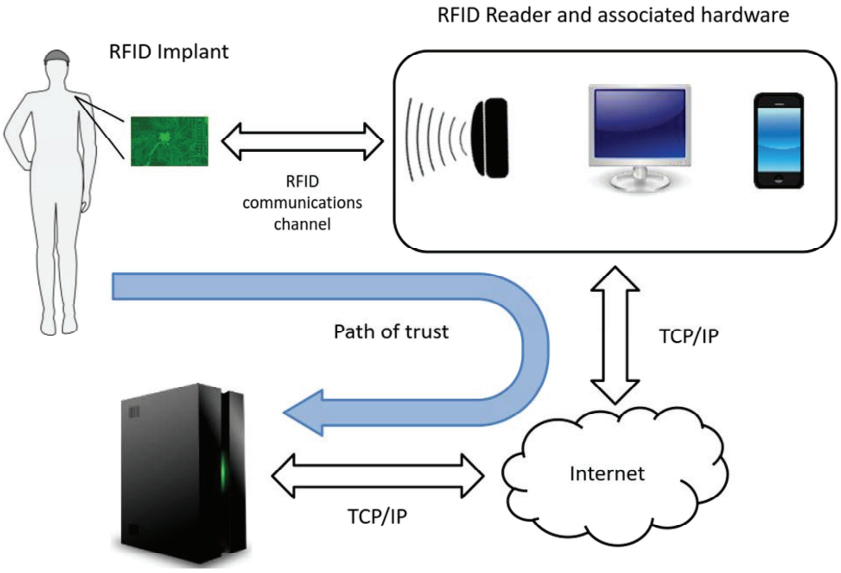

RFID Reader and associated hardware
RFID Implant
RFID communications channel
Path of trust
TCP/IP
Internet
TCP/IP

Figure 3.3: Communication between the RFID implant and the back-end database [101]

of performing mutual authentication between a tag and a reader. The proposed ECC-based mutual authentication scheme provides a secure channel between the tag and the reader in such a way that they can communicate with each other securely and efficiently. The proposed scheme relies on elliptic curve cryptography. An elliptic curve cryptosystem is more efficient in terms of key sizes and required computations than conventional public key cryptosystems.

We show that the scheme is secure against different types of relevant attacks in order to ensure a higher security level than the related work found in the literature. Also, we present that our scheme provides better efficiency in terms of computational cost, total memory required, and communication overhead. Based on the results presented, we prove that the proposed scheme has the appropriate features for use in RFID implant systems. We believe that the scheme is not just limited to RFID implant systems. It can also be applied to any application of IoT that requires secure and efficient authentication.

3.3 ECG Feature Based Cryptographic Key Generation

Our third contribution in this thesis is a low-latency approach for generating secure ECG feature based cryptographic keys. Most existing key generation

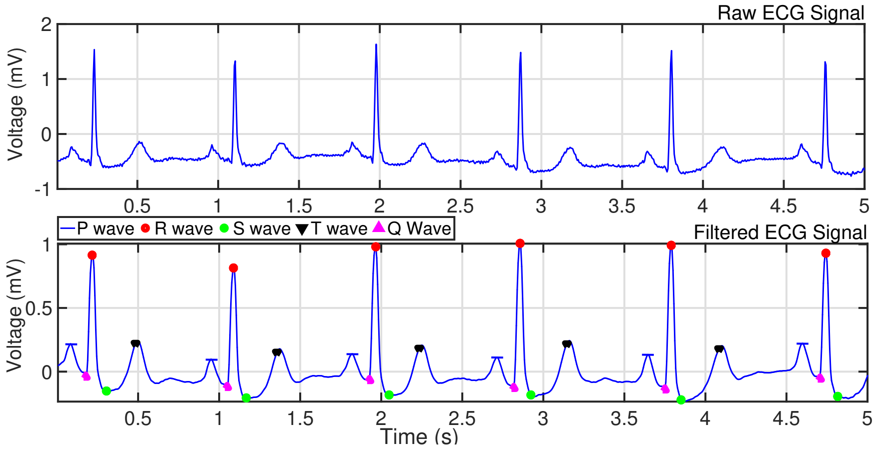


Figure 3.4: An ideal raw ECG signal and the filtered ECG signal with the main fiducial points indicated [20]

approaches are not directly applicable to BANs. Current ECG-based cryptographic keys are mostly generated using Inter Pulse Interval IPI feature of an ECG signal [18, 69, 77, 102, 103, 104, 105]. IPI is measured from two consecutive R peak points, where the R peaks are the tallest and most conspicuous peaks in an ECG signal. In [97], we demonstrated that existing IPI-based key generation approaches suffer from a low level of security in terms of distinctiveness, the test of randomness, and temporal variance. In the IPI-based approach, our main focus was to enhance the security of the generated cryptographic keys while realizing a clear trade-off between the security level and key generation execution time. To address this problem, we present a novel robust key generation approach employing several ECG feature, called Several ECG Feature (SEF). The SEF approach alleviates the key generation execution overhead of the existing and the previous approaches while preserving the achieved high security levels. The first step to generate ECG-based cryptographic keys is raw ECG data acquisition from subjects. The collected ECG data includes information about the heart rate, morphology, and rhythm being recorded by placing a set of electrodes on body surfaces such as neck, chest, legs, and arms. Once collected, raw ECG data need to be prepared for further analysis. Analysis of the ECG signal can be split into two principal steps by functionality: ECG signal *preprocessing* and *feature extraction*. The proposed approach is applied to both normal and abnormal ECG signals. The main contribution of this work is as follows:

1. **ECG Feature Selection:** The SEF approach uses four main reference-free [1] features of the ECG signal along with consecutive IPI

[1] In this context, reference-free property indicates a dynamic technique in which no

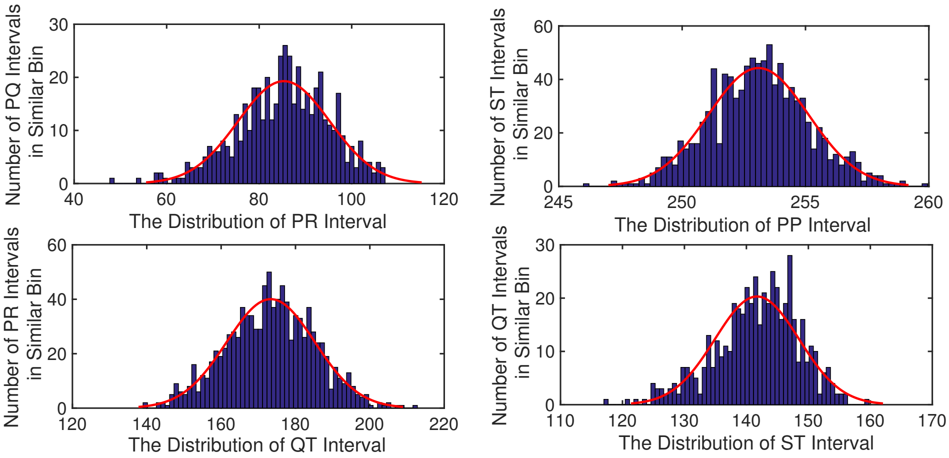


Figure 3.5: The normal distribution of PR, PP, QT, and ST intervals [20]

sequences to generate ECG-based cryptographic keys. The utilized main features include PR, RR, PP, QT, and ST intervals. This is based on the fact that these features are highly reliable and ensure the randomness property.

2. **Optimum Binary Sequence Generation:** A dynamic technique is used to specify the optimum number of bits that can be extracted from each main ECG feature. The used technique ensures the randomness property as the binary sequence is produced based on the real-time variation of the measured ECG signal [79]. The utilized technique to determine the number of optimum bits (M) can be defined as:

$$\mu(FX_i) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{3.1}$$

$$SD(FX_i) = \sigma(FX_i) = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2} \tag{3.2}$$

$$C_v = \frac{\sigma(FX_i)}{\mu(FX_i)} \tag{3.3}$$

$$M = \frac{\ln\left(\sigma(FX_i)\right)}{\ln(2)} + C_v \tag{3.4}$$

where FX_i represents a set of any one of the PR, PP, QT, and ST features from one sampled ECG dataset in the $i_t h$ heartbeat, x_i represents each value in the dataset, μ is the mean value of the dataset, σ is

ECG fiducial point is fixed as reference.

the summation, N is defined as the number of values in the dataset, σ indicates the standard deviation of a dataset, and C_v is the coefficient of variation which is defined as the ratio of the standard deviation to the mean value. As can be seen from Figure 3.5, similar to the RR interval, the distribution of PR, PP, QT, and ST intervals also fits into the normal distribution. Hence, these ECG features also fulfill the property of randomness.

3. **ECG-based Cryptographic Key Generation:** In the SEF key generation approach, depending on the length of the cryptographic key n that needs to be generated, approximately $\frac{n}{16}$ consecutive ECG heartbeat cycles need to be detected. From the detected heatbeats, all of the main ECG features from a t-second segment of a patient's ECG data need to be computed. To achieve this goal, the following tasks must be performed: (1) for a specified period of time t, the main fiducial points or peaks of a sensed ECG signal should be extracted utilizing a generic feature extraction function; (2) from the detected fiducial points, the required x consecutive ECG features should be computed; (3) from the computed main ECG features, the amount of optimum binary values per ECG feature must be calculated; and (4) the produced m_i-bit binary sequences from each ECG feature then need to be concatenated in order to form an n-bit binary sequence. The generated n-bit binary sequence is considered the main cryptographic key.

4. **Strengthening ECG Feature-based Key generation:** To reinforce and enhance the security level of the approach, we consolidate the SEF key generation approach with two different cryptographically secured pseudo- random number generators: (1) SEF-PRNG: we strengthened the security level of the SEF approach by exploiting the Fibonacci-LFSR pseudo-random number generator (2) SEF-AES: the SEF approach is also strengthened by utilizing the AES algorithm in counter mode. This technique exploits our SEF key generation approach as the seed generator for the AES algorithm.

The security evaluation of the generated keys was made in terms of distinctiveness, a test of randomness, temporal variance, and the NIST benchmark. The results show that the strengthened key generation approach offers a higher security level in comparison to existing approaches that rely only on singleton ECG features. The analyses also reveal that the normal ECG signals have slightly better randomness compared to the abnormal ones. Cryptographic keys that are generated from normal ECG signals using the SEF approach have an entropy of about 0.98 on average. Cryptographic keys that are produced using the strengthened SEF approach offer the en-

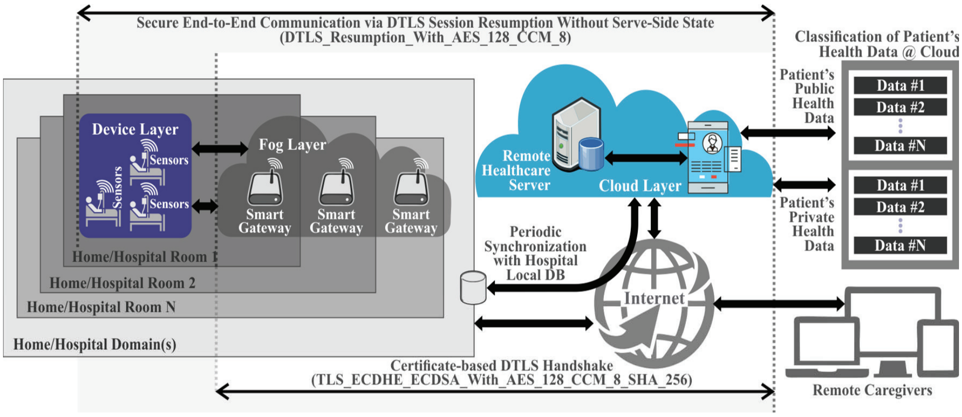

Secure End-to-End Communication via DTLS Session Resumption Without Serve-Side State
(DTLS_Resumption_With_AES_128_CCM_8)
Classification of Patient's Health Data @ Cloud
Patient's Public Health Data
Data #1
Data #2
Data #N
Patient's Private Health Data
Data #1
Data #2
Data #N
Device Layer
Sensors
Sensors
Sensors
Fog Layer
Smart Gateway
Smart Gateway
Smart Gateway
Remote Healthcare Server
Cloud Layer
Periodic Synchronization with Hospital Local DB
Internet
Home/Hospital Room 1
Home/Hospital Room 2
Home/Hospital Room N
Home/Hospital Domain(s)
Certificate-based DTLS Handshake
(TLS_ECDHE_ECDSA_With_AES_128_CCM_8_SHA_256)
Remote Caregivers

Figure 3.6: The architecture of a healthcare IoT system with secure end-to-end communication [96]

tropy of ~ 1. In addition, the reinforced key generation approach also has better P-value NIST pass rates compared to state-of-the-art approaches that rely only on singleton ECG features. We also found out that our approach is approximately faster than existing IPI-based key generation approaches. Future work includes investigating and analyzing other physiological signals within a BAN. The purpose is to realize how the generated cryptographic keys can also be used by other bio-sensors to provide intra-BAN communication security.

3.4 End-to-End Security for Healthcare IoT

The fourth contribution in this thesis is a novel secure and efficient end-to-end security scheme for mobility enabled healthcare IoT. In [21], we presented a secure and efficient authentication and authorization architecture for healthcare IoT system. The proposed architecture, called *SEA*, exploits the unique role of smart e-health gateways in the fog layer. SEA performs the authentication and authorization of remote end-users securely and efficiently on behalf of the medical sensors [21] (lower black arrow shown in Figure 3.6). The three-tier system architecture of the healthcare IoT system on which we apply the end-to-end security scheme is shown in Figure 3.7. The functionality of each layer in this architecture is as follows.

1. **Device Layer**: The lowest layer consists of several physical devices (including implantable or wearable medical sensors) that are integrated into a tiny wireless module to collect contextual and medical data.

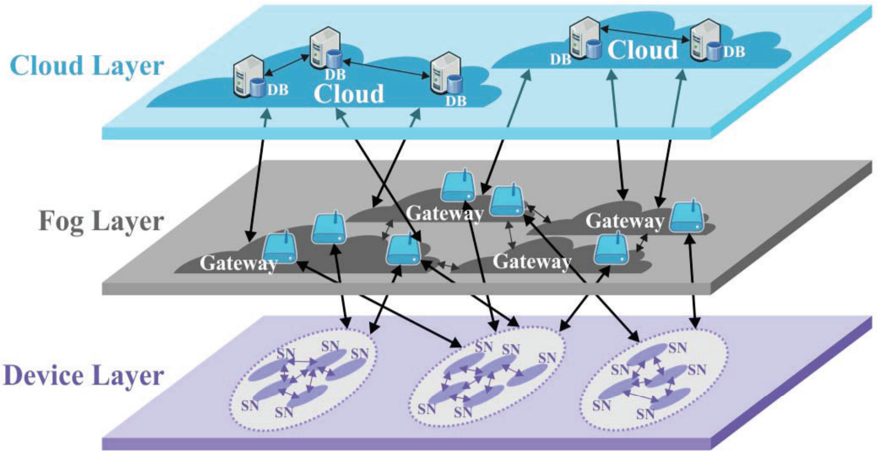


Figure 3.7: The three-tier system architecture of the healthcare IoT system [96] (SN and DB stand for Sensor Node and Database, respectively)

2. **Fog Layer**: The middle layer consists of a network of interconnected smart gateways. A smart gateway receives data from different subnetworks, performs protocol conversion, and provides other higher level services. It acts as a repository (local database) to temporarily store sensors' and users' information and provides intelligence at the edge of the network. In addition, by taking responsibility for handling some computational and processing burdens of the sensors and the cloud, a smart gateway at the fog layer can cope with many challenges such as energy efficiency, scalability, and reliability issues [106].

3. **Cloud Layer**: This layer includes broadcasting, data warehousing, and big data analysis servers, and a local hospital database that periodically performs data synchronization with the remote healthcare database server in the cloud. In the cloud layer, accessibility to patient-related health data is classified as public data (such as patients' ID or blood type) and private data (such as DNA).

In [22], we presented a comprehensive end-to-end security scheme for healthcare IoT systems. The scheme uses the session resumption technique which offloads the encrypted session states of DTLS towards a non-resource-constrained end-user (upper black arrow shown in Figure 3.6). The main motivation to employ the DTLS session resumption is to mitigate the overhead on resource-constrained sensors. Because transmitting and processing of messages in the certificate-based DTLS handshake are resource intensive

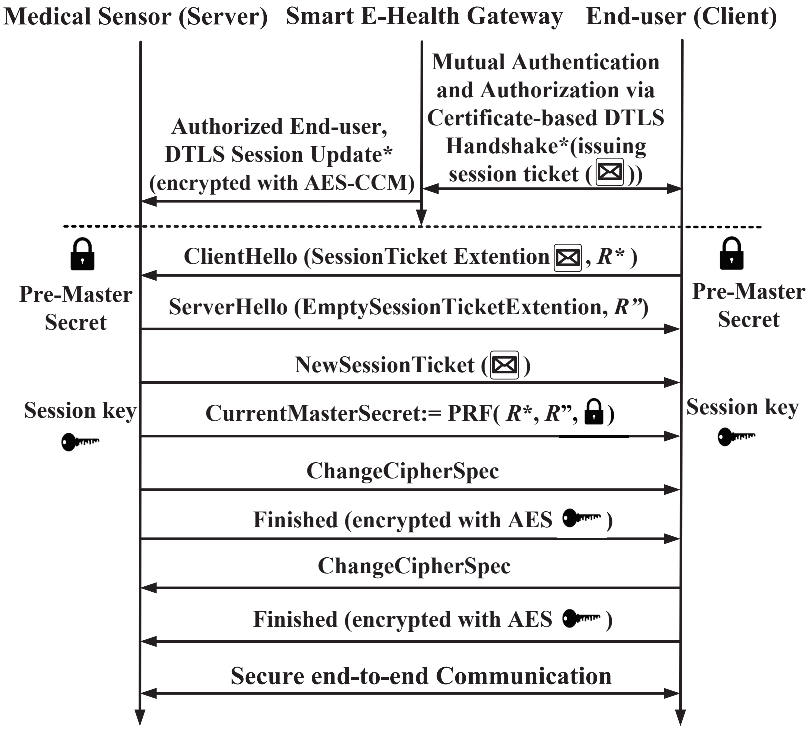

Medical Sensor (Server)
Smart E-Health Gateway
End-user (Client)
Mutual Authentication and Authorization via Certificate-based DTLS Handshake*(issuing session ticket (⊠))
Authorized End-user, DTLS Session Update* (encrypted with AES-CCM)
Pre-Master Secret
Pre-Master Secret
ClientHello (SessionTicket Extention ⊠, R*)
ServerHello (EmptySessionTicketExtention, R")
NewSessionTicket (⊠)
Session key
Session key
CurrentMasterSecret:= PRF(R*, R", 🔒)
ChangeCipherSpec
Finished (encrypted with AES)
ChangeCipherSpec
Finished (encrypted with AES)
Secure end-to-end Communication

Figure 3.8: The proposed session resumption based end-to-end security for healthcare Internet of Things [96]

tasks. The session resumption technique is an extended form of the DTLS handshake, which enables a client or server to continue the communication with a previously established session state without compromising the security properties. The protocol flow for the *SEA* architecture as well as the DTLS session resumption is shown in Figure 3.8. In the end-to-end security scheme, the fog layer facilitates ubiquitous mobility without requiring any reconfiguration at the device layer. To achieve continuous monitoring of patients considering the mobility support, we develop self-configuration or handover mechanisms that are capable of handling secure and efficient data transfers among different MSNs.

Figure 3.9 presents the mobility scenario where a patient wearing medical sensors decides to move from his or her room (base network) to other rooms (visited networks). We assumed a mobility scenario that consists of several MSNs for remote patient monitoring in a hospital or nursing/home environment. In the considered scenario, patients may roam through the hospital wards or move to other rooms due to some medical tests (e.g., Laboratory or X-ray). In the case that a moving sensor loses its connection

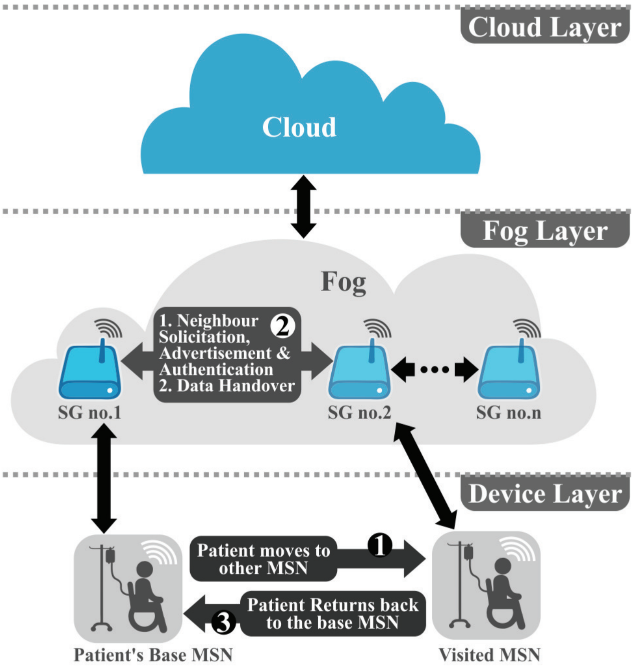

Cloud Layer
Cloud
Fog Layer
Fog
1. Neighbour Solicitation, Advertisement & Authentication
2. Data Handover
2
SG no.1
SG no.2
SG no.n
Device Layer
Patient moves to other MSN
1
Patient Returns back to the base MSN
3
Patient's Base MSN
Visited MSN

Figure 3.9: Mobility Scenario [96]

with one of the smart gateways, he or she will stop being monitored by the caregivers. This condition is not favorable in situations where real-time and continuous monitoring is necessary. To enable seamless transitions of medical sensors and considering the limitations of sensors, providing an efficient and robust data handover mechanism among smart gateways is of essential importance. The mobility scenario is discussed in three phases in the following subsections.

1. **Message Exchange in patients' base MSN:** This phase presents the initial state of the medical sensors where each sensor is connected to its base MSN via a smart e-health gateway and exchange the required messages. These messages may consist of data frames requests, responses, and acknowledgments of data transmission between the medical sensors and the smart gateways. The data frames include: (1) information regarding the DTLS session states for the subsequent DTLS session resumption and (2) information about the validity of remote caregivers. Information is exchanged between both peers using the aforementioned AES-CCM algorithm. Request messages are queries to the medical sensor to either get or change some values.

Response messages include replies to the request messages where the results of the operation can be obtained. In addition, the request and response messages include information that needs to be transmitted between the sensor and the gateway during the DTLS handshake to perform mutual authentication.

2. **Entering a new medical subnetwork:** Healthcare IoT services are supposed to be offered to patients in a seamless and continuous way as the patients move. When a patient moves out of his or her base MSN, the sensor detects that the quality of its connection with the associated smart gateway is reduced below a pre-defined threshold. We propose to provide mobility support to the sensors from the fog layer to alleviate the processing and computation burden of the sensors. To do so, the smart gateway located in the base network needs to check, through the fog layer, whether the medical sensor is accessible from other gateways. This type of mobility (micro-mobility) is just provided to those sensors that are in the same domain or sub-network and their IP addresses do not change. This type of scenario is desirable for MSNs of a hospital as the entire network relies on the same domain.

   To provide continuous monitoring of patients, efficient and seamless data handover mechanisms between smart e-health gateways are needed. These mechanisms should consider the following features: (1) Data handover between smart gateways should be quick and seamless, considering that the connection to the sensor needs to be preserved during the whole process; (2) after a successful data handover, the changes of routes to the moving medical senor should be spread quickly by the entire healthcare IoT system; and (3) the number of messages that need to be exchanged among gateways should be kept minimal (transmission overhead).

3. **Returning back to the base MSN:** When the patient returns back to the base network, the medical sensor sends a reassociation request to inform the smart gateway regarding its new location. Mobility is enabled in our proposed end-to-end security scheme using the fog concept. It is shown that by exploiting the fog layer, the mobility support can be ubiquitously provided to the medical sensors without compromising the end-to-end security.

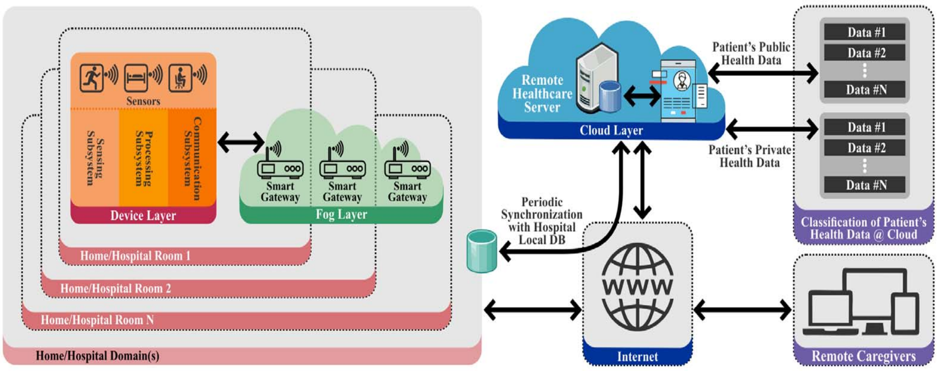


Figure 3.10: The system architecture of our healthcare IoT system with secure end-to-end communication [107]

3.5 End-to-End Security Scheme Performance Analysis

As the fifth contribution in this thesis, we analyzed the performance of the state-of-the-art end-to-end security schemes in healthcare IoT systems. The system architecture illustrated in Figure 3.10 was implemented for experimental evaluation for two different scenarios: in-home and hospital room(s). The main contributions of this work which is the holistic integration of our recent published works [20,22,96,97,98], are twofold. First, we identified and present the essential requirements of robust security solutions for healthcare IoT systems, which include (1) secure ECG-based cryptographic key generation, (2) authentication and authorization of each healthcare IoT component based on certificate-based DTLS, and (3) secure mobility-enabled end-to-end communication based on the session resumption technique, as well as the concept of fog layer in the IoT for realizing efficient and seamless mobility. Second, we analyze the performance of the state-of-the-art security solutions, including the end-to-end security scheme, which is tested by developing a prototype healthcare IoT system.

To Implement the proposed healthcare IoT system architecture, we setup a platform that consists of medical sensor nodes, UT-GATE smart e-health gateways, a remote server, and end-users. UT-GATE is constructed from the combination of a Pandaboard and a Texas Instruments (TI) SmartRF06 board that is integrated with a CC2538 module [31]. In our configuration, UT-GATE uses 8GB of external memory and is powered by Ubuntu OS which allows to control devices and services such as local storage and notification. To investigate the feasibility of our proposed architecture, the

Wismote [32] platform, which is a common resource-limited sensor nodes, is utilized in Contiki's network simulation tool Cooja [33]. For the evaluation, we use the open source tool *OpenSSL* version 1.0.1.j to create elliptic curve public and private keys from the NIST P-256 and X.509 certificates. *TinyDTLS* [35] is used as the code-base of the proposed scheme. For the public-key functions, we utilize the *Relic-toolkit* [36] that is an open source cryptography library tailored for specific security levels with emphasis on efficiency and flexibility. The MySQL database is set up for static and non-static records. The cloud server database is processed using xSQL Lite which is the third party tool for data synchronization. With respect to the cryptographic primitives and to make a fair comparison, we followed similar cipher suites as employed in the most recently proposed authentication and authorization architecture for IP-based IoT [36]. In this regard, we utilize elliptic curve NIST-256 for public-key operations, $AES\_128\_CCM\_8$ (with an IV of 8 bytes) for symmetric-key, and SHA256 for hashing operations. To asses the performance of different ECG-based cryptographic key generation approaches in terms of execution time, we conduct the experiments on ECG signals of 48 subjects with Arrhythmia obtained from the publicly available database, that is, Physiobank [28]. The recordings are digitized at 360 samples per second with 11-bit resolution over a 10 mV range per patient with 16 bit resolution over a range of 16 mV. We have captured 100 different samples of 5 minute long ECG data for each subject. We have implemented the key generation approaches utilizing MATLAB.

Based on the analysis, we found out that our solution has the most extensive set of performance features in comparison to related approaches found in the literature. Our end-to-end security scheme was designed by generating ECG-based cryptographic keys for medical sensor devices, certificate-based DTLS handshake between end-users and smart gateways as well as employing the session resumption technique for the communications between medical sensor devices and end-users. Our performance evaluation revealed that, the ECG signal based cryptographic key generation method that is employed in our end-to-end security scheme is on average 1.8 times faster than existing similar key generation approaches while being more energy-efficient. Compared to existing end-to-end security approaches, our scheme reduces the communication overhead by 26% and the communication latency between smart gateways and end users by 16%. Our scheme performed approximately 97% faster than certificate-based and 10% faster than symmetric key-based DTLS. In terms of memory requirements, certificate-based DTLS needs about 2.9 times more ROM and 2.2 times more RAM resources than our approach. In fact, the ROM and RAM requirements of our scheme are almost as low as insymmetric key-based DTLS. Our scheme is a very promising solution for ensuring secure end-to-end communications for healthcare IoT systems with low overhead.

Chapter 4

Overview of Original Publications

This chapter presents a summary of the original publications presented in Part II of this thesis, along with a description of the authors' contributions to each publication. It also provides a correlation between the RQs presented in Section 1.1 and the individual publications in Part II. Finally, it discusses how the original publications relate to one another.

4.1 Overview of Original Publications

This thesis is a collection of five original publications, which are referred to in the text by their Roman numerals. In this section, we present a summary of the individual publications while highlighting the authors' contributions to each publication.

4.1.1 Publication I: Pervasive Health Monitoring Based on Internet of Things: Two Case Studies

Publication I presents our health monitoring wireless sensor network architecture for remote monitoring of biomedical signals to alleviate issues in traditional health monitoring systems and to improve the quality of medical care. Two variants of the wireless health monitoring system are implemented to monitor patients remotely. One system implements a wireless sensor network based on low power ZigBee. The system consists of a set of sensor nodes (clients) to read, process, and send data from various medical sensors wirelessly over ZigBee to a server node. The other system implements an IP-based wireless sensor network, using IEEE 802.11 WLAN. The system consists of IEEE 802.11 WLAN based sensor modules to access biomedical signals from patients and send these to a remote server which updates the database in real-time. Our developed architectures are analyzed with the aim of identifying their pros and cons and discussing the suitability of mentioned wireless communication technologies for different healthcare application domains. In both implementations, the server node collects the medical data from several client nodes and updates a remote database. The webserver application accesses the database and updates the webpage in real-time, which can be accessed remotely. We observed that the power consumption in a ZigBee based network is almost six to seven times less (seven times for 802.11g and six times for 802.11b/n) when compared with the IEEE 802.11 WLAN based network for the same experimental setup. The IEEE 802.11 WLAN based network consumes more power than ZigBee for a lower data-rate. However, when data rate increases, power consumption in ZigBee enhances rapidly when compared to IEEE 802.11 WLAN. In practice the maximum data-rate achieved for transmitting sensor data with ZigBee using Contiki OS is 160 kbps, when the nodes are placed at a distance of approximately 10 meters.

To evaluate the efficiency of our health monitoring architectures, implementations were performed on the Contiki OS and Cooja simulator.

Author's contribution: The main idea presented in this paper was developed jointly by co-authors Sanaz Rahimi Moosavi and Anurag. Sanaz Rahimi Moosavi developed the implementation of the IoT-based architecture for remote health monitoring based on ZigBee. The paper was written jointly by co-authors Sanaz Rahimi Moosavi and Anurag under the guidance of Amir-Mohammad Rahmani, Tomi Westerlund, Geng Yang, Pasi Liljeberg, and Hannu Tenhunen.

4.1.2 Publication II: An Elliptic Curve-based Mutual Authentication Scheme for RFID Implant Systems

Publication II presents our novel secure elliptic curve-based mutual authentication scheme for RFID implant systems. To the best of our knowledge, previously presented elliptic curve-based authentication schemes, concerning RFID systems in general, cannot fully fulfill the essential security and performance requirements of RFID implant systems. The proposed mutual authentication scheme relies on elliptic curve cryptography. An elliptic curve cryptosystem is more efficient in terms of key sizes and required computations than conventional public key cryptosystems. In the proposed scheme, reader authentication and verification is performed based on ECDLP, while tag identification and tag verification phases rely on ECDSA using Quark lightweight hash. We proved that our proposed scheme is secure against the relevant attacks and also ensures a higher security level than related work found in the literature. In addition, we carried out a computational performance analysis of our proposed scheme. The analysis results show that our elliptic curve-based mutual authentication scheme has less communication overhead than similar available schemes. It also requires less total memory than existing schemes. Based on the results presented in this paper, we conclude that the proposed scheme has the appropriate features for use in RFID implant systems. We believe that our scheme is not just limited to RFID implant systems; it can also be applied to any application of the IoT that requires secure and efficient authentication.

Author's contribution: The author Sanaz Rahimi Moosavi developed the main idea presented in this paper under the guidance of Ethiopia Nigussie, Seppo Virtnane, and Jouni Isoaho. Sanaz Rahimi Moosavi is the main author of this paper.

4.1.3 Publication III: Low-latency Approach for Secure ECG Feature Based Cryptographic Key Generation

Publication III presents our low-latency approach for generating secure ECG feature based cryptographic keys. The approach is done by taking advantage of the uniqueness and randomness properties of ECG's main features. This approach achieves low-latency since the key generation relies on four reference-free ECG main features that can be acquired in a short time. We call the approach Several ECG Feature (SEF) based cryptographic key generation. SEF consists of (1) detecting the arrival time of ECG's fiducial points using a Daubechies wavelet transform to compute ECG's main features accordingly; (2) using a dynamic technique to specify the optimum number of bits that can be extracted from each main ECG feature, comprising of PR, RR, PP, QT, and ST intervals; (3) generating cryptographic keys by exploiting the above-mentioned ECG features; and (4) consolidating and strengthening the SEF approach with cryptographically secure pseudo-random number generators. The Fibonacci linear feedback shift register and AES algorithms are implemented as the pseudo-random number generator to enhance the security level of the generated cryptographic keys. Our approach is applied to different subjects' ECG signals. The security analyses of the proposed approach are carried out in terms of distinctiveness, the test of randomness, temporal variance, and using the NIST benchmark. The analyses reveal that the normal ECG rhythms have slightly better randomness compared to the abnormal ones. The analyses also show that the strengthened SEF key generation approach provides a higher security level in comparison to existing approaches that rely only on singleton ECG features. For the normal ECG rhythms, the SEF approach has in average the entropy of about 0.98 while cryptographic keys that are generated utilizing the strengthened SEF approach offer an entropy of about 1. The execution time required to generate the cryptographic keys on different processors is also examined. The results reveal that our SEF approach is on average faster than existing key generation approaches that only utilize the IPI feature of ECG. To evaluate the efficiency of our cryptographic key generation approach implementations have been performed using MATLAB platform and NIST benchmark.

Author's contribution: The author Sanaz Rahimi Moosavi developed the main idea presented in this paper under the guidance of Ethiopia Nigussie, Marco Levorato, Seppo Virtanen, and Jouni Isoaho. Sanaz Rahimi Moosavi is the main author of this paper.

4.1.4 Publication IV: End-to-End Security Scheme for Mobility Enabled Healthcare Internet of Things

Publication IV presents our end-to-end security scheme for mobility enabled healthcare IoT systems. The presented scheme consists of (1) a secure and efficient end-user authentication and authorization architecture based on the certificate based DTLS handshake, (2) secure end-to-end communication based on session resumption, and (3) robust mobility based on interconnected smart gateways. The smart gateways act as an intermediate processing layer (called fog layer) between IoT devices and sensors (device layer) and cloud services (cloud layer). In our scheme, the fog layer facilitates ubiquitous mobility without requiring any reconfiguration at the device layer. The scheme is demonstrated by simulation and a full hardware and software prototype. Based on our analysis, our scheme has the most extensive set of security features in comparison to related approaches found in the literature. Energy-performance evaluation results show that compared to existing approaches, our scheme reduces the communication overhead, as well as the communication latency, between smart gateways and end users. In addition, our scheme is faster than certificate-based and symmetric key based DTLS. Compared to our scheme, certificate based DTLS consumes more RAM and ROM resources. On the other hand, the RAM and ROM requirements of our scheme are almost as low as those in symmetric key-based DTLS. Analysis of our implementation revealed that the handover latency caused by mobility is low, and the handover process does not incur any processing or communication overhead on the sensors.

To evaluate the efficiency of our end-to-end security scheme implementations were performed on the Contiki OS and Cooja simulator using Relic toolkit.

Author's contribution: The main idea presented in this paper was developed by the author Sanaz Rahimi Moosavi in a close collaboration with co-authors Tuan Nguyen Gia, Ethiopia Nigussie, Amir M. Rahmani, Seppo Virtnane, and Jouni Isoaho. The implementation of the proposed end-to-end security scheme is done by Sanaz Rahimi Moosavi. Sanaz Rahimi Moosavi is the main author of this paper.

4.1.5 Publication V: Performance Analysis of End-to-End Security Schemes in Healthcare IoT

Publication V presents our performance analysis of the state-of-the-art end-to-end security schemes in healthcare IoT systems. We identified that the essential requirements of robust security solutions for healthcare IoT systems are comprised of (1) low-latency secure key generation approach using patients' Electrocardiogram (ECG) signals, (2) secure and efficient authentication and authorization for healthcare IoT devices based on the certificate-based datagram Transport Layer Security (DTLS), and (3) robust and secure mobility-enabled end-to-end communication based on DTLS session resumption. The performance of the state-of-the-art security solutions, including our end-to-end security scheme is tested by developing a prototype healthcare IoT system. The prototype is built of a PandaBoard, a TI SmartRF06 board and WiSMotes. The PandaBoard along with the CC2538 module acts as a smart gateway and the WisMotes act as medical sensor nodes. Based on the analysis, we found out that our solution has the most extensive set of performance features in comparison to related approaches found in the literature. The performance evaluation results show that the cryptographic key generation approach proposed in our end-to-end security scheme is faster than existing key generation approaches while being more energy-efficient. In addition, the scheme reduces the communication overhead and the communication latency between smart gateways and end users. Our scheme is also faster than the certificate-based and the symmetric key-based DTLS. The certificate based DTLS requires more ROM and RAM resources. On the other hand, the ROM and RAM requirements of our scheme are almost as low as in symmetric key-based DTLS.

To evaluate the performance analysis of our end-to-end security scheme implementations were performed utilizing the MATLAB platform, Contiki OS, Cooja simulator, and Relic toolkit.

Author's contribution: The author Sanaz Rahimi Moosavi developed the main idea presented in this paper under the guidance of Ethiopia Nigussie, Marco Levorato, Seppo Virtanen, and Jouni Isoaho. Sanaz Rahimi Moosavi is the main author of this paper.

Chapter 5

Conclusions

In this final chapter, we outline the main achievements put forward in this dissertation, as well as point out future research directions. In this dissertation, we identified and provided research-based solutions and suggestions for the problems related to the standards-based communication architecture, as well as building blocks, concerning secure end-to-end communications for the healthcare IoT systems. Healthcare IoT systems are distinct in that they are built to serve human beings, which inherently raises the requirements of security, privacy, and reliability. Moreover, the systems have to provide real-time notifications and responses regarding the statuses of patients. We presented wireless system architectures for remote monitoring of biomedical signals to alleviate issues in traditional health monitoring systems and to improve the quality of medical care. Two variants of the wireless health monitoring system architectures are implemented in this dissertation to monitor patients remotely. One system implements the WSN based on low power ZigBee and the other system implements the WSN based on the IEEE 802.11 WLAN. In both implementations, the sink node collects the medical data from several medical sensor nodes and updates a remote database. In a typical healthcare IoT system, the system has to ensure the safety of patients by monitoring patients' activities and vital signs. To guarantee these requirements, the smart components in the system require a predictable latency and reliable communication with the upper computing layer. The conventional cloud-based approaches cannot assure low-latency and high-availability requirements of healthcare IoT systems, as the connection to the cloud is less reliable and may incur additional latency.

In this dissertation, we discussed and introduced Fog computing as a means of enhancing the end-to-end security in an IoT-based healthcare system. Fog devices are heterogeneous in nature, ranging from end-user devices and access points to edge routers and switches, allowing their use in a wide variety of environments. Through the system implementation and verification in health monitoring case studies, this dissertation demonstrated that Fog computing is an appropriate solution, in particular, for improving IoT-based remote health monitoring and enhancing the quality of healthcare. The proposed solutions consist of (1) a low-latency approach for generating secure ECG feature-based cryptographic keys, (2) a secure and efficient end-user authentication and authorization architecture based on the elliptic curve cryptography and the certificate based DTLS handshake, (3) secure end-to-end communication based on session resumption, and (4) robust mobility based on interconnected smart gateways.

Medical sensors rely on cryptography to secure their communications. The proper application of cryptography requires the use of secure keys and key generation methods. Key generation in sensor networks generally requires some form of pre-deployment. Given the constrained nature of medical sensors used in BSNs, conventional key generation approaches may potentially involve reasonable computations, as well as latency, during network or any subsequent adjustments, due to their need for pre-deployment. Key generation solutions relying on humans' biometric systems best suit for tiny medical sensors, as those solutions are lightweight and require low resources. By developing robust and efficient key generation using biometric systems, the security of medical sensors can be provided in a plug-n-play manner where neither a network establishment nor a key pre-distribution mechanism is required. Cryptographic keys can be generated, renewed, and revoked within the network on the fly by using the information collected by medical sensors when and as needed. To alleviate these limitations, we proposed a robust key generation approach employing several ECG features, called SEF. Our SEF approach utilizes four main reference-free ECG features comprising of PR, RR, PP, QT, and ST. A dynamic technique is used to specify the optimum number of bits that can be extracted from each main ECG feature. We consolidated and strengthened the SEF approach with cryptographically secure pseudo-random number generator techniques. The Fibonacci linear feedback shift register and the AES algorithm are implemented as pseudo-random generators to enhance the security level of our approach. These keys can be employed in end-to-end communications to securely encrypt or decrypt messages transmitted between medical sensors and health caregivers. The keys can also be used for authentication and authorization of peers in MSNs.

We also leveraged the strategic position and the distributed nature of smart gateways in fog computing to provide a seamless authentication and authorization architecture, secure end-to-end communication, and mobility for healthcare IoT systems. The proposed authentication and authorization solution relied on the elliptic curve cryptography and the certificate-based DTLS handshake protocol. The solution reduces the overhead imposed on the medical sensors without compromising the security. Our end-to-end security scheme enables end-users and medical sensors to communicate without the need of performing heavy computations directly. The scheme relies on a certificate-based DTLS handshake between non-resource-constrained smart gateways and end-users at the start of the communication. To provide end-to-end security, DTLS session resumption without a server-side state is utilized. The session resumption technique has an abbreviated form of DTLS and neither requires heavy-weight certificate-related nor public-key operations as it relies on the previously established DTLS connection. In our scheme, ubiquitous mobility is feasible without requiring any reconfiguration at the device layer.

Results from the test-bed platform demonstration of our end-to-end security show that the ECG-based cryptographic key generation method that is employed in our end-to-end security scheme is faster than existing similar key generation approaches while being more energy-efficient. The security evaluation of the generated keys was performed in terms of distinctiveness, the test of randomness, and temporal variance by using the NIST benchmark. Our approach is applied to normal and abnormal ECG signals. The analysis showed that the strengthened key generation approach offers a higher security level in comparison to existing approaches that rely only on singleton ECG features. Our analyses also reveal that the normal ECG signals have slightly better randomness compared to the abnormal ones. Cryptographic keys that are generated from normal ECG signals using the SEF approach demonstrate lower entropy compared to cryptographic keys that are produced using the strengthened SEF approach. In addition, the reinforced key generation approach also has a better P-value NIST pass rate compared to state-of-the-art approaches, which rely only on singleton ECG features. Compared to the existing end-to-end security solutions, our scheme reduces the communication overhead, as well as the communication latency, between smart gateways and end users. Our scheme is faster than the certificate-based DTLS and the symmetric key-based DTLS. In terms of memory requirements, certificate-based DTLS consumes more RAM and ROM resources than our approach. In fact, the RAM and ROM requirements of our scheme are almost as low as in symmetric key-based DTLS. Taking into account that the handover latency caused by mobility is low and the handover process does not incur any processing or communication overhead on the sensors, we summarize that our scheme is a promising solution for ensuring end-to-end security and secure ubiquitous sensor-level mobility for healthcare IoT systems.

5.1 Future Work

This research will be extended by improving our communication architecture that securely monitors the end-to-end communications in healthcare IoT systems over the time and provides a finer performance of the end-to-end security scheme. Our future work focuses on the trade-off analysis between the security level and performance of the end-to-end security scheme in terms of latency and energy consumption. For this purpose, we are improving the latency and energy consumption of our scheme, while preserving the achieved high-security levels. We published the promising preliminary results in the Elsevier Ambient Systems, Networks and Technologies (ANT-2018) conference [107]. One of the main future goals is to conduct a more realistic experiment in order to fully realize the benefits and limitations of the proposed approaches. To validate our developed end-to-end communication architecture in Finland, we have chosen an application of healthcare as a case-study to be demonstrated in the experimental test-bed. The case study is on pain assessment with the collaboration of the Department of Nursing Science at the University of Turku and Turku University Hospital (TYKS). In addition, we are planning to consider device interoperability and data interoperability in our healthcare IoT architecture and investigate the security and privacy issues that result.

Bibliography

[1] Internet of Things Strategic Research Roadmap, 2009. http://www.internet-of-things-research.eu [accessed 2019-05-13].

[2] L. Xu, W. He, and S. Li. Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics Journal*, 10(4):2233–2243, 2014.

[3] S. Li, L. Xu, and S. Zhao. The Internet of Things: A Survey. *Information Systems Frontiers Journal*, 17(2):243–259, 2015.

[4] A.M. Rahmani, N.K. Thanigaivelan, Tuan Nguyen Gia, J. Granados, B. Negash, P. Liljeberg, and H. Tenhunen. Smart e-Health Gateway: Bringing Intelligence to IoT-Based Ubiquitous Healthcare Systems. In *Proceedings of the 12th Annual IEEE Consumer Communications and Networking Conference*, pages 826–834, Las Vegas, NV, USA, 2015.

[5] C.E. Koop, R. Mosher, L. Kun, J. Geiling, E. Grigg, S. Long, C. Macedonia, R. Merrell, R. Satava, and J. Rosen. Future Delivery of Health Care: Cybercare. *IEEE Engineering in Medicine and Biology Magazine*, 27(6):29–38, 2008.

[6] R. Mueller. Demo: A Generic Platform for Sensor Network Applications. In *Proceedings of the IEEE International Conference on Mobile Adhoc and Sensor Systems*, pages 1–3, Pisa, Italy, 2007.

[7] W. Shen, Y. Xu, D. Xie, T. Zhang, and A. Johansson. Smart Border Routers for eHealthCare Wireless Sensor Networks. In *Proceedings of the 7th International Conference on Wireless Communications, Networking and Mobile Computing*, pages 1–4, Wuhan, China, 2011.

[8] Intel® IoT Gateway, 2014. http://www.intel.com/content/products [accessed 2019-05-13].

[9] S. Kumar and C. Paar. Are Standards Compliant Elliptic Curve Cryptosystems Feasible on RFID? In *Proceedings of the Workshop on RFID Security*, pages 1–19, Graz, Austria, 2006.

[10] B. Xu, L. Xu, H. Cai, C. Xie, J. Hu, and F. Bu. Ubiquitous Data Accessing Method in IoT-Based Information System for Emergency Medical Services. *IEEE Transactions on Industrial Informatics Journal*, 10(2):1578–1586, 2014.

[11] G. Yang, L. Xie, M. Mantysalo, X. Zhou, Z. Pang, L. Xu, S. Kao-Walter, Q. Chen, and L. Zheng. A Health-IoT Platform Based on the Integration of Intelligent Packaging, Unobtrusive Bio-Sensor, and Intelligent Medicine Box. *IEEE Transactions on Industrial Informatics Journal*, 10(4):2180–2191, 2014.

[12] H. Yan, L. Xu, Z. Bi, Z. Pang, J. Zhang, and Y. Chen. An Emerging Technology– Wearable Wireless Sensor Networks With Applications in Human Health Condition Monitoring. *Journal of Management Analytics*, 2(2):121–137, 2015.

[13] K. Malasri and L. Wang. Addressing Security in Medical Sensor Networks. In *Proceedings of the 1st International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments*, pages 7–12, San Juan, Puerto Rico, 2007.

[14] D. Amiri, A. Anzanpour, I. Azimi, A.M. Levorato, M.and Rahmani, P. Liljeberg, and N. Dutt. Edge-assisted sensor control in healthcare iot. In *Proceedings of the IEEE Global Communications Conference*, pages 1–6, Abu Dhabi, United Arab Emirates, 2018.

[15] A.M. Rahmani, P. Liljeberg, J.S. Preden, and A. Jantsch. *Fog Computing in the Internet of Things - Intelligence at the Edge*. Springer, Berlin, Heidelberg, 04 2018.

[16] J. Gao F. Agrafioti and D. Hatzinakos. *Heart Biometrics: Theory, Methods and Applications*. IntechOpen, London, UK, 2011.

[17] C. Poon, Y. Zhang, and S. Bao. A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and m-Health. *IEEE Communications Magazine Journal*, 44(4):73–81, 2006.

[18] G. Zhang, C.Y. Poon, and Y. Zhang. Analysis of Using Interpulse Intervals to Generate 128-Bit Biometric Random Binary Sequences for Securing Wireless Body Sensor Networks. *IEEE Transactions on Information Technology in Biomedicine journal*, 16(1):176–182, 2012.

[19] F. Hao, R. Anderson, and J. Daugman. Combining Crypto with Biometrics Effectively. *IEEE Transactions on Computers Journal*, 55(9):1081–1088, 2006.

[20] S.R. Moosavi, E. Nigussie, M. Levorato, S. Virtanen, and J. Isoaho. Low-latency approach for secure ecg feature based cryptographic key generation. *IEEE Access Journal*, PP(99):1–1, 2017.

[21] S.R. Moosavi, T.N. Gia, A.M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, and H. Tenhunen. SEA: A Secure and Efficient Authentication and Authorization Approach for IoT-Based Healthcare Systems Using Smart Gateways. In *Proceedings of the 6th International Conference on Ambient Systems, Networks and Technologies*, pages 452–459, London, UK, 2015.

[22] S.R. Moosavi, T.N. Gia, E. Nigussie, A.M. Rahmani, S. Virtanen, H. Tenhunen, and J. Isoaho. Session Resumption-Based End-to-End Security for Healthcare Internet-of-Things. In *Proceedings of the IEEE International Conference on Computer and Information Technology*, pages 581–588, Liverpool, UK, 2015.

[23] D. Amiri, A. Anzanpour, I. Azimi, M. Levorato, A. Rahmani, P. Liljeberg, and N. Dutt. Edge-assisted Sensor Control in Healthcare IoT. In *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, 2018.

[24] D. Amiri, A. Anzanpour, I. Azimi, A. Rahmani, P. Liljeberg, N. Dutt, and M. Levorato. Optimizing Energy in Wearable Devices Using Fog Computing. In *Fog Computing: Theory and Practice*, pages 1–22. 2019.

[25] D. Amiri, A. Anzanpour, I. Azimi, M. Levorato, P. Liljeberg, N. Dutt, and A. Rahmani. Context-Aware Sensing via Dynamic Programming for Edge-Assisted Wearable Systems. In *ACM Transactions on Computing for Healthcare*, pages 1–26, 2019.

[26] Y.Liao and C. Hsiao. A Secure ECC-based RFID Authentication Scheme Integrated With ID-verifier Transfer Protocol. *Ad Hoc Networks Journal*, 2013.

[27] N. Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation Journal*, 48:203–209, 1987.

[28] A. Goldberger, L. Amaral, L. Glass, J. Hausdorff, P. Ivanov, R. Mark, J. Mietus, G. Moody, C. Peng, and H. Stanley. PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals. *Circulation Journal*, 101(23):e215–e220, 2000.

[29] MATLAB. *R2016a.* The MathWorks Incorporation, Davis, CA, USA, 2016.

[30] PandaBoard Platform Information. http://pandaboard.org/ [accessed 2019-05-13].

[31] SmartRF06 Evaluation Board. http://www.ti.com/lit/ug/swru321a [accessed 2019-05-13].

[32] Arago Systems. Wismote. http://www.aragosystems.com/en/document-center [accessed 2019-05-13].

[33] R. Hummen, H. Shafagh, S. Raza, T. Voig, and K. Wehrle. Delegation-based Authentication and Authorization for IP-based Internet of Things. In *Proceedings of the 11th IEEE International Conference on Sensing, Communication, and Networking*, pages 284–292, Singapore, Singapore, 2014.

[34] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W.polk. Internet X.509 Public Key Infrastructure Certificate Profile. http://tools.ietf.org/html/rfc5280 [accessed 2019-05-13].

[35] O. Bergmann. TinyDTLS. http://sourceforge.net/p/tinydtls [accessed 2019-05-13].

[36] D. Aranha and C. Gouv. RELIC is an Efficient Library for Cryptography. http://code.google.com/p/relic-toolkit/ [accessed 2019-05-13].

[37] S. Chakrabarti, E. Nordmark, and C. Bormann. Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs), 2012. https://rfc-editor.org/rfc/rfc6775.txt [accessed 2019-05-13].

[38] IEEE Standard. Ieee standard for low-rate wireless networks. *IEEE Std 802.15.4-2015 Journal*, pages 1–709, 2016.

[39] T. Chen, J. Ghaderi, D. Rubenstein, and G. Zussman. Maximizing broadcast throughput under ultra-low-power constraints. In *Proceedings of the 12th International on Conference on Emerging Networking EXperiments and Technologies*, pages 457–471, Irvine, CA, USA, 2016.

[40] M. Ryan. Bluetooth: With low energy comes low security. In *Proceedings of the 7th Conference on Offensive Technologies*, pages 1–4, Berkeley, CA, USA, 2013.

[41] C. Kuo, M. Luk, R. Negi, and A. Perrig. Message-in-a-bottle: User-friendly and Secure Key Deployment for Sensor Nodes. In *Proceedings of the 5th International Conference on Embedded Networked Sensor Systems*, pages 233–246, Sydney, Australia, 2007.

[42] Z. Shelby and C. Bormann. *6LoWPAN: The Wireless Embedded Internet*. Wiley, Sussex, UK, 2010.

[43] N. Kushalnagar, G. Montenegro, and C. Schumacher. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals, 2007. https://tools.ietf.org/html/rfc4919 [accessed 2019-05-13].

[44] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. https://tools.ietf.org/html/rfc4944, 2007. https://tools.ietf.org/html/rfc4919 [accessed 2019-05-13].

[45] J.P. Vasseur and A. Dunkels. *Interconnecting Smart Objects with IP: The Next Internet*. 2010.

[46] Carsten B. 6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs), 2014.

[47] B. Barker, C. Barker, E. Burr, W. Polk, and E. Smid. Sp 800-57. recommendation for key management, part 1: General (revised). Technical report, 2007.

[48] D Evans. The internet of things: How the next evolution of the internet is changing everything. *Cisco Internet Business Solutions Journal*, pages 1–11, 2011.

[49] L. Piccini, L. Arnone, F. Beverina, A. Cucchi, L. Petrelli, and G. Andreoni. Wireless dsp architecture for biosignals recording. In *Proceedings of the 4th IEEE International Symposium on Signal Processing and Information Technology*, pages 487–490, Bordeaux, France, 2004.

[50] H. She, Z. Lu, A. Jantsch, L. Zheng, and D. Zhou. A network-based system architecture for remote medical applications. *Proceedings of the Asia-Pacific Advanced Network Meeting Journal*, 2007.

[51] B. Lo, S. Thiemjarus, R. King, and G. Yang. Body Sensor Network - A Wireless Sensor Platform for Pervasive Healthcare Monitoring. In *Proceedings of the 3rd International Conference on Pervasive Computing*, pages 77–80, London, UK, 2005.

[52] R.S.H. Istepanian, S. Hu, N.Y. Philip, and A. Sungoor. The potential of internet of m-health things “m-iot” for non-invasive glucose level sensing. In *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 5264–5266, Boston, MT, USA, 2011.

[53] P. Tuyls and L. Batina. RFID-tags for Anti-Counterfeiting. In *Proceedings of the 2006 The Cryptographers' Track at the RSA conference on Topics in Cryptology*, pages 115–131, San Jose, CA, USA, 2006.

[54] Y. Lee, L. Batina, D. Singelée, B. Preneel, and I. Verbauwhede. Anti-counterfeiting, Untraceability and Other Security Challenges for RFID. In *Towards Hardware-Intrinsic Security*, pages 237–257. Springer, 2010.

[55] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. Public-Key Cryptography for RFID-Tags. In *Proceedings of the Pervasive Computing and Communications Workshops*, pages 217–222, White Plains, NY, USA, 2007.

[56] K. Yong, L. Batina, and I. Verbauwhede. EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID Authentication Protocol. In *Proceedings of the IEEE International Conference on RFID*, pages 97–104, Las Vegas, NV, USA, 2008.

[57] Z. Zhang, H. Wang, A.V. Vasilakos, and H. Fang. ECG-Cryptography and Authentication in Body Area Networks. *IEEE Transactions on Information Technology in Biomedicine Journal*, 16(6):1070–1078, 2012.

[58] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D. Culler. Spins: Security protocols for sensor networks. *Wireless Networks Journal*, 8(5):521–534, 2002.

[59] O. Garcia-Morchon, S. Keoh, S. Kumar, F. Moreno-Sanchez, P.and Vidal-Meca, and J. Ziegeldorf. Securing the ip-based internet of things with hip and dtls. In *Proceedings of the 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 119–124, Budapest, Hungary, 2013.

[60] C. Blundo, A. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly secure key distribution for dynamic conferences. *Information and Computation Journal*, 146(1):1 – 23, 1998.

[61] M. Marian and E. Sendroiu. A PKI Case Study: Implementing the Server-based CertificateValidation Protocol. In *Proceedings of the 18th International Conference on Systems, Signals and Image Processing*, pages 1–4, 2008.

[62] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, and M. Rossi. Secure communication for smart iot objects: Protocol stacks, use cases and practical examples. In *Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pages 1–7, San Francisco, CA, USA, 2012.

[63] S. Fouladgar, B. Mainaud, K. Masmoudi, and H. Afifi. Tiny 3-tls: A trust delegation protocol for wireless sensor networks. In *Proceedings of the Security and Privacy Workshop in Ad-Hoc and Sensor Networks*, pages 32–42, Berlin, Heidelberg, 2006.

[64] V. Gupta, M. Wurm, Y. Zhu, M. Millard, S. Fung, N. Gura, H. Eberle, and S.C. Shantz. Sizzle: A Standards-based End-to-end Security Architecture for the Embedded Internet. *Pervasive and Mobile Computing Journa*, 1(4):425 – 445, 2005.

[65] N. Modadugu and E. Rescorla. The Design and Implementation of Datagram TLS. 2003. https://pdfs.semanticscholar.org/ [accessed 2019-05-13].

[66] S. Bajikar. Trusted platform module (tpm)-based security on notebook pcs. *Mobile Platforms Group, Intel Corporation magazine*, 20, 2002.

[67] W. Hu, H. Tan, P. Corke, W. Shih, and S. Jha. Toward trusted wireless sensor networks. *ACM Transactions on Sensor Networks Journal*, 7(1):1–25, 2010.

[68] T. Kothmayr, C. Schmitt, Wen Hu, M. Brunig, and G. Carle. A DTLS Based End-to-End Security Architecture for the Internet of Things with Two-Way Authentication. In *Proceedings of the IEEE 37th Conference on Local Computer Networks Workshops*, pages 956–963, Clearwater, FL, USA, 2012.

[69] D.K. Altop, A. Levi, and V. Tuzcu. Towards Using Physiological Signals as Cryptographic Keys in Body Area Networks. In *Proceedings of the International Conference on Pervasive Computing Technologies for Healthcare*, pages 92–99, Istanbul, Turkey, 2015.

[70] K. Venkatasubramanian, A. Banerjee, and S. Gupta. PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks. *IEEE Transactions on Information Technology in Biomedicine Journal*, 14(1):60–68, 2010.

[71] K. Venkatasubramanian, A. Banerjee, and S. Gupta. Plethysmogram-based Secure Inter-Sensor Communication in Body Area Networks. In *Proceedings of the IEEE Military Communications Conference*, pages 1–7, San Diego, CA, USA, 2008.

[72] F. Miao, L. Jiang, Y. Li, and Y.T. Zhang. Biometrics Based Novel Key Distribution Solution for Body Sensor Networks. In *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 2458–2461, Minneapolis, MN, USA, 2009.

[73] A. Banerjee, K. Venkatasubramanian, and K.S. Gupta. Challenges of Implementing Cyber-Physical Security Solutions in Body Area Networks. In *Proceeding of International Conference on Body Area Networks*, pages 1–8, Los Angeles, California, 2009.

[74] A. Juels and M. Wattenberg. A Fuzzy Commitment Scheme. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pages 28–36, New York, NY, USA, 1999.

[75] S. Bao, Y. Zhang, and L. Shen. Physiological Signal Based Entity Authentication for Body Area Sensor Networks and Mobile Healthcare Systems. In *Proceedings of IEEE Engineering in Medicine and Biology Society Annual Conference*, pages 2455–2458, Shanghai, China, 2005.

[76] S. Bao, C. Poon, Y. Zhang, and L. Shen. Using the Timing Information of Heartbeats as an Entity Identifier to Secure Body Sensor Network. *IEEE Transactions on Information Technology in Biomedicine Journal*, 12(6):772–779, 2008.

[77] F. Xu, Z. Qin, C.C. Tan, B. Wang, and Q. Li. IMDGuard: Securing Implantable Medical Devices With The External wearable guardian. In *Proceedings of the IEEE Conference on Computer Communications*, pages 1862–1870, Shanghai, China, 2011.

[78] A. Rukhin, J. Soto, J. Nechvatal, E. Barker, S. Leigh, M. Levenson, D. Banks, A. Heckert, J. Dray, S. Vo, A. Rukhin, J. Soto, M. Smid, S. Leigh, M. Vangel, A. Heckert, J. Dray, and L. Bassham. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final/ [accessed 2019-05-13].

[79] G. Zheng, G. Fang, R. Shankaran, M. Orgun, J. Zhou, L. Qiao, and K. Saleem. Multiple ECG Fiducial Points based Random Binary Sequence Generation for Securing Wireless Body Area Networks. *IEEE Journal of Biomedical and Health Informatics*, PP(99):1–9, 2016.

[80] N. Modadugu E. Rescorla. Datagram Transport Layer Security (DTLS) Version 1.2. Technical report, 2012.

[81] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton. CodeBlue: An Ad hoc Sensor Network Infrastructure for Emergency Medical Care. pages 12–14, 2004.

[82] K. Lorincz, D. Malan, T. Fulford, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton. Sensor Networks for

Emergency Response: Challenges and Opportunities. *IEEE Pervasive Computing Journal*, 3(4):16–23, 2004.

[83] C. Karlof, N. Sastry, and D. Wagner. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. In *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, pages 162–175, Baltimore, MD, USA, 2004.

[84] G. Kambourakis, E. Klaoudatou, and S. Gritzalis. Securing Medical Sensor Environments: The CodeBlue Framework Case. In *Proceedings of the 2nd International Conference onAvailability, Reliability and Security*, pages 637–643, Vienna, Austria, 2007.

[85] J. Ko, J. Lim, Y. Chen, R. Musvaloiu, A. Terzis, G. Masson, T. Gao, W. Destler, L. Selavo, and R. Dutton. MEDiSN: Medical Emergency Detection in Sensor Networks. *ACM Transactions on Embedded Computing Systems Journal*, 10:1–29, 2010.

[86] C. Tan, H. Wang, S. Zhong, and Q. Li. IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks. *IEEE Transactions on Information Technology in Biomedicine*, 13(6):926–932, 2009.

[87] J. Granjal, E. Monteiro, and J. Silva. End-to-end Transport-Layer Security for Internet-Integrated Sensing Applications with Mutual and Delegated ECC Public-Key Authentication. In *Proceedings of the International Conference on Networking*, pages 1–9, Brooklyn, NY, USA, 2013.

[88] N. Kang, J. Park, H. Kwon, and S. Jung. ESSE: Efficient Secure Session Establishment for Internet-Integrated Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*, 2015(7):1–12, 2015.

[89] S. valenzuela, M. Chen, and V. Leung. Mobility Support For Health Monitoring at Home Using Wearable Sensors. *IEEE Transactions on Information Technology in Biomedicine Journal*, 15(4):539–549, 2011.

[90] A. Jara, M. Zamora, and A. Skarmeta. An Initial Approach to Support Mobility in Hospital Wireless Sensor Networks Based on 6LoWPAN (HWSN6). *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 1(2/3):107–122, 2010.

[91] A. Jara, M. Zamora, and A. Skarmeta. HWSN6: Hospital Wireless Sensor Networks Based on 6LoWPAN Technology: Mobility and

Fault Tolerance Management. In *Proceedings of the IEEE International Conference on Computational Science and Engineering*, pages 879–884, Vancouver, BC, Canada, 2009.

[92] A. Jara, M. Zamora, and A. Skarmeta. Intra-mobility for Hospital Wireless Sensor Networks Based on 6LoWPAN. In *Proceedings of the 6th International Conference on Wireless and Mobile Communications*, pages 389–394, Valencia, Spain, 2010.

[93] H. Fotouhi, M. Alves, M. Zuniga, and A. Koubaa. Reliable and Fast Hand-Offs in Low-Power Wireless Networks. *IEEE Transactions on Mobile Computing Journal*, 13(11):2620–2633, 2014.

[94] S. Li, L. Xu, and X. Wang. Compressed Sensing Signal and Data Acquisition in Wireless Sensor Networks and Internet of Things. *IEEE Transactions on Industrial Informatics journal*, 9(4):2177–2186, 2013.

[95] S. Li, L. Xu, and X. Wang. A Continuous Biomedical Signal Acquisition System Based on Compressed Sensing in Body Sensor Networks. *IEEE Transactions on Industrial Informatics Journal*, 9(3):1764–1771, 2013.

[96] S.R. Moosavi, T.N. Gia, E. Nigussie, E. Rahmani, S. Virtanen, H. Tenhunen, and J. Isoaho. End-to-End Security Scheme for Mobility Enabled Healthcare Internet of Things. *Future Generation Computer Systems Journal*, 2016.

[97] S.R. Moosavi, E. Nigussie, S. Virtanen, and J. Isoaho. Cryptographic key generation using ECG signal. In *Proceedings of the 14th IEEE Annual Consumer Communications Networking Conference*, pages 1024–1031, Las Vegas, USA, 2017.

[98] S.R. Moosavi, E. Nigussie, M. Levorato, S. Virtanen, and J. Isoaho. Low-latency Approach for Secure ECG Feature Based Cryptographic Key Generation, year=2017. *IEEE Access Journal*.

[99] Anurag, S. R. Moosavi, A. Rahmani, T. Westerlund, G. Yang, P. Liljeberg, and H. Tenhunen. Pervasive Health Monitoring Based on Internet of Things: Two Case Studies. In *4th International Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH)*, pages 275–278, 2014.

[100] S. Martinez, M. valls, C. Roing, J. Miret, and F. Gine. A Secure Elliptic Curve-Based RFID Protocol. *Journal of Computer Science and Technology*, 24(2):309–318, 2009.

[101] S. Rahimi, A. Hakkala, J. Isoaho, S. Virtanen, and J. Isoaho. Specification Analysis for Secure RFID Implant Systems. *Journal of Computer Theory and Engineering*, 6(2):177–189, 2014.

[102] S. Bao, C.Y. Poon, Y. Zhang, and L. Shen. Using the Timing Information of Heartbeats as an Entity Identifier to Secure Body Sensor Network. *IEEE Transactions on Information Technology in Biomedicine Journal*, 12(6):772–779, 2008.

[103] G.H. Zhang, C.Y. Poon, and Y.T. Zhang. A Fast Key Generation Method Based on Dynamic Biometrics to Secure Wireless Body Sensor Networks for P-health. In *Proceedings of the International Conference of the IEEE Engineering in Medicine and Biology*, pages 2034–2036, Buenos Aires, Argentina, 2010.

[104] M. Rostami, A. Juels, and F. Koushanfar. Heart-to-Heart (H2H): Authentication for Implanted Medical Devices. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 1099–1112, Berlin, Germany, 2013.

[105] G. Zheng, G. Fang, R. Shankaran, and M.A. Orgun. Encryption for implantable medical devices using modified one-time pads. *IEEE Access Journal*, 3:825–836, 2015.

[106] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli. Fog Computing and Its Role in The Internet of Things. In *Proceedings of the Workshop on Mobile Cloud Computing*, pages 13–16, Helsinki, Finland, 2012.

[107] S.R. Moosavi, E. Nigussie, M. Levorato, S. Virtanen, and J. Isoaho. Performance analysis of end-to-end security schemes in healthcare iot. pages 432 – 439, 2018.

Part II

Original Publications

Publication I

”Pervasive Health Monitoring Based on Internet of Things: Two Case Studies”

Anurag, Sanaz Rahimi Moosavi, Amir M. Rahmani, Tomi Westerlund, Guang Yang, Pasi Liljeberg, Hannu Tenhunen

Original published in Proceeding of the IEEE International Conference on Wireless Mobile Communication and Healthcare (ICST-2014), 2014, pages 275-278, Greece.

Pervasive Health Monitoring Based on Internet of Things: Two Case Studies

Anurag[1], Sanaz Rahimi Moosavi[1], Amir-Mohammad Rahmani[1], Tomi Westerlund[1], Geng Yang[2],
Pasi Liljeberg[1], and Hannu Tenhunen[1]
[1]Department of Information Technology, University of Turku, Turku, Finland
[2]School of Information and Communication, Royal Institute of Technology (KTH), Stockholm, Sweden
Email: {anutha, saramo, amirah, tovewe, pakrli, hatenhu}@utu.fi, gengy@kth.se

***Abstract*—With the continuous evolution of wireless sensor networks and Internet of Things (IoT) various aspects of life will benefit. IoT based pervasive healthcare system has potential to provide error free medical data and alerting system in critical conditions with continuous monitoring. The system will minimize the need of dedicated medical personnel for patient monitoring and help the patients to lead a normal life besides providing them with high quality medical service. In this paper, we provide the implementation of IoT-based architectures for remote health monitoring based on two popular wireless technologies, Wi-Fi and ZigBee. We analyse the two architectures with the aim of identifying their pros and cons and discuss suitability of mentioned wireless communication technologies for different healthcare application domains.**

***Abstract*—Internet of Things, e-Health, ZigBee , Wi-Fi, Wireless Sensor Network (WSN), Remote Patient Monitoring.**

I. Introduction

Internet of Things (IoT) is enabling and revolutionising the way in which physical objects are communicating with each other. IoT can be utilised in several application domains such as: smart homes and cities, food safety and security and healthcare. The possibilities that IoT provides will innovate novel applications and devices whose communication capability will create new markets and a new economy. It is predicted that number of devices with the internet capability (connected to internet) will be around 25 billion by 2015 and 50 billion by 2020 [1].

IoT offers enormous opportunities to revolutionise healthcare in the near future. It can play a vital role in a wide range of healthcare devices that, for example, enable remote vital sign monitoring in hospitals and more importantly at home. Indeed, remote monitoring offers tremendous possibilities to decrease the costs of healthcare, and, at the same time, to increase healthcare quality by identifying and preventing diseases. In many cases health care is becoming increasingly costly, as patients are required to stay in hospital for the entire duration of their treatment due to the lack of devices with a capability to remotely provide patient's health information to authorised health professionals. Using IoT, gathering patient's health information and transferring it in real time to healthcare professionals will not only reduce the cost of healthcare services but also enable the treatment of health issues before they become critical.

In this paper, we present a health monitoring wireless sensor network architecture and assess the usability of two wireless communication technologies in the presented context. The aim is to identify the advantages and shortcomings of these architectures and find application domains in which these architectures can be properly utilized.

There exist several wireless communication technologies such as Bluetooth, ZigBee, 6LoWPAN or Wi-Fi that can be used to implement wireless network systems. Every technology has its own advantages and drawbacks. The most suitable technology strongly depends on the application requirements. For our health monitoring platform, we use Wi-Fi and ZigBee wireless technologies. For example, if a ZigBee based sensor network is supposed to transfer data to smart phones or tablets, which normally does not support IEEE 802.15.4 standard, a translation gateway is needed to transform ZigBee to another protocol such as Wi-Fi or Bluetooth. To avoid transforming protocols, interoperability should be an intrinsic feature of a sensor based wireless network. For this purpose, Wi-Fi is one of the most popular choices for wireless communication protocol.

II. Related Work and Motivation

There have been many efforts in the field of IoT based remote patient monitoring systems. Piccini *et al.* [2] discuss wireless system based on Bluetooth for acquiring bio-medical signals such as Electrocardiography (ECG), Electromyography (EMG), Electroencephalography (EEG) and Electrooculography (EOG). The architecture consists of two operational units: one to acquire single lead ECG signal and the other a DSP system to clean the acquired signal from the first unit. More research is required for integrating the associated sensors with a hardware board and miniaturising the system to make it wearable. She *et al.* [3] present a wireless sensor network architecture based on the IEEE 802.15.4 standard (ZigBee) and 3G networks for healthcare applications for home or hospital. The system reads signals including ECG, EMG, EEG and EOG, heart rate, breathing and blood pressure, processes it and sends it to a remote server or displays it over LCD screen. The system implements priority scheduling and data compression, which reduces the transmission delays of critical signals and saves bandwidth and power. Lo *et al.* [4] explain body sensor network (BSN) based on the IEEE 802.15.4 standard which not only monitors and process medical data such as ECG and SpO2 but also implements context aware sensing with the help of context sensors (e.g. temperature, accelerometer, and humidity). The BSN is power efficient requiring only 0.01 mA in active mode and 1.3 mA for computations such as fast Fourier transform (FFT). The collected and processed data is displayed by a flash BSN card for PDAs. A PDA also works as an access point to send the processed data to a central server. Istepanian *et al.* [5] propose m-IoT (Internet of M-Health Things), an IP based wireless sensor network architecture based on 6LoWPAN, which is used to

978-1-63190-014-3 © 2014 ICST
DOI 10.4108/icst.mobihealth.2014.257395

measure medical data such as glucose level in blood and blood pressure. A central access point collects data from the sensor nodes and send to IP based medical server, from where it can be accessed and analysed. Our motivation in this paper is to compare the implementation of health monitoring wireless sensor network architectures based on two popular wireless technologies (Wi-Fi and ZigBee) and analyse the suitability of these technologies for different medical applications.

III. System Architectures for Health Monitoring

In this section, we discuss the implementation of two architectures for remote monitoring of bio-medical signals. Medical applications have certain nature and requirements that usually have life or death consequences when data is not successfully transferred (e.g. lost, corrupted, delayed, etc.) as opposed to most other applications where requirements and concerns are mostly financial. These requirements such as data rate and delay have been defined by the IEEE 1073 group. For example, in case of 3-lead ECG system, a patient node (i.e., a wireless electrode) generates 2.4 Kbits/s of data [6]. In our implementations, the sensors used to collect medical data include Blood Pressure, Heart Rate, Temperature, Respiration, Glucose, SpO2, and ECG. Data rate for bio-medical signal varies significantly. The data rates of various signals are presented in Table 1.

Table 1: Data rate of various bio-medical signals

Bio-medical Signal	Latency	Data Rate
Blood pressure	< 3 s	80 - 800 bps
Pulse / Heart Rate	< 3 s	80 - 800 bps
Glucose	< 3 s	80 - 800 bps
Temperature	< 3 s	80 - 800 bps
Respiration	< 300 ms	50 - 120 bps
SpO2	< 300 ms	50 - 120 bps
ECG	< 300 ms	3-lead (2.4 kbps), 5-lead (10 kbps), 12-lead (72 kbps),

The first architecture implements wireless sensor network based on low-power ZigBee, while the second architecture implements IP-based wireless sensor network using Wi-Fi.

A. ZigBee-Based Architecture

ZigBee is based on low-rate IEEE 802.15.4 standard, designed for supporting low-power, low-cost, and low-data rate applications. The ZigBee based architecture consists of several patient nodes and a sink node. The system is implemented with ZigduinoR2 [7] hardware platform, which is an Arduino compatible microcontroller platform (ATmega128RFA1). *contiki* operating system is used to implement WSN. ZigBee based architecture as shown in Figure 1 can be divided into four sections; sensor interface, WSN implementation, database application and webserver application.

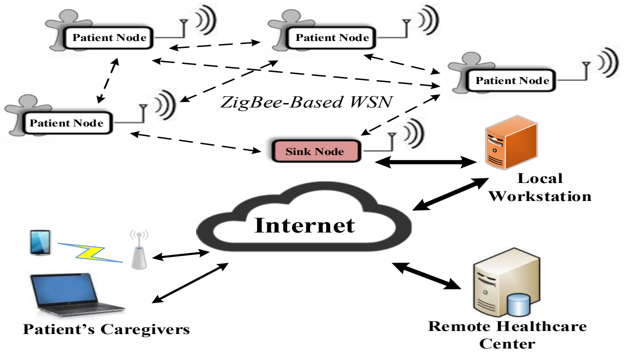


Figure 1: ZigBee Based Health Monitoring System

Sensor interface: The sensor interface is implemented using an Arduino-compatible E-health shield on top of the Zigduino hardware. The E-health shield is basically a gateway between the medical sensors and Zigduino board. Data measured from various sensors are collected by the Zigduino board via the E-health shield.

WSN implementation: The Zigduino's microcontroller contains an on-chip 2.4 GHz IEEE 802.15.4 radio. The implemented WSN consists of several patient (client) nodes and a sink (server) node. Patient nodes collect data from various sensors and send wirelessly over ZigBee to the sink (server) node. The code architecture of sink and patient nodes are shown in Table 2.

Table 2: Code architecture of sink and patient node

Server (sink) node architecture	
ZigBeeServer	Send and receive data over ZigBee
ServiceServer	Add and remove nodes in the network and assign ID to them
MACServer	Grants permission to the nodes to access media.
Client (Patient) node architecture	
ZigBeeServer	Send and receive data over ZigBee
MeasurementServer	Collect data and store them in FIFO
ServiceServer	Add and remove nodes in the network and assign ID to them
MACServer	Grants permission to the nodes to access media

Database application: The sink (server) node is connected to a local PC (Personal computer) where a Python code executes to collect data from the serial terminal and save it into a remote database.

Webserver Application: Web-server application written with PHP accesses the database and updates the web page in real time. The data from the webpage can be accessed remotely by patient's caregivers through their laptops or smart phones using any browser.

B. Wi-Fi-Based Architecture

The Wi-Fi based architecture consists of Wi-Fi enabled sensor nodes (Patient node) to access patient's medical data and Wi-Fi access point (Wi-Fi router). The sensor nodes (Patient node) are designed using an Analog Front-End (AFE, ADS1192 from Texas Instruments, [8]) and Wi-Fi module (RTX4140 Wi-Fi module, [9]). The RTX module is provided with proprietary operating system (ROS). Processor used in the Wi-Fi module is EFM32GG230F1024. The architecture (Figure 2) can be divided into four sections; sensor interface, WSN implementation, database application and webserver application.

Sensor interface: The sensor interface is implemented using the AFE to read data from the medical sensors and perform analog to digital conversion. The digital data from the output of AFE is read by RTX4140 through SPI (Serial Peripheral Interface).

WSN implementation: A UDP (User Datagram Protocol) client application running on the RTX4140 sends the UDP data packet to a remote server through Wi-Fi, once the connection to the Wi-Fi access point is established.

Database application: A UDP server application (running on a remote system), written in python, continuously listens to the UDP port, collects the incoming data and updates a remote database.

Webserver application: Webserver application is same as that of the ZigBee-based architecture.

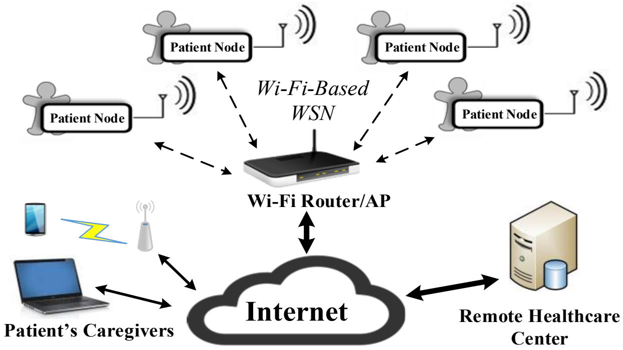


Figure 2: Wi-Fi Based Health Monitoring System

Figure 3 shows the implemented WSN. The patient (client) node collects medical (ECG) data from patient and transmits to the sink (server) node over ZigBee. The sink (server) node is connected to a local PC (Personal computer). The webserver application displays the ECG data on the webpage. In Figure 3, the ECG graph is displayed on a local PC, but it can be accessed from any remote location.

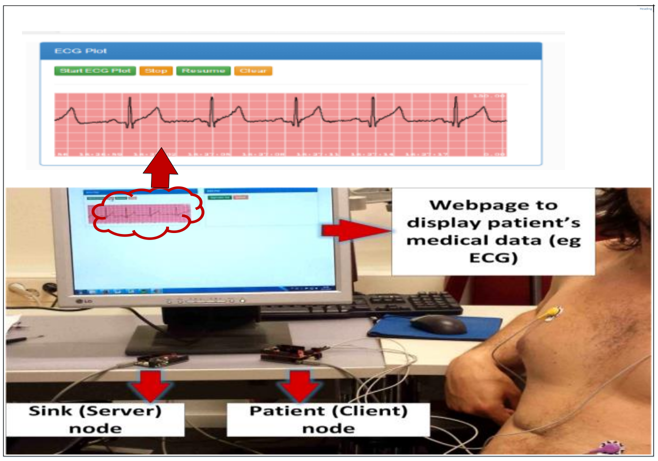


Figure 3: Implementation of WSN

C. Comparison

Both of the communication technologies, Wi-Fi and ZigBee, have their advantages and drawbacks. In this section, we discuss some features that influence the selection of the communication technology in the context of healthcare. The features that we will consider are interference, security, energy consumption, reliability, and issue of coexistence. In the following, we further elaborate these features. Table 3 presents a comparison between the two technologies.

ZigBee uses mesh topology which has several advantages over point to point networks in terms of reliability, scalability, and addressing interference issue by virtue of their structure. Reliability in case of Wi-Fi can be addressed with overlapping WAPs (Wireless access points). The mesh topology can scale to hundreds of client nodes easily, but in case of point to point network in order to add an extra client node above 255, an extra access points or router needs to be added [10]. The interference issue in case of mesh can be resolved by choosing an alternate (or best) path [11], whereas in case of point to point networks, it is either required to lower the data rate, lower the transmit power, or change the channel [12]. In order to address the issue of coexistence between ZigBee and Wi-Fi, dynamic frequency selection and transmission power control is used [13]. Wi-Fi being IP based network provides all the benefits of IP standard such as heterogeneity, compatibility, flexibility, speed, security, efficiency, and accuracy. Power consumption is a concern in case of Wi-Fi with battery life usually ranging from 0.5 to 5 days, whereas in case of ZigBee the battery life can be as long as 1000 days depending upon the application [14]. For security both the technologies use encryption and authentication mechanism; ZigBee uses AES (Advanced Encryption Standard) block cipher with counter mode (CTR), whereas Wi-Fi uses RC4 stream cipher for data encryption. In case of Wi-Fi in order to overcome the weakness of WEP (Wire equivalent privacy), Wi-Fi protected access 2 (WPA2) is used.

Table 3: Comparison between ZigBee and Wi-Fi

Standard	ZigBee	Wi-Fi
IEEE spec.	802.15.4	802.1 1a/b/g
Frequency band	868/915 MHz; 2.4 GHz	2.4 GHz; 5 GHz
Max signal rate	250 Kb/s	54 Mb/s
Nominal range	10 - 100 m	100 m
Number of RF channels	1/10; 16	14 (2.4 GHz)
Channel bandwidth	0.3/0.6 MHz; 2 MHz	22 MHz
Coexistence mechanism	Dynamic freq. selection	Dynamic freq. selection, transmit power control
Battery Life (days)	100 – 1,000	0.5 – 5.0
Basic cell	Star	BSS (basic service set)
Extension of the basic cell	Cluster tree, Mesh	ESS (extended service set)
Max number of cell nodes	> 65000	255
Encryption	AES block cipher (CTR, counter mode)	RC4 stream cipher (WEP), AES block cipher

IV. Demonstrators, Results and Discussion

The experimental setup to compare both the architectures is shown in Figure 4. The scenario consists of a hospital room with twenty patient nodes reading patient's medical data from various sensors including 2-lead ECG, SpO2, Blood Pressure, Heart Rate, Temperature, Respiration, and Glucose level. There is one sink node (for ZigBee based architecture) or a Wi-Fi access point (for Wi-Fi based architecture) to collect data from all the patient nodes in their respective setup. The distance between the adjacent patient nodes in same column is two meters and the distance between the adjacent patient nodes in different column is six meters. Every patient node transmits about 8.7 kbits (payload) of data per second. Figure 5 summarizes the average power consumption (mW) by the patient (client) nodes of Wi-Fi and ZigBee based architectures, with respect to the experimental setup discussed.

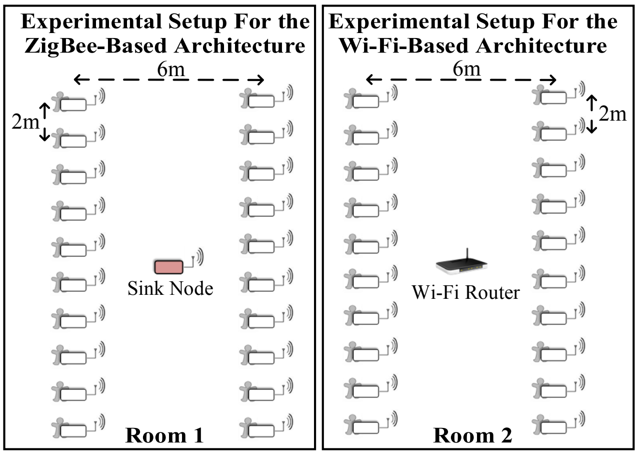

Experimental Setup For the ZigBee-Based Architecture
6m
2m
Sink Node
Room 1
Experimental Setup For the Wi-Fi-Based Architecture
6m
2m
Wi-Fi Router
Room 2

Figure 4: Experimental setup to compare both the architectures

The power consumption in case of three different Wi-Fi protocols 802.11b/g/n are 14, 17.5, and 14 mW respectively, whereas in case of the ZigBee based network the power consumption is considerably less (2.4 mW).

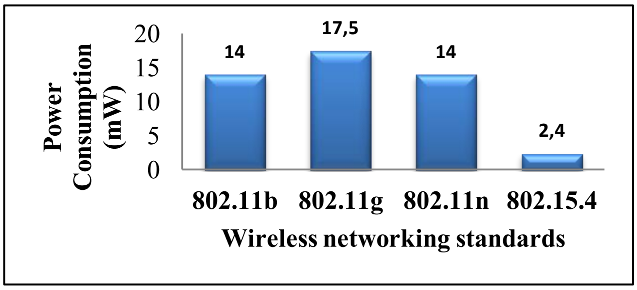


Figure 5: Average power consumption in ZigBee and Wi-Fi based sensor nodes

Thus we can observe that the power consumption in ZigBee based network is almost 6 to 7 times less (7 times for 802.11g and 6 times for 802.11b/n) when compared with Wi-Fi based network for the same experimental setup. At this point it is worth noting that although Wi-Fi based network consumes more power than ZigBee for lower data-rate, with increase in data rate, power consumption in ZigBee increases rapidly when compared to Wi-Fi. In practise the maximum data-rate achieved for transmitting sensor data with ZigBee using *contiki* OS is 160 Kbits/sec, when the nodes are placed at a distance of around 10 meters. In case of star topology the network can support up to 18 nodes, whereas in case of mesh topology using multi-hopping each nodes can route data of up to 17 other nodes apart from transmitting the data acquired, thus increasing the scalability to higher number. At the present data rate (8.7kbits/sec payload) required, scalability is not an issue in case of Wi-Fi and the system can be scaled to large number of nodes using single access-point.

V. CONCLUSIONS

In this paper, we presented wireless systems for remote monitoring of bio-medical signals to alleviate issues in traditional health monitoring systems and to improve the quality of medical care. Two variants of the wireless health monitoring systems are implemented to remotely monitor patients. One system implements wireless sensor network based on low power ZigBee. The system consists of set of sensor nodes (clients) to read data from various medical sensors process it and send wirelessly over ZigBee to a server node. The other system implements IP-based wireless sensor network, using Wi-Fi. The system consists of Wi-Fi based sensor module to access bio-medical signals from patients and send it to a remote server which updates the database in real-time. In both implementations, the server node collects the medical data from several client nodes and updates a remote database. The webserver application accesses the database and updates the webpage in real-time, which can be accessed remotely.

REFERENCES

[1] D. Evans, “The Internet of Things How the Next Evolution of the Internet Is Changing Everything", “Cisco Internet Business Solutions Group (IBSG)”, white paper, 2011, retrieved on May 2, 2014 from https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[2] L. Piccini et al., "Wireless DSP architecture for biosignals recording", December 2004, Volume 18 Issue 21 pages 487-490

[3] Huimin She et ai., "A Network-based System Architecture for Remote Medical Applications", Dept. of Electronic, Computer and Software Systems, Royal Institute of Technology, Sweden, ASIC & System State Key Lab., Dept. of Microelectronics, Fudan Univ., Shanghai, China, 2007.

[4] Benny P.L. Lo et al., "Body sensor network – A wireless sensor platform for pervasive healthcare monitoring", Adjunct Proceedings of the 3rd International conference on Pervasive Computing (PERVASIVE'05), May 2005, pages 77-80

[5] R.S .H. Istepanian et al., “The Potential of Internet of m-health Things “m-IoT” for Non-Invasive Glucose level Sensing". In proceeding of IEEE, 2011 pages 5264-5266

[6] Christos Tachtatzis et al., "An Energy Analysis of IEEE 802.15.6 Scheduled Access Modes for Medical Applications", D. Simplot-Ryl et al. (Eds.): ADHOCNETS 2011, LNICST 89, pp. 209–222.

[7] Zigduino r2 , retrieved on Jul 17 2014 from http://www.logos-electro.com/store/zigduino-r2

[8] ADS1192 Demonstration Kit, retrieved on Jul 17 2014 from http://www.ti.com/tool/ads1192ecg-fe

[9] RTX41xx Low Power Modules, retrieved on Jul 17 2014 from http://www.rtx.dk/RTX41xx_Modules-4024.aspx

[10] Wireless Connectivity for Medical Applications, retrieved on June 12 2014, from http://www.arrownac.com/events-training/training/pdfs/wireless.pdf

[11] ZigBee and Wireless Radio Frequency Coexistence, retrieved on Jun 12 2014 from https://docs.zigbee.org/zigbee-docs/dcn/07-5219.PDF

[12] Coping with Wi-Fi's biggest problem: interference, retrieved on Jun 12 2014 from http://www.networkworld.com/article/2215287/tech-primers/coping-with-wi-fi-s-biggest-problem--interference.html

[13] Jin-Shyan Lee et al., "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee , and Wi-Fi", In proceeding Industrial Electronics Society, 2007. IECON, IEEE, 2007, Pages 46-51

[14] Kartik Rathod et al., "Wireless automation using ZigBee protocols ", published in Wireless and Optical Communications Networks (WOCN),2012,pages 1-5

[15] D. Miorandi et al., "Internet of things: Vision, applications and research challenges", Ad Hoc Networks, Sep 2012, Volume 10 Issue 7, pages 1497-1516

Publication II

An Elliptic Curve-based Mutual Authentication Scheme for RFID Implant Systems

Sanaz Rahimi Moosavi, Ethiopia Nigussie, Seppo Virtanen, Jouni Isoaho

Original published in Elsevier International Conference on International Conference on Ambient Systems, Networks and Technologies (ANT-2014), 2014, pages 198-206, Belgium.

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 32 (2014) 198 – 206

Procedia
Computer Science

5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014)

An Elliptic Curve-based Mutual Authentication Scheme for RFID Implant Systems

Sanaz Rahimi Moosavi*, Ethiopia Nigussie, Seppo Virtanen, Jouni Isoaho

Department of Information Technology, University of Turku, 20014 Turku, Finland

Abstract

In this paper, a secure mutual authentication scheme for an RFID implant system is developed. An insecure communication channel between a tag and a reader makes the RFID implant system vulnerable to attacks and endangers the user's safety and privacy. The proposed scheme relies on elliptic curve cryptography and the D-Quark lightweight hash design. Compared to the available public-key cryptosystems, elliptic curve-based cryptosystems are the best choice due to their small key sizes as well as their efficiency in computations. The D-Quark lightweight hash design is tailored for resource constrained pervasive devices, cost, and performance. The security analysis of the proposed authentication scheme revealed that it is secure against the relevant threat models and provides a higher security level than related work found in the literature. The computational performance comparison shows that our work has 48% less communication overhead compared to existing similar schemes. It also requires 24% less total memory than the other approaches. The required computational time of our scheme is generally similar to other existing schemes. Hence, the presented scheme is a well-suited choice for providing security for the resource-constrained RFID implant systems.

Keywords: RFID implant system; IoT; security; healthcare; authentication and identification; elliptic curve cryptography

1. Introduction

Internet of Things (IoT) is emerging as an attractive future networking paradigm. The new generation of Internet is an IPv6 network interconnecting traditional computers and a large number of smart objects or networks. IoT consists of smart objects and low-power networks such as Wireless Sensor Networks (WSNs)[1], Radio Frequency Identification (RFID) networks[2], Body Area Networks (BANs)[3], and actuators. IoT provides an integration approach for all physical objects that contain embedded technology to be coherently connected and enables them to communicate, sense and interact with the physical world. Thus, information of any object or service will be accessible in a systematic way. This results in the generation of enormous amounts of data which have to be stored, communicated, processed and presented in a seamless, secure, and easily interoperable manner. IoT has many potential applications in our everyday life: a smart home where no energy is wasted, productive businesses where offices turn into smart and interactive environments and factories transmit production-related information in real-time, and a proactive healthcare system

* Corresponding author. Tel.: +3-582-333-8647.
E-mail address: saramo@utu.fi

doi:10.1016/j.procs.2014.05.415

that reduces costs without compromising the quality of health services. In the near future, most of the population will benefit from the BANs. The combination of ”things” such as sensors, wireless radio, RFIDs and 6LoWPAN[1] will enhance monitoring methods and measurements of vital functions such as temperature, blood pressure, heart rate, cholesterol levels and blood glucose. IoT services and applications will also have a great impact on independent living of elderly population by detecting their chronic diseases and activities of daily living using wearable and ambient sensors.

An RFID implant system is one of the components of IoT-based healthcare solutions. It can be introduced into the human's body in order to store health and medical records that can save a patient's life in emergency situations. In such a system, the identification process can be done completely automatically and there is no need to type, confirm or remember passwords. People who suffer from cancer, diabetes, coronary heart disease, cognitive impairments, seizure disorders and Alzheimer's are the best choice to benefit from the RFID implant system. It was approved by the U.S. Food and Drug Administration (FDA) in 2004 for clinical use[4]. VeriMed, the commercial application of VeriChip RFID implants, has been designed to be used for patient identification in healthcare. An RFID Implant system, consists of three components: *Implantable RFID Tags*, *RFID Reader(s)*, and *Back-end Database Server*. Implantable RFID Tags are medical devices embedded into a human body through a surgical procedure. The commercial implantable tags used for patients are passive tags, they do not need any built-in battery and their operation relies on energy that is emitted by an external RFID reader. As these tags do not have any moving parts, once implanted they can remain activated for more than 10 years[4]. An RFID Reader communicates with the implantable RFID tags and the back-end database server. In an RFID implant system, the reader runs queries to the tags. The essential information associated to the owner of the tag is kept in a back-end database server for the subsequent utilization.

The communication channel between the tag and the reader is insecure and our goal is to make this channel secure. Security is a major concern wherever networks are deployed at large scale. Due to direct involvement of humans in IoT healthcare, providing robust and secure data communication among healthcare sensors, caregivers and patients carrying RFID tags are crucial. Whether the data gathered from patients or individuals are obtained with the consent of the person or without it due to the need by the system, misuse or privacy concerns may restrict people from taking advantage of the full benefits from the system. An RFID implant system in healthcare is a resource-constrained system and it requires efficient and optimized security solutions where the data concerning the patients is secured with Confidentiality, Integrity, and Authentication (CIA). Without strong security foundations, attacks and malfunctions in the RFID implant system will outweigh any of its benefits. Conventional security and protection mechanisms including existing cryptographic solutions and privacy assurance methods that have been proposed to the RFID systems in general, cannot be re-used. This is because of resource constraints, different security level requirements, and the system architecture of an RFID implant system. Thus, an RFID implant system requires a robust, optimized, and lightweight security framework to fulfill the security level requirement and hardware footprint constraints efficiently.

In this paper, we propose a secure elliptic curve-based mutual authentication scheme for RFID implant systems that can be used in healthcare applications. Compared to related work proposed for RFID systems in general, our proposed scheme is more efficient in terms of communication overhead and memory requirement while offering higher level of security. In previous work[4], we have discussed that the hardware footprint, power consumption limitations, and security level requirements of RFID implant systems are different from mainstream applications of RFID due to the delicate use cases and safety-critical specifications. Thus, security solutions being proposed in this regard must be optimized based on characteristic restrictions and requirements of RFID implant systems.

The remainder of this paper is organized as follows: Section 2 provides an overview of related work. Section 3 discusses the security requirements and threat models of RFID implant systems. Section 4 presents our proposed ECC-based mutual authentication scheme to the RFID implant systems. Section 5 provides a comprehensive security and computational performance analysis of our scheme. In this section, the comparison of this work with similar existing approaches is also presented. Finally, Section 6 concludes the paper.

2. Related Work

Several communication security schemes, either ECC-based or non ECC-based, have been proposed in literature to solve security and privacy issues in RFID systems. In this section, we examine some of the existing ECC-based security schemes for RFID systems since our proposed authentication scheme also relies on ECC.

In 2006, Tuyls *et al.*[5] proposed an ECC-based RFID identification scheme using the Schnorr identification protocol. They claimed that their scheme can resist against tag counterfeiting. However, in 2008 Lee *et al.*[6] presented that this scheme suffers from the location tracking attack as well as forward security. In such a scheme when an adversary can compute the public key $X(= -t.P)$ of a tag, it can benefit from X in order to get access to other information related to the tag. Lack of scalability is another problem of the Tuyls *et al.*'s scheme. This is because at each time a tag needs to be identified, the reader should fetch the tag's public key from the database server to verify it. This means that the reader requires to perform linear search to identify each tag. By doing so, considerable computational cost will be imposed to the whole system.

In 2007, Batina *et al.*[7] proposed an ECC-based RFID identification scheme based on Okamoto's authentication algorithm. Although they claimed that their scheme can resist against active attacks, in 2008, Lee *et al.*[8] asserted that this scheme suffers from tracking as well as a forward secrecy problem. Lee *et al.* in 2010[6], proposed an ECC-based RFID authentication scheme in order to address the existing tracking problems in[5] and[7]. Nevertheless, in the mentioned schemes, the authors merely consider tag to reader identification, excluding reader to tag authentication[9]. This causes tags to reply to any malicious query being sent by an adversary. The major reason is that tags are not capable of confirming to whom they are talking to. In 2011, Zhang *et al.*[10] proposed an ECC-based randomized key scheme in order to improve Tuyls *et al.*'s and Lee *et al.*'s schemes. Although their scheme is secure against relevant attacks concerning the RFID systems, it still not capable of performing mutual authentication. In 2013, Liao *et al.*[9] proposed a secure ECC-based authentication scheme integrated with ID-verifier transfer protocol. Similar to Zhang *et al.*'s work, Lial *et al.*'s scheme achieves the required security level of RFID systems. However, their tag identification scheme lacks performance efficiency in terms of the tag's computation time and its memory requirement.

Based on the above-mentioned weaknesses and vulnerabilities, we believe that there still is lack of secure and efficient authentication scheme for RFID implant systems. In addition, hardware footprint and power consumption limitations and security level requirements of RFID implant systems differ from mainstream applications of RFID due to the safety-critical specifications and delicate use cases.

3. Security Requirements and Threat Models of RFID Implant Systems

Security requirements and threat models of RFID implant systems in healthcare will be discussed in this section. First, we present the security requirements of RFID implant systems and then we introduce the most relevant threat and attack models.

3.1. Security Requirements

When designing an authentication scheme, the security requirements of an RFID implant system need to be well defined. The security requirements can be defined in terms of mutual authentication, confidentiality, integrity, availability, and forward security.

Mutual Authentication: mutual authentication is a scheme where both sides, a tag and a reader, authenticate each other. Unlike the most common authentication schemes, where just a party authenticates another party, mutual authentication is critical if each of the parties is involved in a communication. Without having mutual authentication in an RFID system, either of the parties can falsify their identities.

Confidentiality: all of the secret information concerning the RFID implant system are securely transmitted during all communications. To ensure the confidentiality, one of the two parties, either the tag or the reader, transmit the encrypted information and just the other one can decrypt it.

Data Integrity: the data collected and stored by a device must be protected from tampering by unauthorized parties.

Availability: the device should be resilient to Denial of Service (DoS) attacks, and a malicious entity should not be able to affect the operational capabilities of the device in any way.

Forward Security: The property of forward security ensures that the revelation of the tag's secret information will not threaten the security of previously transmitted information.

3.2. Threat Models

In the following, we sketch some of the most relevant attack models concerning the RFID implant systems.

Unauthorized Location Tracking: such an attack is directed against the privacy of tagged people in order to track their activities. For example, the activity of a person who is implanted with an RFID tag can be tracked by any unauthorized person. This will happen if an adversary pretends to be a trusted component of an RFID implant system. By doing so, the adversary will be able to track an implanted person and access his/her confidential information, or implement a counterfeiting attack to probing the information that he captured from the tag.

Eavesdropping Attack: in an RFID implant system, with an eavesdropping attack the adversary can capture the communications conveyed between the tag and the reader. In this type of attack the adversary does not need to communicate with the RFID tag. He/she only captures the transmitted signals using Radio Frequency (RF) equipment. The information gained by the adversary can be utilized later against the privacy of the implanted users.

Impersonation Attack: to impersonate either a tag or a reader in an RFID implant system. In this system, when there is no authentication scheme to prove that the tag/reader is authentic, it is possible that the adversary implements the impersonation attack against the whole system and utilizes the gained information (e.g. medical history of a patient) in malicious ways. As a result, such a system requires a robust and secure authentication scheme to verify that the tag/reader is valid.

Replay Attack: all messages transmitted between a tag and a reader can be captured and saved by an adversary. Then, he/she can transmit the intercepted information in an attempt to deceive an authorized device and pass the authentication phase. For example, an illegal reader may listen and capture the information transmitted between a tag and an unauthorized reader, and then replay the communication in order to gain the same result that a legal reader and tag can benefit from.

4. The Proposed Authentication Scheme

This section presents an ECC-based mutual authentication scheme that satisfies the security requirements in an RFID implant system. A mutual authentication scheme enables the communicating parties, a tag and a reader, to respectively verify and ensure each other's identity. Later, it will be shown that the proposed communication scheme is secure against several relevant attacks and compared to related work has less communication overhead and requires less memory to perform the authentication.

The proposed scheme consists of three phases: 1. the reader authentication and verification phase, 2. the tag identification phase, and 3. the tag verification phase. In the proposed scheme, we suppose that the communication between the reader and the back-end database server is done through a secure channel, while communication between the RFID implant tag and the reader is not secure. Our proposed ECC-based mutual authentication scheme will provide a secure channel between the tag and the reader in such a way that they can communicate with each other securely and efficiently. Before describing the three mentioned phases, in Definition 1, we first introduce parameters and notations used in our proposed scheme.

4.1. Reader Authentication and Verification (Phase 1)

The reader authentication and verification phase of our proposed scheme relies on Elliptic Curve Discrete Logarithm Problem (ECDLP)[11]. In this phase, the reader chooses a random number $r_1 \in Z_n$ and computes $R_1 = r_1.P$ as its public key. Next, it initializes its counter value i_1 to one and sends both R_1 and i_1 to the tag. It then increments the value i_1 by r_1. Upon receiving the message, the tag checks whether i_2 (which is initialized to zero) is greater than i_1. If the condition holds, it replaces i_2 by i_1 and selects a random number $r_2 \in Z_n$. Then, the tag computes $r_3 = X(r_2.P) * Y(R_1)$ where * is a non-algebraic operation over the abscissa of $(r_2.P)$ and the ordinate of R_1 (This operation can be either modular addition if the field is binary or a bitwise *xor* if the field is prime) and it sends the value r_3 to the reader. After receiving r_3, the reader computes $R_2 = r_1.ID_t + r_3.s_3$ and sends the value R_2 to the tag.

Definition 1 Parameters and Notations Used in This Work

G : a group of order q on an elliptic curve having the order n,

P : a primitive element or the base point of G,

s_1 , s_2: each tag keeps two secret points s_1 , s_2 $\in E(F_g)$, which will change over time. These secret points will be varied each time the tag is successfully identified,

ID_t : the tag's identification number or ID,

s_3 : each reader keeps a secret point $s_3 \in Z_n$, which will change over time. This secret point will be varied each time the reader is successfully authenticated,

$ID_r = s_3.P$: the reader's public key,

r_s, i_1, i_2 : random numbers in Z_n,

h : a lightweight hash function,

(d, c) : a signature generated by the tag during its identification phase,

Algorithm 1 Pseudo-code of Reader Authentication and Verification

Inputs: (r_1, R_1): The private key and the public key of the reader. i_1: The reader's counter value.

Output: Determine whether the reader authentic or not?

Body:

```
$i_1 \leftarrow 1$;
for $i = 1$ to $n - 1$ do
    $r_1 \leftarrow i$;
    $R_1 \leftarrow r_1.P$;
    $i_1 \leftarrow i_1 + r_1$;
end for
send $R_1$ to the tag;
for $j = 1$ to $n - 1$ do
    if $i_1 \geq i_2$ then
        $i_2 \leftarrow i_1$;
        $r_3 \leftarrow X(r_2.P) * Y(R_1)$;
    end if
end for
Tag send $r_3$ to the reader;
Reader computes $R_2 \leftarrow r_1.ID_t + r_3.s_3$ and sends the value
  $R_2$ to the tag;
if $(R_2 - r_1.ID_t)r_3^{-1}.P = ID_r$ then
    return Success;
end if
```

Finally, the tag checks whether $(R_2 - r_1.ID_t)r_3^{-1}.P = ID_r$ holds. Then, the tag verifies that the reader is authentic. Algorithm 1 shows how the authentication and verification of the reader is done in this scheme.

4.2. Tag Identification (Phase 2)

Both the tag identification and the tag verification phases of our proposed scheme rely on Elliptic Curve Digital Signature Algorithm (ECDSA)[11] using Quark lightweight hash design. Quark is one of the most recent lightweight hash designs and it was first proposed by Aumasson *et al.* in 2013[12]. The design of Quark lightweight hash relies on non-linear Boolean functions and bit shift registers. Therefore, not only its implementation becomes feasible, but also, the circuit area requirements of this hash design are well suited for implantable medical devices. In addition, a digital signature offers identification along with integrity and non-repudiation. In our previous work, we stated that due to the resource limitations and the delicate use cases of the RFID implant systems, the need for lightweight cryptographic hash designs has to be carefully considered. That is the reason why in our proposed ECC-based tag identification algorithm, we utilized the D-Quark (one of the flavors of Quark) lightweight hash design rather than the general purpose hash designs (e.g. SHA-1[13] and SHA-3[14])[15].

In the tag identification phase of our proposed scheme, the tag's initial secret point is $s_1 \in E(F_g)$ from which the next secret point s_2 and ID_t will be computed. To generate the second secret point, the tag computes $s_2 = f(X(s_1)).P$. Obtaining the first secret point from the second is difficult, as it requires the computation of an elliptic discrete logarithm. Since the second key is generated from the second key, our scheme provides forward security.

For the sake of efficiency, the function f should be selected in a manner that avoids large Hamming weights for s_2, assuring that the computation of $s_2.P$ will be fast without compromising security[16]. Once the generation of the second secret point s_2 is done, the tag selects a random integer $k \in Z_g$ and computes a curve point $(x, y) = k.G$. In order to send its digital signed message (d, c) to the reader, the tag computes $d = x \bmod n$. If $d = 0$, the tag starts to select another random number $k \in Z_g$ and computes the next curve point. The tag computes its $ID_t = Mb(X(s_1)) * Mb(X(s_2)).P$ where Mb will output some middle bits of the input values. The operand * is a non-algebraic operation $\in F_g$ done over the abscissa of the first and the second secret points (This operation is modular addition as the field is binary). Then, the tag computes $c = k(hash(ID_t) + X(s_1).d)$. Here again, if the computed $c = 0$, the tag will start the algorithm by selecting another random integer k. Finally, the tag sends the computed values (d, c) and (ID_t) to the reader. Algorithm 2 shows the pseudo-code of the tag identification phase of the proposed scheme.

4.3. Tag Verification (Phase 3)

In this phase, in order to verify the tag is authentic the reader selects a random integer $r_s \in Z_n$ and it computes its public key $p_r = r_s.P$. for $j \in [1, n - 1]$, the reader checks whether $d, c \in Z_n$. If the result is valid, the reader calculates

Algorithm 2 Pseudo-code of Tag Identification

Inputs: $r_s \in Z_n$: a random integer (sent from the reader's side) and a hello request. s_1: tag's first secret point.

Output: ID_t: Tag's *ID* and (d, c): the tag's digital signature.

Body:

```
1: The tag checks:
2: if $r_s \neq 0$ then
3:     $s_2 = f(X(s_1)).P$;
4:     for $i = 1$ to $n - 1$ do
5:         The tag selects a random integer $k$ and computes the curve point $(x, y) = k.G$;
6:         The tag computes $d = x \bmod n$;
7:         if $d = 0$ then
               goto 3;
8:         end if
9:         The tag computes the value of its ID as: $ID_t = (Mb(X(s_1)) * Mb(X(s_2))).P$;
10:        Then, the tag computes: $c = k.(Hash(ID_t) + X(s_1) * d) \bmod n$;
11:        if $c = 0$ then
               goto 3;
12:        end if
13:        send $ID_t, (d, c)$ to the reader;
14:    end for
15: end if
```

Algorithm 3 Pseudo-code of Tag Verification

Inputs: ID_t: The tag's *ID* and (d, c): the tag's digital signature.

Output: Determine whether the tag is authentic or not?

Body:

```
for $j = 1$ to $n - 1$ do
    if $d, c \in [1, n - 1]$ then
        $h = Hash(ID_t)$;
        $z$= left most bit of $h$;
        $w = c^{-1} \bmod n$;
        $u_1 = zw \bmod n$;
        $u_2 = dw \bmod n$;
        curve point $(x, y) = u_1.P + p_r$;
    end if
end for
if $r = x \bmod n$ then
    return Success;
end if
```

$h = Hash(ID_t)$, where Hash is the same Quark lightweight hash function that is used in the previous phase to generate the tag's signature. Once the hash value of (ID_t) is computed, the reader selects the leftmost bit of h and denotes it as z. Then, the reader calculates the values w, u_1, u_2 exactly as shown in Algorithm 3. Based on the calculated values, the reader computes the curve point $(x, y) = u_1.P + p_r$. Finally, the reader will accept the tag's signature as a valid one if the equation $r = x \bmod n$ holds.

5. Security and Computational Performance Analysis of The Proposed Authentication Scheme

In this section, we will analyze the security and performance of the proposed scheme in order to verify whether the essential requirements have been satisfied.

5.1. Security Analysis

In the following, we analyze our proposed scheme against some of the most relevant attacks. As it is mentioned in section 4, we assume that the communication between the reader and the back-end database server is done through a secure channel, while communication between the implantable tag and the reader is not secure.

Mutual Authentication: in the reader authentication phase of our proposed scheme, to verify that the reader is legal, the tag computes whether $(R_2 - r_1.ID_t)r_3^{-1}.P = ID_r$. Conversely, to verify whether the tag is authentic (based on its transmitted (ID_t) and the digital signed message), the reader checks if $r = x \bmod n$ holds. This is how mutual authentication is achieved in our proposed scheme.

Availability: in our scheme, since the tag and the reader change their secret points s_1, s_2, and s_3 once they are successfully authenticated, it is not possible that an adversary performs a denial of service attack.

Forward Security: in our scheme, if an adversary tries to decrypt some of the information that he has eavesdropped, for example the tag's second secret key s_2, he/she will not benefit from the gained information. Obtaining the first secret key from the second one will require a solution to the ECDSA, which is not easily possible.

Unauthorized Tracking of The Tag: In our proposed scheme, the only public information concerning the tag is its *ID*. In the tag identification phase, it was shown that the value of the tag's *ID* results from the product of a non-algebraic operation done over some middle bits of the abscissa of the first and second secret keys of the tag. As a result, it is impossible to compute and obtain the tag's secret keys from its current *ID*. The main reason is that obtaining the secret points implies the computation of the elliptic curve discrete logarithm problem. Since solving the discrete logarithm problem is as hard as the integer factorization problem, this problem cannot be solved effortlessly. Thus far, there has not been any polynomial time algorithm proposed to solve discrete logarithm problems.

Table 1. Security properties comparison with the available ECC-based designs.

	Batina et al.[7]	Zhang et al.[10]	Liao et al.[9]	Lee et al.[6]	This work
Tracking of the tag	No	Yes	Yes	Yes	Yes
Eavesdropping attack	Yes	Yes	Yes	Yes	Yes
Impersonation attack	No	Yes	Yes	Yes	Yes
Replay attack	Yes	Yes	Yes	Yes	Yes
Forward security	No	Yes	Yes	Yes	Yes
Anonymity	No	Yes	Yes	No	Yes
Mutual authentication	No	No	Yes	No	Yes
Availability	Yes	Yes	Yes	Yes	Yes

Eavesdropping Attack: In our scheme, from one hand, in the tag identification phase, if an adversary tries to guess the tag's secrets s_1 and s_2, the only public information concerning it is *ID*. As it was discussed earlier, the bits of the tag's *ID* result from a non-algebraic operation done over some middle bits of the abscissa of two different secret points s_1 and s_2. Thus, it is computationally unfeasible to obtain the secret from its *ID*. On the other hand, in the digital signature generation section, if an adversary could guess the value d, it cannot obtain the value c effortlessly. This value is also generated from a non-algebraic operation done over the abscissa of the secret point s_1 and the value d. The gained result will be added to the hash value of ID_t and multiplied by a random number k. Such an operation cannot be easily computed by an adversary as it requires to compute the discrete logarithm problem that is not computationally feasible. For the same reason, in the reader authentication phase, even if an adversary could guess one of the values R_1 or R_2 or r_3, he/she still cannot easily obtain other secure information related to the reader. Based on the discussion above, the adversary also cannot implement any *Replay Attack*.

Impersonation Attack: concerning this type of attack, we consider two different scenarios:

- *Impersonation of the reader*: here, if an adversary tries to impersonate the reader, he/she will fail. This is because if the attacker tries to impersonate as a fake reader to the tag, he/she must compute R_1 and at the same time try to guess the value r_2 (which is not easily feasible). Nevertheless, without the reader's computed value $R_2 = r_1.ID_t + r_3.s_1$, the adversary (fake reader) cannot compute $(R_2 - r_1.ID_t)r_3^{-1}.P = ID_r$ to verify whether the reader is authentic.
- *Impersonation of the tag*: in order to impersonate the tag of our proposed scheme, an adversary needs to have an access to the tag's secrets s_1 and s_2 and as it was presented earlier in this section, the values of the secret keys cannot be acquired from the public information of the system ID_t.

Based on the discussion above, our proposed scheme is secure and robust against relevant attacks related to RFID systems. The security properties comparison of our proposed scheme and other ECC-based related works is presented in Table 1. In the table, the term "Yes" states that the available ECC-based designs are secure against the above-mentioned attacks. "No" indicates that those ECC-based designs are not robust and secure against the specified attacks and the threats models. From the security point of view, as the table shows, Lee *et al.*'s and Zhang *et al.*'s schemes have almost the same properties against different types of attacks. Nevertheless, their major disadvantage is that they do not have any security solution for mutual authentication. Although the security properties of our scheme are similar to Liao *et al.*'s scheme, in the next section we will show that our scheme provides better efficiency in terms of computational cost, total memory required, and communication overhead.

5.2. Computational Performance Analysis

As it was presented earlier, implantable tags are resource-constrained pervasive devices. They are tiny in terms of size and computational capacity. Hence, it is important to analyze the performance of the authentication scheme to ensure that the overhead is minimal. Such an analysis can be done based on various criteria including computational cost, memory requirements, and communication overhead. In this work, we mainly focus on the performance analysis of implantable tags since RFID readers are known to be robust devices[9].

As a common cryptographic primitive, we utilize standardized 163-bit elliptic curve domain parameters recommended by National Institute of Standard and Technology (NIST). The parameters are defined over the binary finite field F(2^{163}). We utilize ECDSA algorithm having the coordinate (x, y). As a reminder, the elliptic curve domain parameters over F(2^m) are specified by the tuple $T = (m, f(x), a, b, G, n, h)$ where $m = 163$ and the representation of F(2^{163}) is defined by, $f(x) = x^{163} + x^7 + x^6 + x^3 + 1$[11]. In their work, Godor *et al.*[17] measured the **computational time** required for scalar multiplication of 163-bit point elliptic curve, the SHA-1 hash function[13], and the Advanced Encryption Standard (AES)[18] algorithm. As an environment to measure the computational time for the mentioned cryptography algorithms, they used an Intel Core2 CPU T5500 1.66 GHz having 1GB RAM. Based on the results deduced from their work, at the frequency of 5 MHz, the computational time required to compute the scalar multiplication of 163-bit point elliptic curve is 64 ms[19].

Kumar *et al.*[20] presented that in High Frequencies (HF) such as 13.56 MHz, which is normally the frequency used in most RFID applications (e.g. smart cards, access control and libraries), the scalar multiplication of 163-bit point elliptic curve is done in 31.8 ms. Nevertheless, such a frequency and other higher frequencies have not been approved by the U.S. Food and Drug Administration (FDA) neither for Implantable Medical Device (IMD) applications nor human identification purposes[4]. In Low Frequencies (LF) such as 323 KHz, 243 ms computational time is needed for completing the scalar multiplication, which is too long compared to 64 ms. Hence, we evaluate the performance of our proposed ECC-based scheme at 5 MHz frequency. In addition to reducing the computation time, this allow us to make a fair comparison with related work and also to take into account the restriction of the FDA.

In our proposed scheme, we outline the **storage requirement** by considering the tag's memory including its public key and private key. The private key is denoted as the tag's secret keys s_1 and s_2 and the public key is the tag's public key ID_t. In the proposed scheme, the required memory consists of (ID_t, s_1, s_2) where the ID_t needs 163 bits memory and s_1 and s_2 together require 326 bits memory. So the total required memory is: 62 bytes= 163 bits + 326 bits. Table 2 presents the performance comparison of our proposed tag identification scheme with related work.

The computational cost of our proposed tag identification algorithm includes three scalar points and it is computed as: (64 ms * 3 = 192 ms). Thus, our tag identification algorithm requires 192 ms to compute the multiplication of the three scalar points of the scheme. As Table 2 presents, when the number of ECC scalar point multiplication (ECm) increases, it will have a direct impact to the time required to do this multiplication. Hence, in real-time systems, the system will require considerable time until the authentication is performed successfully.

Table 2. Performance comparison with the available ECC-based designs.

	Batina et al.[7]	Zhang et al.[10]	Liao et al.[9]	Lee et al.[6]	This work
Communication-overhead	82	82	82	82	42
(ECm,hash)	(2,0)	(3,0)	(5,0)	(3,0)	(3,1)
Public-key memory	41	41	61	41	21
Private-key memory	41	41	41	41	41
Total memory (byte)	82	82	102	82	62
Computational time (ms)	128	192	320	192	192

To evaluate the **communication overhead** of our algorithm, the information that is transmitted between the tag and the reader during the tag identification phase needs to be considered. Hence, in our scheme we evaluated the value of communication overhead based on the messages $ID_t, (d, c)$ exchanged between the tag and the reader in the mentioned phase. Here, the overhead is 42 bytes and it is evaluated as: (163 * 2 = 326/8 bytes).

The communication overhead of the proposed elliptic curve-based mutual authentication scheme is compared with the other schemes. The proposed scheme achieves 48% reduction in communication overhead compared to the Batina *et al.*'s, the Zhang *et al.*'s, the Liao *et al.*'s and the Lee *et al.*'s schemes, respectively. In case of total memory, it requires 24% less memory than the Batina *et al.*'s, the Zhang *et al.*'s and the Lee *et al.*'s schemes. Compared to Liao *et al.*'s scheme, the proposed scheme requires 39% less storage. Our proposed scheme needs the same amount of computation time as Zhang *et al.*'s and the Lee *et al.*'s to perform the authentication between the tag and the reader. Compared to Liao *et al.*'s scheme, the computational time of the proposed scheme reduces by 60%. However, the computation time increases by 50% compared to Batina *et al.*'s scheme.

6. Conclusion

In this paper, we presented a novel secure elliptic curve-based mutual authentication scheme for RFID implant systems. To the best of our knowledge, previously proposed elliptic curve-based authentication schemes, concerning RFID systems in general, cannot fully fulfill the essential security and performance requirements of RFID implant systems. Most of the earlier proposed solutions were not secure against the most relevant attacks of the RFID systems or they were not capable of performing mutual authentication between a tag and a reader. The proposed mutual authentication scheme relies on elliptic curve cryptography. An elliptic curve cryptosystem is more efficient in terms of key sizes and required computations than conventional public key cryptosystems. In the proposed scheme, reader authentication and verification is performed based on ECDLP. While tag identification and tag verification phases rely on ECDSA using Quark lightweight hash. We proved that our proposed scheme is secure against the relevant attacks and also ensures a higher security level than related work found in the literature. In addition, we carried out computational performance analysis of our proposed scheme and the analysis results show that our elliptic curve-based mutual authentication scheme has 48% less communication overhead than similar available schemes. It also requires 24-39% less total memory than the compared existing schemes. Based on the results presented in this paper, we conclude that the proposed scheme has the appropriate features for use in RFID implant systems. We believe that our scheme is not just limited to RFID implant systems, it can also be applied to any application of IoT that requires secure and efficient authentication.

References

1. G. Pottie. Wireless Sensor Networks. In *Information Theory Workshop*, pages 139–140, 1998.
2. C. Roberts. Radio frequency identification (RFID). *Journal of Computers and Security*, 25:18–26, 2006.
3. L. Huan-Bang, K. Takizawa, Z. Bin, and R. Kohno. Body Area Network and Its Standardization at IEEE 802.15.MBAN. In *Mobile and Wireless Communications Summit*, pages 1–5, 2007.
4. N. Gasson, E. Kosta, and D. Bowman. Technical Challenges of Human ICT Implants. In *Human ICT Implants: Technical, Legal and Ethical Considerations*, pages 55–63, 2012.
5. P. Tuyls and L. Batina. RFID-tags for Anti-Counterfeiting. In *Topics in Cryptology*, pages 115–131. Springer Verlag, 2006.
6. Y. Lee, L. Batina, D. Singele, B. Preneel, and I. Verbauwhede. Anti-counterfeiting, Untraceability and Other Security Challenges for RFID. In *Towards Hardware-Intrinsic Security*, pages 237–257. Springer, 2010.
7. L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. Public-Key Cryptography for RFID-Tags. In *Pervasive Computing and Communications Workshops*, pages 217–222, 2007.
8. K. Yong, L. Batina, and I. Verbauwhede. EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol. In *RFID, 2008 IEEE International Conference on*, pages 97–104, 2008.
9. Yi-Pin Liao and Chih-Ming Hsiao. A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. *Ad Hoc Networks*, 2013.
10. Xinglei Zhang, Jianhua Li, Yue Wu, and Quanhai Zhang. An ECDLP-Based Randomized Key RFID Authentication Protocol. In *Network Computing and Information Security (NCIS), 2011 International Conference on*, volume 2, pages 146–149, 2011.
11. N. Koblitz. Elliptic Curve Cryptosystems. *Journal of American Mathematical Society*, 48:203–209, 1987.
12. J. Aumasson, L. Henzen, W. Meier, J. Miret, and M. Plasencia. Quark: A Lightweight Hash. *Journal of Cryptography*, 26(2):313–339, 2013.
13. R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Journal of Association for Computing Machinery*, 21(2):120–126, 1978.
14. E. Kavun and T. Yalcin. A Lightweight Implementation of Keccak Hash Function for Radio-Frequency Identification Applications. In *Radio Frequency Identification: Security and Privacy Issues*, volume 6370, pages 258–269, 2010.
15. S. Rahimi, A. Hakkala, J. Isoaho, S. Virtanen, and J. Isoaho. Specification Analysis for Secure RFID Implant Systems. *Journal of Computer Theory and Engineering*, 6(2):177–189, 2014.
16. S. Martinez, M. valls, C. Roing, J. Miret, and F. Gine. A Secure Elliptic Curve-Based RFID Protocol. *Journal of Computer Science and Technology*, 24(2):309–318, 2009.
17. G. Godor and S. Imre. Elliptic curve cryptography based authentication protocol for low-cost RFID tags. In *RFID-Technologies and Applications (RFID-TA), 2011 IEEE International Conference on*, pages 386–393, 2011.
18. J. Daemen and V. Rijmen. Specication of Rijndael. In *The Design of Rijndael*, volume 17, pages 31–50, 2002.
19. G. Godor, M. Antal, and S. Imre. Mutual Authentication Protocol for Low Computational Capacity RFID Systems. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–5, 2008.
20. S. Kumar and C. Paar. Are standards compliant elliptic curve cryptosystems feasible on rfid? In *In Proc. of RFIDSec06*, 2006.

Publication III

Low-latency Approach for Secure ECG Feature Based Cryptographic Key Generation

Sanaz Rahimi Moosavi, Ethiopia Nigussie, Marco Levorato, Seppo Virtanen, Jouni Isoaho

Original published in IEEE Access Journal, 2017,pages 428- 442

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 20, 2017, accepted October 16, 2017, date of publication October 31, 2017,
date of current version February 14, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2766523

Low-Latency Approach for Secure ECG Feature Based Cryptographic Key Generation

SANAZ RAHIMI MOOSAVI[1], (Student Member, IEEE), ETHIOPIA NIGUSSIE[1], (Senior Member, IEEE), MARCO LEVORATO[2], (Member, IEEE), SEPPO VIRTANEN[1], (Senior Member, IEEE), AND JOUNI ISOAHO[1]

[1]Department of Future Technologies, University of Turku, 20500 Turku, Finland
[2]Department of Computer Science, University of California at Irvine, Irvine, CA 92697, USA

Corresponding author: Sanaz Rahimi Moosavi (saramo@utu.fi)

ABSTRACT We propose a low-latency approach for generating secure electrocardiogram (ECG) feature-based cryptographic keys. This is done by taking advantage of the uniqueness and randomness properties of ECG's main features. This approach achieves a low-latency since the key generation relies on four reference-free ECG's main features that can be acquired in short time. We call the approach several ECG features (SEF)-based cryptographic key generation. SEF consists of: 1) detecting the arrival time of ECG's fiducial points using Daubechies wavelet transform to compute ECG's main features accordingly; 2) using a dynamic technique to specify the optimum number of bits that can be extracted from each main ECG feature, comprising of PR, RR, PP, QT, and ST intervals; 3) generating cryptographic keys by exploiting the above-mentioned ECG features; and 4) consolidating and strengthening the SEF approach with cryptographically secure pseudo-random number generators. Fibonacci linear feedback shift register and advanced encryption standard algorithms are implemented as the pseudo-random number generator to enhance the security level of the generated cryptographic keys. Our approach is applied to 239 subjects' ECG signals comprising of normal sinus rhythm, arrhythmia, atrial fibrillation, and myocardial infraction. The security analyses of the proposed approach are carried out in terms of distinctiveness, test of randomness, temporal variance, and using National Institute of Standards and Technology benchmark. The analyses reveal that the normal ECG rhythms have slightly better randomness compared with the abnormal ones. The analyses also show that the strengthened SEF key generation approach provides a higher security level in comparison to existing approaches that rely only on singleton ECG features. For the normal ECG rhythms, the SEF approach has in average the entropy of about 0.98 while cryptographic keys which are generated utilizing the strengthened SEF approach offer the entropy of $\sim$1. The execution time required to generate the cryptographic keys on different processors is also examined. The results reveal that our SEF approach is in average 1.8 times faster than existing key generation approaches which only utilize the inter pulse interval feature of ECG.

INDEX TERMS Cryptographic key generation, electrocardiogram, bio-electrical signal, body area network.

I. INTRODUCTION

Body Area Network (BAN) is one of the main enabling technologies for ubiquitous healthcare systems [1]. It has emerged as a new design to carry out remote patient monitoring efficiently. BAN comprises of medical sensors that obtain, process, manage, transmit, and store patients' health information at all times. Since medical sensor nodes deal with patients' vital health data, securing their communication is an absolute necessity [2]. Without robust security features not only patients' privacy can be breached but also adversaries can potentially manipulate actual health data resulting in inaccurate diagnosis and treatment [3].

Medical sensors rely on cryptography to secure their communications [4]. Proper application of cryptography requires the use of secure keys and key generation methods. Key generation approaches that are proposed for generic wireless sensors are not directly applicable to tiny sensors used in BANs as they are highly resource-constrained and demand a higher security level [5]. Key generation in sensor networks generally requires some form of pre-deployment. Nevertheless, given the constrained nature of medical sensors used in BSNs, conventional key generation approaches may potentially involve reasonable computations as well as latency during network or any subsequent adjustments, due to their need for pre-deployment. Biometrics are generally regarded as the only solution that is lightweight, requires low resources, and indeed can identify authorized subjects in BANs [4], [6]–[8]. By developing robust key generation approaches using biometric systems, the security of medical sensors can be offered in a plug-n-play manner where neither a network establishment nor a key pre-distribution mechanism is required. Cryptographic keys can be generated within the network on the fly through the usage of information collected by medical sensors. Furthermore, key revocation and renewal will be done automatically when and as needed. The choice of a biometric to be used for generating cryptographic keys relies on the capability of medical sensors on extracting an individual's relevant biometric information. The selected feature(s) should also meet the following design goals [4]: (i) *Distinctive*, meaning that it should be different for different subjects at any given time. (ii) *Time-variant*, meaning that it should be different for the same person at different time intervals. (iii) *Random*, meaning that it should be cryptographically random to provide security. A low degree of randomness enables an attacker to acquire a patient's cryptographic key and manipulate their medical data. (iv) *Universal*, meaning that the feature should be measurable from each subject.

Iris, fingerprints, and voice are some physiological features of the body which have the potential to identify individuals with a high degree of assurance. However, these biometric traits are not secure enough to be used for key generation techniques. The reason is that people often leave their fingerprints everywhere, audio recorders can be utilized to deceive speech recognition systems, and iris images can be captured by hidden cameras [1]. Over the last decades, several efforts have been made for the development of the next generation of biometrics known as internal biometrics (also called physiological biometrics or bio-signals) [9]. The main physiological biometrics include electrocardiogram (ECG), electroencephalogram (EEG) [10], and photoplethysmogram (PPG) [11]. From mentioned bio-signals, ECG is the only fiducial-based physiological signal of humans. Fiducials are points of interest (P, Q, R, S, and T waves) that can be extracted from each ECG signal. It has been found that the ECG meets the aforementioned design goals of a biometric trait to be used for cryptographic key generation techniques [4], [7].

Current ECG-based cryptographic keys are mostly generated using Inter Pulse Interval (IPI) feature of an ECG signal [5], [7], [12]–[16]. IPI is measured from two consecutive R peak points where the R peaks are the tallest and most conspicuous peaks in an ECG signal. In [17], we demonstrated that existing IPI-based key generation approaches suffer from a low level of security in terms of distinctiveness, test of randomness, and temporal variance. In this regard, in [17], we presented two different ECG-based cryptographic key generation approaches that offer higher security levels compared to conventional approaches. More precisely, we proposed to integrate Cryptographically Secure Pseudo-Random Number Generators (CSPRNG) along with IPI sequences to generate robust ECG-based cryptographic keys. First, we proposed a strengthened IPI-based key generation approach using a sequence of IPIs and the Fibonacci Linear Feedback Shift Register Pseudo Random Number Generator (LFSR-PRNG), called IPI-PRNG [18]. Second, we proposed an alternative key generation approach that utilized the Advanced Encryption Standard (AES) algorithm [19] and IPI sequences as the seed generator for the AES, called IPI-AES. In IPI-PRNG and IPI-AES approaches, our main focus was to enhance the security of the generated cryptographic keys while realizing a clear trade-off between the security level and key generation execution time.

In this article, we propose a new approach, called Several ECG Feature (SEF) based cryptographic key generation. The SEF approach alleviates the key generation execution overhead of the existing as well as our previous approaches, while preserving the achieved high security levels. The proposed approach is applied to both normal and abnormal ECG signals. The main contributions of this article, which is a major extension of our recent work published in [17], are threefold:

- The SEF approach uses 4 main reference-free[1] features of the ECG signal (being extracted from every ECG heartbeat cycle) along with consecutive IPI sequences to generate ECG-based cryptographic keys.
- To reinforce and enhance the security level of our approach, we consolidate the SEF key generation approach with two different cryptographically secured pseudo random number generators: (i) SEF-PRNG: we strengthened the security level of the SEF approach by exploiting the Fibonacci-LFSR pseudo random number generator (ii) SEF-AES: our SEF approach is also strengthened by utilizing the AES algorithm in counter mode. This technique exploits our SEF key generation approach as the seed generator for the AES algorithm.
- We evaluate the efficiency of our SEF, SEF-PRNG, and SEF-AES approaches by simulations in terms of distinctiveness, test of randomness, temporal variance, and execution time on real ECG data from 239 subjects with different heart health conditions.

The remainder of the paper is organized as follows: in Section II, the related work and motivation are discussed. In Section III, bio-electrical signals and ECG characteristics are discussed. Section IV presents the proposed cryptographic key generation approaches utilizing the ECG bio-electrical signal. Simulation results including distinctiveness, test of randomness, temporal variance, and key generation execution time are provided and discussed in Section V. Finally, Section VI concludes the paper.

II. RELATED WORK AND MOTIVATION

In [20]–[24], fuzzy vault-based bio-cryptographic key generation protocols are proposed for BANs. In each of these protocols, frequency domain characteristics of PPG and ECG signals are used as the physiological parameters. Bao *et al.* [25] presented an entity authentication protocol and a fuzzy commitment-based key distribution protocol, in which the IPI values generated from the PPG signals are

[1] In this context, the reference-free property indicates a dynamic technique in which no ECG fiducial point is fixed as reference.

employed as the physiological parameters. In their work, adaptive segmentation is used to divide the value range of the IPI into segments. The main drawback of the above-mentioned approaches is that they are not applicable enough to be used for generating cryptographic keys for medical sensors. This is due to the required heavy-weight computations. Poon *et al.* [4] and Zhang *et al.* [7] further evaluated the performance of Bao *et al.*'s [25] approach using both PPG and ECG signals with respect to their error rates. In another study by Bao *et al.* [12], another solution is proposed for which physiological parameter generation is utilized in a bio-cryptographic security protocol. The authors claimed that the physiological parameters which are generated utilizing the individual and multi-level IPI sequences have comparable distinctiveness and randomness. Nevertheless, the latency of these approaches is very high as 256 IPIs are required in order to generate a 64 bit cryptographic key.

Altop *et al.* [5] and Xu *et al.* [14] proposed key generation approaches in which the IPI values generated from ECG signals are utilized. In both of these works, the authors employ Gray encoding to map each IPI value to a 4-bit binary number using a uniform quantization method. According to the authors, the generated physiological parameters pass the randomness measurement tests presented by the NIST test benchmark [26]. They also stated that the generated physiological parameters pass both temporal variance and distinctiveness tests. However, in [5] and [14] no related numerical information for experimental performance evaluation in terms of key generation execution time is provided. In addition, compared to our approach, these works have failed to provide as high a security level as our approach in terms of distinctiveness, test of randomness, and temporal variance. Zhang *et al.* [7], Poon *et al.* [4], and Bao *et al.* [12] evaluated the performance of the physiological parameter generation, utilizing both PPG and ECG signals. The authors developed physiological parameter generation techniques which can be utilized in bio-cryptographic key generation approaches. In their work, these authors claimed that physiological parameters generated utilizing IPI sequences offer promising features to be exploited for cryptographic key generation approaches.

Zheng *et al.* [27] proposed a time-domain physiological parameter generation method. They used the time distances between the R peaks as the **reference points** and other peak values of an ECG signal from one heartbeat cycle. The authors claimed that their solution is faster than the conventional IPI-based methods and it ensures the property of randomness. However, their proposed approach lacks reliability as it is only applicable to ECG records collected form subjects with normal ECG rhythm or subjects with no sever cardiovascular diseases. In healthcare systems, subjects often suffer from Cardiovascular Diseases (CVDs) such as Cardiac Arrhythmia, Poor R-wave Progression, Myocardial infraction and Anterior Wall MI in which the R peaks are not easily detectable, or might be even missing within one heartbeat cycle. Choosing the R peak as the reference for calculation all the other features is not always reliable to be used for the binary sequence generations. In addition, as the main focus of the approach present in [27] is on rapid key generation, distinctiveness and temporal variance properties were not analyzed and reported in their approach. In this context, we claim that a robust ECG-based cryptographic key generation approach needs to cover both healthy and unhealthy human subjects. This necessities ECG features selection which is independent of any reference point. In a scenario where one or more fiducial points cannot be detected (due to some abnormalities), the system tries to compute and use as many features as it can collect from the current heartbeat cycle. This will be continued until the next heartbeat cycle(s) that ECG signal becomes normal. When ECG features selection is independent of any reference point, the efficiency and reliability of the ECG-based cryptographic key generation will not be affected.

In [17], our main focus was on the development and analysis of secure and efficient ECG-based cryptographic key generation techniques. We proposed two different ECG-based cryptographic key generation approaches for which the IPI feature of ECG underlays both of the approaches. The aim was to enhance the security of BANs through a robust key generation approach where keys are generated on the fly without requiring key pre-distribution solutions. It was realized that there is a clear trade-off between the security level and the key generation execution time of the proposed ECG-based cryptographic key generation approaches. This article essentially extends our previous work by reducing the key generation execution times yet providing high security levels. Our proposal is motivated by the fact that to alleviate the key generation execution times, while preserving high security levels, other main features of an ECG signal in addition to RR (also known as IPI) can be exploited. In this regard, our proposed approach exploits the main fiducial points of an ECG signal to detect and compute the the main ECG features. The utilized main features include PR, RR, PP, QT, and ST intervals. This is based on the fact these features are highly reliable and ensure the randomness property. For this purpose, we have comprehensively studied the aforementioned main features of most known ECG signals ranging from normal to abnormal ones belonging to patients with various cardiovascular diseases. We have also investigated the property of randomness of the aforementioned features to ensure that they can be used along with IPI for generating cryptographic keys. We hypothesize that, by exploiting additional features, cryptographic keys can be generated faster and in more efficient and reliable manner than those approaches which rely only on singleton IPI sequences and require R peaks as the reference points. Our approach considers both normal and abnormal electrocardiogram signal waveforms.

III. BIO-ELECTRICAL SIGNALS AND ELECTROCARDIOGRAM (ECG) CHARACTERISTICS

A Bio-electrical signal is any signal that can be continuously monitored and measured from any living being's body.

Bio-electrical signals refer to the change in electric current generated by the sum of an electrical potential difference across an organ, a specialized tissue or a cell system. Such signals are low frequency and low amplitude electrical signals that can be measured from biological beings, for instance, humans.

ECG is a rhythmically repeating and quasi-periodical signal which is synchronized by the function of the heart, and the heart performs the generation of bio-electrical events. It is the electrical manifestation of the contractile activity of the heart that is recorded at the chest level by measuring signal levels from several electrical leads attached to the patient's skin. ECG has been mainly employed in various medical applications. For instance, it has been utilized to diagnose cardiac diseases, which are one of the leading causes of death in the world [28]. Over the last few decades, there have been many efforts to develop automatic and computer-based diagnostics of heart failures [6], [21], [29]–[31]. Recently, ECG has been broadly utilized for biometric identification [32]–[35].

ECG signals consist of a series of positive and negative waves. Signals captured from each lead provide different information. In a single heartbeat cycle, there are particular waves called P, QRS and T that can be recognized using different leads for measurement. The first peak, the P wave, is a small upward wave, which specifies atrial depolarization. Approximately 160 ms after the onset of the P wave, the QRS wave is produced by ventricle depolarization. The ventricular T wave in the ECG indicates the stage of re-polarization of the ventricles. A significant modification concerning the ECG anatomy occurs from birth to adolescence, that is, during the first 16 years of life [36]. According to the study presented in [36], the amplitude of the P wave does not change considerably while the amplitudes of the S and R waves reduce from childhood to adolescence. A progressive modification of the T wave from childhood to adolescence has also been stated by Dickinson [37]. 48 In addition, the QT interval will shorten much more than the rest of the intervals when the heart rate increases. This change can be corrected by normalizing the QT interval according to the heart rate. The dependence of the QT interval to heart rate can be adjusted utilizing Bazett's QT interval correction for which the corrected QT interval is found to be somewhat constant over the years [38]. It should be mentioned that for simplicity, we have not considered QT interval correction/normalization in this article. Aging does not affect any gender-based variances in cardiac electrophysiological properties in adolescents. However, stress, anxiety, and physical exercise can change the Heart Rate Variability (HRV) and morphology [36].

IV. GENERATING CRYPTOGRAPHIC KEYS UTILIZING ECG BIO-ELECTRICAL SIGNAL

Medical sensors rely on cryptographic keys to secure end-to-end communications or encrypt/decrypt messages that need to be conveyed between the sensors and health caregivers [17], [39]. Solutions based on cryptographic keys generated from individuals' ECG signals are best suited for tiny medical sensors as these solutions are lightweight and require low resources [8]. By developing robust and efficient cryptographic key generation approaches, the security of medical sensors can be offered in a plug-and-play manner where neither a network establishment nor a key pre-distribution mechanism is required. Cryptographic keys can be generated within the network on the fly via the usage of ECG data collected by medical sensors when and as needed. The generated keys can be employed, for example, in end-to-end communications to securely encrypt/decrypt patients' medical data being transferred between sensors and health caregivers [17], [39]. The keys can also be used for authentication and authorization of peers, confidentiality, and integrity of the conveyed messages in BSNs [40]–[42]. A robust cryptographic key generated within a BAN can also prevent probable attack scenarios including passive information gathering and message corruption, replay attacks and Denial of Service attacks (DoS), just to name a few.

As Fig. 1 presents, the first step to generate ECG-based cryptographic keys is raw ECG data acquisition from subjects. The collected ECG data include information about the heart rate, morphology, and rhythm being recorded by placing a set of electrodes on body surfaces such as neck, chest, legs, and arms. Once collected, raw ECG data needs to be prepared for further analysis. Analysis of the ECG signal can be split into two principal steps by functionality: ECG signal *pre-processing* and *feature extraction*.

A. ECG SIGNAL PRE-PROCESSING

The collected data from ECG signals normally contains noise. The noise has to be removed since the presence of noise makes the analysis and the classification of the data less accurate. Pre-processing suppresses or removes noise from an ECG signal by employing an appropriate filtering scheme. Hence, pre-processing is an essential task prior to extracting the features of an ECG signal.

B. ECG SIGNAL FEATURE EXTRACTION

ECG feature extraction is a procedure where the main features of a sample are extracted. The main objective of the ECG feature extraction process is to select and maintain relevant data of an original signal. Current ECG feature extraction methods are classified into two major classes, fiducial methods and non-fiducial methods. In fiducial methods, points of interest including P, Q, R, S, and T within a single heartbeat waveform (i.e., local minima or maxima or amplitude difference between consecutive fiducial points) are used. Algorithms based on non-fiducial points do not utilize peculiar points to generate the feature set. Non-fiducial methods extract discriminative data from an ECG signal without having to concentrate on fiducial points. They are prone to a high dimension feature space, which in turn propagates the computational overhead and requires more information for trainings that are practically unbounded [43]. High dimensional information may include irrelevant and superfluous data that can degrade the performance of the classifier. In this

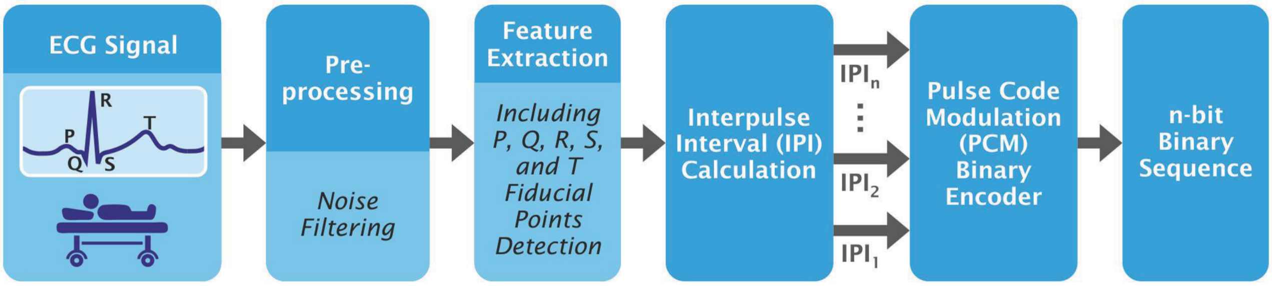

ECG Signal
R
P
T
Q
S
Pre-processing
Noise Filtering
Feature Extraction
Including P, Q, R, S, and T Fiducial Points Detection
Interpulse Interval (IPI) Calculation
IPI$_n$
IPI$_2$
IPI$_1$
Pulse Code Modulation (PCM) Binary Encoder
n-bit Binary Sequence

FIGURE 1. Block diagram of ECG signal analysis and *n*-bit binary sequence generation using consecutive IPI sequences.

article, a fiducial-based algorithm is employed to perform the ECG feature extraction task. In particular, Discrete Wavelet Transform (DWT) is utilized to extract the required features of individuals' ECG signal.

The DWT is a prevalent technique for frequency and time analysis. Wavelet transformation is a linear function which decomposes a signal into components at different resolutions (or scales). Let $\psi(t)$ be a real (or complex valued function) $\in L^2(R)$. The $\psi(t)$ function can be considered as a wavelet, if and only if, its Fourier transform $\hat{\psi}(\omega)$ satisfies the following equation [43]:

$$\int_{-\infty}^{\infty}(\frac{|\hat{\psi}(\omega)|^2}{|\omega|}) = F_\psi < \infty \tag{1}$$

This tolerability clause implies that:

$$\int_{-\infty}^{\infty}\psi(t)dt = 0 \tag{2}$$

This means that $\psi(t)$ is oscillatory which its area is equal to zero. Let $\psi_x(t)$:

$$\psi_x(t) = \frac{1}{\sqrt{x}}\psi\left(\frac{t}{x}\right) \tag{3}$$

be the dilation of $\psi(t)$ by a scale factor of $x > 0$. In the above expression, $\frac{1}{\sqrt{x}}$ is utilized for energy normalization. Wavelet transform utilizes a series of small wavelets with confined duration in order to decompose a signal. Therefore, the wavelet transform of a function $f(t) \in L^2(R)$ at scale x and position l can be written as:

$$W_f(x,l) = \frac{1}{\sqrt{x}}\int_{-\infty}^{\infty}f(t)\psi^*(\frac{t-l}{x})dt \tag{4}$$

where x is the scale factor, l is the translation of $\psi(t)$ and * denotes the complex conjugate of $\psi(t)$.

The non-stationary nature of ECG signals allows one to extend principal functions produced by shifting and scaling of a single prototype function denoted as the mother wavelet. Various wavelet families including Haar and Daubechies exist in the literature and have been broadly utilized for the ECG feature extraction. Haar wavelet is the simplest form of wavelets. Haar wavelet is simple to understand and easy to compute, while some detailed information cannot be captured using it. Daubechies wavelet is theoretically more complex than Haar and has higher computational overhead. But it is more reliable as it can capture details that are missed by the Haar wavelet [28].

In this article, the Daubechies wavelet transform is used for the ECG feature extraction due to the higher reliability it offers. More specifically, Daubechies DB4 wavelet is chosen due to the resemblance of its scaling function to the shape of ECG signals [44]. R peak detection is the core of the Daubechies DB4 wavelet feature extraction where the other fiducial points are extracted with respect to the location of the R peak points. DB4 has four wavelet and scaling function coefficients. Each step of the wavelet transform uses the *wavelet function* to the input data. If the main dataset has N values, the wavelet function needs to be applied in order to calculate $N/2$ differences which reflect change in the data. In the ordered wavelet transform, the wavelet values are saved in the upper half of the N element input vector. The scaling and wavelet functions are computed by taking the inner output of the coefficients and four data values. The scaling function coefficients (h) and the wavelet function coefficient (g) values can be written as:

$$\begin{aligned} h_0 &= \frac{1+\sqrt{3}}{4\sqrt{2}} = -g_3 \qquad & h_1 &= \frac{3+\sqrt{3}}{4\sqrt{2}} = g2 \\ h_2 &= \frac{3-\sqrt{3}}{4\sqrt{2}} = -g_1 \qquad & h_3 &= \frac{1-\sqrt{3}}{4\sqrt{2}} = g_0 \end{aligned} \tag{5}$$

Daubechies DB4 scaling (a) and wavelet (c) functions can be denoted as:

$$\begin{aligned} a_i &= h_0S_{2i} + h_1S_{2i+1} + h_2S_{2i+2} + h_3S_{2i+3} \\ c_i &= g_0S_{2i} + g_1S_{2i+1} + g_2S_{2i+2} + g_3S_{2i+3} \end{aligned} \tag{6}$$

Each iteration in DB4 step computes a scaling function value and a wavelet function value. The index i is incremented by two with each iteration, and new scaling and wavelet function values are computed. It should be mentioned that a normal ECG signal consists of observable P waves, QRS complex and T waves (See Fig. 2). In a normal sinus rhythm, the heart rate for an adult ranges between 60-100 beats per minute. All the main intervals on such an ECG recording are also within normal ranges. Nevertheless, cardiac abnormalities may also be observed in various datasets. These abnormalities usually occurs when patients are suffering from specific cardiovascular diseases, such as myocardial infraction, super vascular arrhythmia, malignant ventricular arrhythmia, and other dangerous types of arrhythmia. Even normal subjects' ECG signals may have some variations due to anxiety, stress, and physical exercises. In these scenarios, the peak values of some waves may not be detectable within one heartbeat using the most common order of the Daubechies wavelet, that is DB4. Hence, the intended main ECG features cannot be extracted and computed. In such scenarios, it is found that DB6 and DB9 are the best candidates among different Daubechies scales to extract features from abnormal types of ECG signals [28], [45]. This is because these Daubechies scales keep certain details and squaring of the remaining signal approximation which result in reliable detection of the R peak points. Once the R peak points of an abnormal ECG signal are detected (using the aforementioned DB scales), other main peak values can be detected with respect to the position of R. Based on the above discussion, the optimum choice of the DB scales relies on the application and the type of ECG signals need to be used. This means that if some of the main features of an ECG signal cannot be extracted by one order of the Daubechies wavelet transform, another scale may provide more detail and accurate results. Thus, there will be low chance that the efficiency of the ECG-based cryptographic key generation approaches is affected. It should be also mentioned accuracy and reliability is more efficient with the higher Daubechies scales. While, the higher Daubechies scales require more coefficients as well as processing time.

1) QRS COMPLEX AND R PEAK DETECTION

The detection of the R peak is the first step of feature extraction. In an ECG signal, the R peak has the highest amplitude among all waves. The QRS complex detection involves specifying the R peak of the heartbeat. Most of the energy of the QRS complex lies between 3-40 Hz and the detection of the QRS complex relies on modulus maxima of the Wavelet Transform. This is due to the fact that modulus maxima and zero crossings of the Wavelet Transform correspond to the sharp edges of an ECG signal. The QRS complex generates two modulus maxima with opposite signs having a zero crossing between them. In a normal ECG signal, the Q and S points occur about 0.1 second before and after the occurrence of the R peaks, respectively. The left point denotes as the Q point and the right point denotes the S point. The QRS width can also be computed from the onset and the offset of the QRS complex. The onset can be defined as the beginning of the Q wave and the offset can be defined as the ending of the S wave.

2) P AND T PEAKS DETECTION

The P wave generally comprises of modulus maxima pair with opposite signs. The T wave also has similar characteristics to the P wave. For the P and the T peak detections, the lower and higher frequency ripples of the signal need to be removed. To detect the P wave, this pair needs to be searched within a window prior to the onset of the QRS complex. The search window starts at about 200 ms before the onset of the QRS complex and ends after the onset of the QRS complex. The zero crossing among the modulus maxima pair corresponds to the peak points of the P wave. The extremum of the signal after the zero crossings of each R peak is denoted as T.

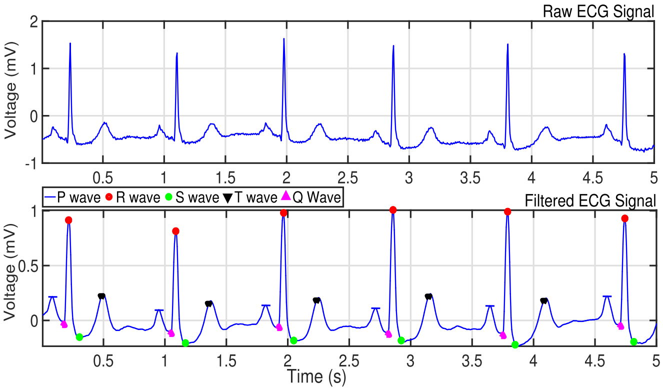


FIGURE 2. An ideal raw ECG signal and the filtered ECG signal with the main fiducial points indicated.

3) PR, RR, PP, QT, AND ST INTERVALS

The PR interval is specified as the interval between the onset of the P wave and the onset of the R wave. The RR interval is defined as the time elapsed between the adjacent R peaks. Heartrate can be calculated as the reciprocal of the RR interval, that is, the time difference between two R peak points. The PP interval is specified as the interval between the adjacent P waves due to atrial depolarization. The PP interval is utilized to calculate the atrial rate. The ST interval is denoted as the interval between the offset of the S-wave and offset of the T-wave. The QT interval is computed by finding the difference between the onset of the Q wave and the offset of the T wave. These intervals are utilized as the main ECG features in this article.

In [17], we presented two different ECG-based cryptographic key generation approaches which use singular ECG feature, that is IPI. Our first approach, IPI-PRNG, relied on a pseudo-random number generator and consecutive IPI sequences. The second approach, IPI-AES, relied upon the AES block cipher in counter mode, using IPI as the seed generator for the AES algorithm. It should be noted that, more explanations and details regarding our IPI-PRNG and IPI-AES approaches can be found in [17]. The following section presents our proposed cryptographic key generation utilizing several ECG features. The proposed approach extends our previous work by reducing the key generation execution times yet providing high security levels. Our proposal is motivated by the fact that to alleviate the key generation execution times, while preserving high security levels, other main features of an ECG signal in addition to IPI can be exploited.

C. GENERATING CRYPTOGRAPHIC KEYS UTILIZING SEVERAL ECG FEATURES (SEF)

In this section, we present a new cryptographic key generation approach, called *SEF*, which employs other main features of an ECG signal rather than using just singleton IPI.

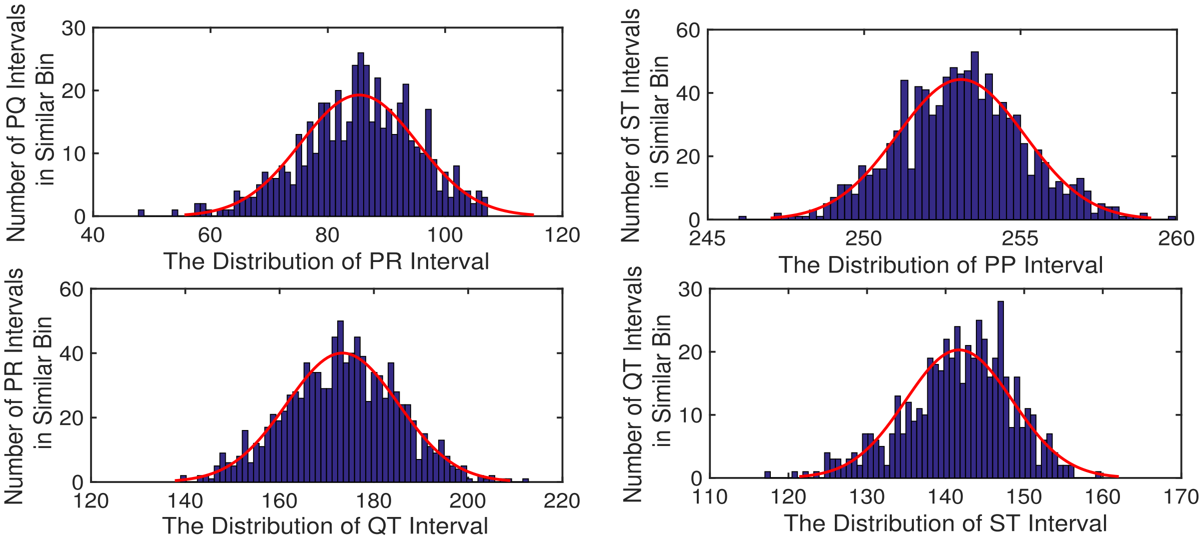


FIGURE 3. **The normal distribution of PR, PP, QT, and ST intervals.**

We describe and justify in more detail the selected features to be used along with the IPI feature of the ECG signal for generating cryptographic keys.

The SEF cryptographic key generation approach uses all of the main ECG features from one heartbeat cycle. The utilized features are PR, RR (also known as IPI), PP, QT and ST. The major reason to use such features is that P, Q, R, S and T waves are noticeable within an ECG signal rhythm for which PR, RR, PP, QT and ST intervals are known as the main and normal components of an ECG waveform [6]. In cardiology, the PR interval is the period which extends from the beginning of the onset of atrial depolarization (P wave) until the beginning of the onset of ventricular depolarization (the QRS complex). The PR interval is normally between 120 to 200 ms in duration. The PP interval is the distance between consecutive P waves due to atrial depolarization. The PP interval is utilized to calculate the atrial rate. In a normal ECG signal, the PP interval and the RR interval are equivalent. Thus, atrial rates and ventricular rates are not independently separated.

In an abnormal ECG signal, for example, when there is an atrioventricular dissociation due to complete heart block, the atrial rate is different from the ventricular rate. This causes for the PP interval to be shorter than the RR interval, meaning that atrial rate is greater than the ventricular rate. The normal PP interval is more than 180-190 ms in duration [6]. The QT interval is measured as the time between the initiation of the Q wave and the termination of the T wave in the heart's electrical cycle. The QT interval demonstrates electrical re-polarization and depolarization of the ventricles. The QT interval is an important feature of the ECG in a sense that it is a marker for the potential of ventricular tachyarrhythmias as well as a risk factor for sudden death. Similar to the RR interval, the QT interval relies on the heart rate. This means that the faster the heart rate, the shorter the RR and QT intervals. This variation can be corrected by normalizing the QT interval according to the heart rate. It should be mentioned that, specifying whether or not the QT interval is normal is not totally a straightforward task as the duration differs according to the patient's heart rate. To allow for this, the corrected QT interval (QTc) must be calculated using Bazett's equation [38]:

$$QTc = \frac{QT}{\sqrt{RR}} \tag{7}$$

where QT is the measured QT interval, QTc is the corrected QT interval, and RR is the computed RR interval. The normal corrected QT interval is below 0.46 for women and below 0.45 for men. In this article, for the sake of simplicity, we have not considered the QT interval correction presented above. Finally, the ST segment specifies the time that ventricles pump the blood to the lungs and the body. The ST segment connects the QRS complex and the T wave which also serve as the base-line from which to measure the amplitudes of the other waveforms. The normal ST segment has a duration of 80-120 ms. In [17], we presented that the fluctuation of the RR interval fits into the normal distribution which indicates the randomness of RR intervals. This finding was also supported by our measurement of entropy, the NIST benchmark, and the Chi-square test presented in [4] and [7]. Likewise, in this section, we show that the distributions of PR, PP, QT and ST intervals also fit into the normal distribution. Thus, these features can be utilized along with RR interval for ECG-based cryptographic key generations. The feasibility of using the PR, PP, QT, and ST intervals is based on the fact that all these features should also fulfill the property of randomness. We examined this property by collecting 30 seconds ECG data of different subjects obtained from the Physiobank database [46]. From the collected ECG data, we have computed all of the consecutive ECG features and plotted their histograms. As can be seen from Figure 3, similar to the RR interval, the distribution of PR, PP, QT and ST intervals also fit into the normal distribution. Hence, these additional main ECG features also fulfill the property of randomness. This is an essential property to ensure that the cryptographic keys which are generated from these ECG intervals are random. Moreover, in [17], we extracted a fixed number of 8 bits from each IPI. This was done using a Pulse Code Modulation (PCM) [47] binary encoder. PCM is a digital interpretation of an analog signal which takes samples of the amplitude of the analog signal at certain intervals. The sampled analog data then is quantized and represented as a digital *n*-bit binary number. Bit 1, most significant bits, is the first bit that specifies the polarity of the sample. Bit "0" represents negative polarity and bit "1" represents positive polarity. Bits 2, 3, and 4 reveal the segment where the sample data is placed. Bits 5, 6, 7, and 8, least significant bits, define the quantized value of the sample inside one of the segments.

In this article, we enhance our approach by using a dynamic technique which can specify the optimized number of bits that can be extracted from each ECG feature. In this regard, our comprehensive analyses have revealed that the alteration range of each ECG feature differs whitin each dataset. This is due to the fact that each ECG feature offers different Standard Deviations (SDs) and mean values. These variations are visible for the PR, PP, QT, and ST features as shown in Figure 3. As a result, extracting a fixed number of bits (e.g., 8 bits) per ECG feature is not an efficient and optimum solution. Therefore, an efficient technique is required where the number of binary values per ECG feature can be extracted as optimum as possible while considering the variation range of SDs and mean values per ECG feature. Based on the discussion above, we utilize a dynamic technique in order to specify the optimized number of bits which need to be extracted from each ECG feature. The used technique enables to extract optimal binary values and ensures the randomness property as the binary sequences are produced based on the real-time variation of the measured ECG signal [27]. The utilized technique to determine the number of optimum bits (M) can be defined as:

$$\mu(FX_i) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{8}$$

$$SD(FX_i) = \sigma(FX_i) = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i-\mu)^2} \tag{9}$$

$$C_v = \frac{\sigma(FX_i)}{\mu(FX_i)} \tag{10}$$

$$M = \lceil\frac{\ln(\sigma(FX_i))}{\ln(2)}\rceil + \lceil C_v\rceil \tag{11}$$

where FX_i represents a set of any one of the PR, PP, QT, and ST features from one sampled ECG dataset in the i_th heartbeat, x_i represents each value in the dataset, μ is the mean value of the dataset, Σ is the summation, N is defined as the number of values in the dataset, σ indicates the standard deviation of a dataset, and C_v is the coefficient of variation which is defined as the ratio of the standard deviation to the mean value. The main reason to use the *ln* function in the equation (14) is that from the information theory point of view, *ln* provides a solution for determining the number of optimal bits needed in a code (even when the code is not known). Since the SD and mean values of each main feature within one ECG dataset are different, the number of extracted optimum bits vary accordingly. In the j_{th} heartbeat, the efficient number of binary bits B_{opt} that can be extracted efficiently from one ECG feature can be defined as:

$$B_{opt} = GET\_BITS\_FROM\_F_{LSB}(FX_j, lsb, M) \tag{12}$$

F_{LSB} is a function which extracts M bits from Least Significant Bits (LSB) of its input FX_i. By exploiting the aforementioned technique, optimum binary values can be extracted from the required main ECG features per heartbeat cycle. The extracted binary values per heartbeat cycle then need to be concatenated to form an *m*-bit binary sequence. Finally, to generate an *n*-bit sequence using the SEF approach, binary sequences which are produced from *k* consecutive heartbeats are required to be concatenated.

Our study also reveals that the variation range of all of the main ECG features differs in different ECG datasets. To give an example, the number of optimum binary values which can be extracted from the PR feature of Normal Sinus dataset is not identical to the number of the binary values which can be extracted from PR feature of the European ST-T dataset. Table 1 presents the results of different subject groups which we have investigated for this purpose. We have selected 10 of the most-known ECG recording and cardiovascular disease datasets from the open source Physiobank database [46]. In this regard, from each of the following 10 datasets, 5 subjects are randomly chosen for this study. The last dataset, that is, the motion artifact ECG, includes short duration ECG signals recorded from one healthy 25-year-old male performing different physical activities. The selected datasets are: (i) Motion Artifact Contaminated ECG Database, sampled at 500 Hz per second with 16-bits resolution, (ii) Super Vascular Arrhythmia (Arrhyth.) sampled at 125 Hz, (iii) Malignant Ventricular Arrhyth. sampled at 250 Hz, (iv) MIT-BIH Long-Term sampled at 360 Hz, (v) Atrial Fibrillation sampled at 250 Hz, (vi) MIT-BIH Arrhyth. sampled at 360 Hz, (vii) Myocardial Infraction sampled at 125 Hz, (viii) MIT-BIH Noise Stress sampled at 360 Hz, (viiii) European ST-T Database sampled at 250 Hz, and (x) Normal Sinus sampled at 128 Hz. The main motivation to select these datasets is the fact that they are among the most recognized ECG recordings and prevalent cardiovascular diseases according to Physiobank [46]. Moreover, no recognizable ECG recording nor a specific patient having one of these cardiovascular diseases is found among each dataset. Thus, any bias that can help in the identification of a specific subject cannot be found. It should be also mentioned that in a motion artifact contaminated ECG database, there is no other information than the subject's age and gender available. Our experiments to extract the ideal number of binary values from all of the main ECG features of each ECG dataset are presented in Table 1. As can be deduced from our measurements, the optimum number of binary values which can be extracted

TABLE 1. Optimum binary sequences produced from main general features of ECG signals of subjects with different heart health conditions.

ECG Dataset	Binary Value Extracted Per ECG Feature (bit)					Total Binary Values Extracted from One Heartbeat Cycle (bit)
	PR	RR	PP	QT	ST	
Motion Artifact ECG	2	4	4	4	2	16
Super Vascular Arrhyth.	2	3	4	3	2	14
Malignant Ventricular Arrhyth.	2	3	3	2	3	13
MIT-BIH Long-Term	2	4	4	3	3	16
Atrial Fibrillation	2	3	4	3	3	15
MIT-BIH Arrhyth.	3	4	4	3	2	16
Myocardial Infraction	3	3	3	3	2	14
MIT-BIH Noise Stress	2	3	4	3	2	14
European ST-T	3	3	4	3	2	15
MIT-BIH Normal Sinus	2	4	4	3	3	16

from various features of one ECG dataset totally differs from one dataset to another. This is due to the utilization of the aforementioned technique (where the optimum number of bits can be extracted from each main ECG feature) instead of a fixed number of bits representation since each feature of the ECG has different mean and SD values.

According to the above discussion, in the SEF key generation approach, depending on the length of the cryptographic key n that needs to be generated, approximately $\lceil \frac{n}{16} \rceil$ consecutive ECG heartbeat cycles need to be detected. From the detected heatbeats, all of the main ECG features (PR, RR, PP, QT and ST) from a t-second segment of a patient's ECG data need to be computed. To achieve this goal, the following tasks are required to be performed: (i) for a specified period of time t, the main fiducial points or peaks of a sensed ECG signal (P, Q, R, S, and T) should be extracted utilizing a generic feature extraction function, (ii) from the detected fiducial points, the required x consecutive ECG features (PR_1, RR_1, PP_1, QT_1, ST_1), (PR_2, RR_2, PP_2, QT_2, ST_2), $\ldots$, (PR_x, RR_x, PP_x, QT_x, ST_x) should be computed, (iii) from the computed main ECG features, the amount of optimum binary values per ECG feature needs to be calculated. This should be done using an equation where the ideal binary values per ECG feature, that is $m_1, m_2, \ldots, m_x$, will be selected based on their mean values and SDs, and (iv) the generated m_i-bit binary sequences from each ECG feature then need to be concatenated in order to form an n-bit binary sequence. The generated n-bit binary sequence is considered as the main cryptographic key generated using this approach. It should be mentioned that the produced n-bit binary sequence using the SEF approach underlays the SEF-PRNG and SEF-AES approaches presented in the following sections.

1) STRENGTHENING SEVERAL ECG FEATURE-BASED KEY GENERATION THROUGH PRNG (SEF-PRNG)

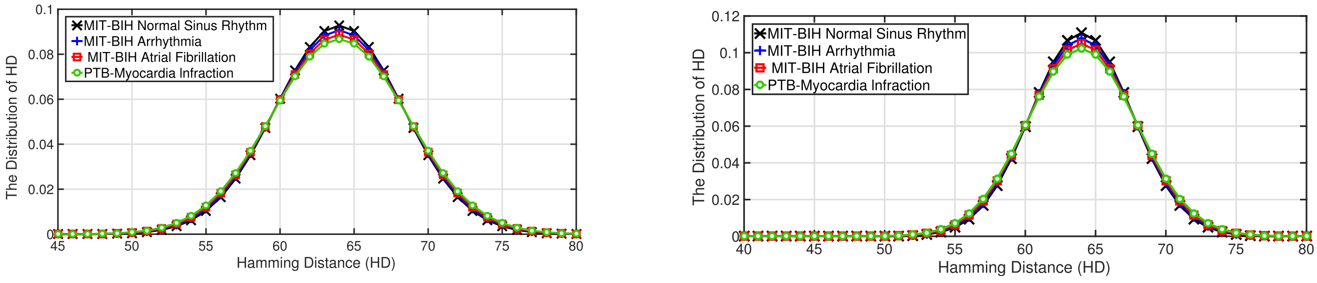
Similar to the IPI-PRNG, the SEF-PRNG approach also consists of two main phases: (i) generating an n-bit binary sequence from each subject's ECG data. To do this, as discussed previously, about $\lceil \frac{n}{16} \rceil$ heartbeat cycles of a patient's ECG data needs to be collected. From the collected data, consecutive PR, RR, PP, QT, and ST features each of which encoded into its optimum x-bit binary value (using the previously mentioned technique) need to be computed. After that, the aforementioned steps in SEF approach need to be performed in such a way that for each subject, an n-bit binary sequence is generated. (ii) a Pseudo Random Number Generator (PRNG) is used to generate a random n-bit binary sequence. To generate a random n-bit binary sequence, the Fibonacci Linear Feedback Shift Register (LFSR) is employed. We have utilized the Fibonacci LFSR function of MATLAB similarly as we did in the IPI-PRNG approach to produce a random n-bit binary sequence. Once the n-bit random binary sequence is generated (using the Fibonacci LFSR function), the main cryptographic key can be generated. If SEF_n is the n-bit binary sequence generated from ECG and and $FLFSR_n$ is the n-bit random binary sequence generated using the Fibonacci LFSR, the main n-bit cryptographic key is produced by XORing the outputs of phases (i) and (ii).

2) STRENGTHENING SEVERAL ECG FEATURE-BASED KEY GENERATION THROUGH AES (SEF-AES)

Similarly as IPI-AES, the SEF-AES approach also uses the AES [19] block cipher in counter mode as the cryptographic pseudo-random number generator to generate n-bit cryptographic keys. In SEF-AES, to generate an n-bit cryptographic key, two n-bit binary sequences need to be generated as the main seeds of the AES algorithm. The first seed is considered as input data (plaintext) of the AES and the second one is considered as the encryption/decryption key. To generate these two seeds, we exploit the SEF key generation approach as the seed generator. To do this, $\lceil \frac{n}{8} \rceil$ consecutive heartbeat cycles of a patient's ECG signal need to be collected. From the collected data, consecutive PR, RR, PP, QT and ST features are encoded into their optimum x-bit binary values The produced x-bit binary sequences from each heartbeat cycle further need to be concatenated to form a $2n$-bit binary sequence. After that, the $2n$-bit binary sequence needs be divided into two n-bit binary sequences. The first sequence is used as the input data (plaintext) and the second one is used as the AES encryption key. At the final stage, the output of the AES-n algorithm (ciphertext) is considered as the main n-bit cryptographic key generated utilizing the subjects' ECG signals.

V. EXPERIMENTS AND RESULTS

In this section, we assess the security level and performance of our proposed ECG-based cryptographic key generation approaches in terms of distinctiveness, test of randomness, temporal variance, and key generation execution time. We conduct our experiments on both normal and abnormal ECG signals obtained from the publicly available and widely used database, that is, Physiobank [46]. PhysioBank comprises of databases of multi-parameter neural, cardiopulmonary, and other biomedical signals from patients and healthy subjects with a variety of conditions including sudden cardiac death, irregular heartbeat (arrhythmia), congestive



(a)

(b)

FIGURE 4. The distribution of hamming distance of any two 128-bit cryptographic keys generated using IPI-AES and SEF-AES approaches for subjects with different heart health conditions. (a) The distribution of hamming distance between any two 128-bit cryptographic keys generated using IPI-AES approach for subjects with different heart health conditions. (b) The distribution of hamming distance between any two 128-bit cryptographic keys generated using SEF-AES approach for subjects with different heart health conditions.

heart failure, sleep apnea, and epilepsy. Our experiments are carried out on both normal and abnormal ECG signals which are obtained from 239 subjects studied by the Beth Israel Hospital Laboratory in Boston and Physikalisch-Technische Bundesanstalt (PTB), the National Metrology Institute of Germany. The employed ECG signals include: (i) ECG signals of of 18 subjects (5 men, aged 26 to 45, and 13 women, aged 20 to 50) with Normal Sinus Rhythm. The recordings are digitized at 128 samples per second with resolution over a 10 mV range. (ii) ECG signals of 48 subjects with Arrhythmia (22 women of age 23 to 89 and 26 men of age 32 to 89) which they were recorded by a two-channel ambulatory ECG system. The recordings are digitized at 360 samples per second with 11-bit resolution over a 10 mV range per patient. (iii) ECG signals of 25 subjects with Atrial Fibrillation. The individual recordings are each 10 hours in duration, and contain two ECG signals each digitized at 250 samples per second with 12-bit resolution over a range of 10 mV. (iv) ECG signals of 148 subjects with Myocardial Infraction (89 men aged 17 to 87 and 59 women aged 19 to 83). Each signal is digitized at 1000 samples per second, with 16 bit resolution over a range of 16 mV. We have captured 100 different samples of 5 minute long ECG data for each subject and evaluated the efficiency of our approach in terms of distinctiveness, test of randomness and temporal variance. The collected ECG signals are filtered using a low-pass filter with a 30 Hz threshold frequency. Such a filter reduces the environmental noise and provides a smoother signal for further analysis. For our experiment, we have generated 128-bit cryptographic keys using the aforementioned approaches. We have implemented and analyzed our key generation approaches utilizing MATLAB [48].

A. DISTINCTIVENESS

The first experiment is to determine whether the cryptographic keys generated utilizing the presented approaches are distinctive for different individuals. Distinctiveness indicates that the generated keys should be significantly different for different subjects, at any given time. Hamming Distance (HD) is utilized as the main metric in order to evaluate the difference between any two cryptographic keys of equal length. For two sufficiently long binary sequences, the distribution of HD should be centered at half of the length of the binary sequences. This indicates that these sequences are randomly generated [5]. The reason is that any bit of a random binary number should have equivalent probability to be zero or one. Hence, the average of HD of a sufficiently large and random set of n-bit binary sequences is anticipated to be about $n/2$, provided that the binary sequence is distinctive. For two different bits, i and j, which are extracted from the same position of two independently generated cryptographic keys (K), the probability $P(K_i, K_j)$ can be represented as [5]:

$$P(K_i, K_j) = 0.25 \quad K_i = 1, 0 \;\&\; K_j = 1, 0 \tag{13}$$

$$HD_d = \sum_{P_1 \neq P_2} \frac{(\mid ECG_{i,P_1} - ECG_{i,P_2} \mid)}{\mid sig \mid^2} \tag{14}$$

To evaluate the distinctiveness of different keys generated using the presented approaches, we use the average Hamming Distance metric, as defined in Equation (17).

HD_d is the computed Hamming Distance between the cryptographic keys generated using ECG signals of different subjects, $\mid\ sig\ \mid$ is the length of the used physiological signal set, i defines the ECG index, and P_1 and P_2 defines the patient's indexes. We have investigated the distinctiveness of the cryptographic keys generated utilizing our SEF, IPI-PRNG, IPI-AES, SEF-PRNG, and SEF-AES approaches and compared the results with the conventional IPI approach. We have sampled the ECG signals of each subject over 100 random start-times. The average HD between the cryptographic keys of the two different subjects generated at the same start-time is then calculated.

The HDs between different subjects' cryptographic keys are calculated (See Figures 4a and 4b). The results of our distinctiveness calculations show that the average HD between the cryptographic keys generated from the ECG signals of two different subjects using IPI, SEF, IPI-PRNG, SEF-PRNG, IPI-AES, and SEF-AES are 47.76% (≈ 62 bits), 48.13% (≈ 62 bits), 49.09% (≈ 63 bits), 49.41% (≈ 63 bits), 49.84% (≈ 64 bits), and 49.93% (≈ 64 bits), respectively.

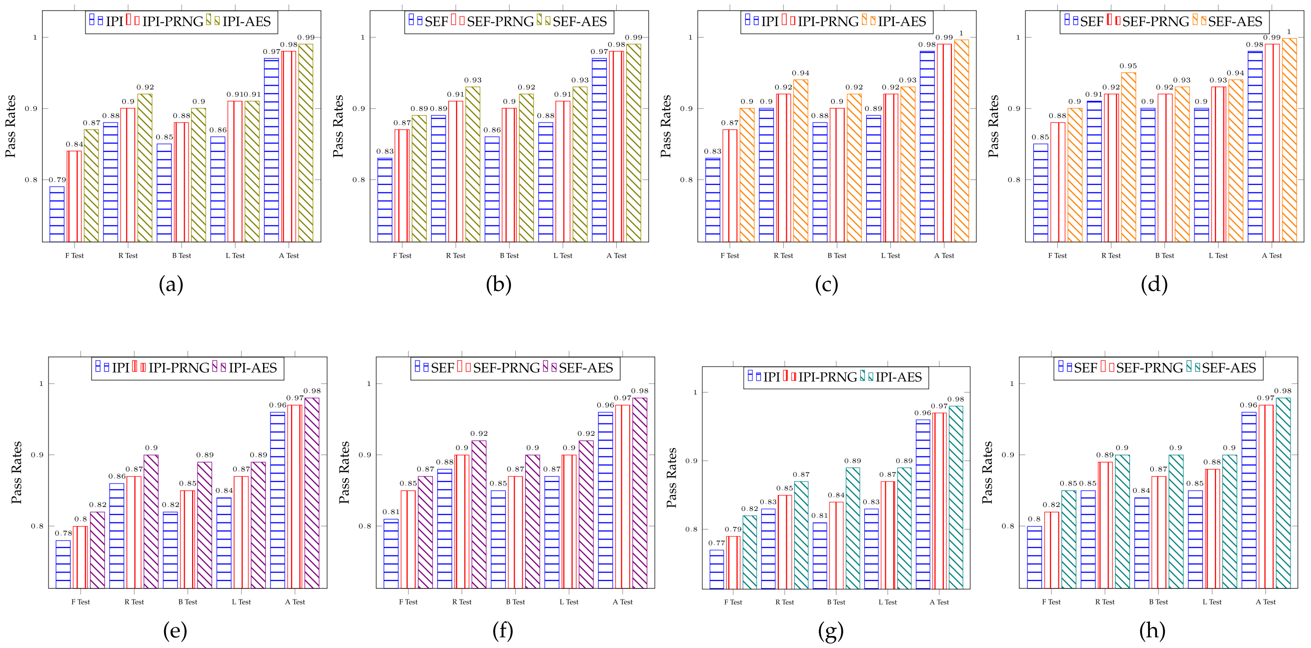


FIGURE 5. NIST pass rate comparison of different ECG-based cryptographic key generation approaches for subjects with different heart health conditions. (a) NIST Tests, MIT-BIH Arrhythmia. (b) NIST Tests, MIT-BIH Arrhythmia. (c) NIST Tests, MIT-BIH Normal Sinus Rhythm. (d) NIST Tests, MIT-BIH Normal Sinus Rhythm. (e) NIST Tests, MIT-BIH Atrial Fibrillation. (f) NIST Tests, MIT-BIH Atrial Fibrillation. (g) NIST Tests, PTB-Myocardial Infarction. (h) NIST Tests, PTB-Myocardial Infarction.

B. TEST OF RANDOMNESS

Generating distinctive and long keys is not sufficient as it is also necessary to ensure that the keys are sufficiently random and cannot be predicted easily. Randomness is related to Shannon entropy. Entropy is a measure of uncertainty for many cryptographic purposes. The Shannon entropy equation can be written as [49]:

$$H(r) = -\sum_{i=1}^{n} P(ECG_i) \log_2 P(ECG_i) \tag{15}$$

r is an information source with n mutually exclusive events, $P(ECG_i)$ is the probability of the ith event. According to this evaluation metric, the randomness level of a binary sequence increases when $H(r)$ closes to 1.

We have evaluated the randomness of the 128-bit cryptographic keys generated using the SEF, IPI-PRNG, SEF-PRNG, IPI-AES, and SEF-AES approaches. Then, we have compared our results with the conventional IPI approach. The randomness of the generated keys is evaluated from two perspectives: (i) Shannon entropy and (ii) the pass rates of the NIST statistical benchmark. To evaluate randomness from the Shannon entropy point of view, we have computed the entropy of the keys generated from each subject's ECG signal over 100 random start-times using IPI, SEF IPI-PRNG, SEF-PRNG, IPI-AES, and SEF-AES approaches. The randomness of the generated cryptographic keys are also evaluated using the NIST benchmark. The NIST benchmark is developed for cryptographic random and pseudo-random number generator applications. The results of the NIST statistical tests are pass rates (also called P-values) which indicate the probability of randomness of the generated cryptographic keys. If a P-value is less than the threshold, that is, 1% the randomness hypothesis fails.

Five main tests proposed by NIST for evaluating randomness are utilized in this article. They are the frequency test (F-Test), the runs test (R-Test), the frequency test within a block (B-Test) and the test for the longest run of ones in a block (L-Test). Description of the above-mentioned tests can be found in more detail in [26] and they are briefly summarized as follows: (i) The F-Test specifies whether the number of 0s and 1s in the input sequence are approximately the same as would be anticipated for a real random sequence. (ii) The R-Test specifies if the number of runs of 0s and 1s of different lengths is as anticipated for a random sequence. Run, refers to an uninterrupted sequence of identical bits. (iii) The B-Test specifies whether the frequency of 1s in an N-bit block is approximately $N/2$, as would be expected under an assumption of randomness. (iv) The L-Test specifies if the length of the longest run of 1s in the tested sequence is consistent with the length of the longest run of 1s that would be anticipated in a random sequence. (v) The A-Test compares the frequency of overlapping blocks of two adjacent lengths, that is, l and $l + 1$ versus the expected result for a random sequence.

As shown in Figures 5, in all approaches the entropy values as well as the NIST pass rates are close to 1 signifying that the distribution of 0s and 1s in the generated keys among the 6 approaches are quite uniform. In addition, we find out that the randomness of abnormal ECG signals is slightly worse than the normal ones. This is due to the fact that for some abnormal ECG signals their ECG feature patterns were

TABLE 2. Execution time comparison of different ECG-based key generation approaches to produce 128-bit cryptographic keys.

Processor	Execution Time, Single Iteration (ms)						Execution Time, Total (s)					
	IPI [4], [7]	IPI-PRNG	IPI-AES	SEF	SEF-PRNG	SEF-AES	IPI [4], [7]	IPI-PRNG	IPI-AES	SEF	SEF-PRNG	SEF-AES
ARM Cortex-M3	57.2	66.1	95.3	37.4	41	61.9	0.9	1.1	1.5	0.3	0.4	0.5
ATSAMD21G18A	169.2	192.7	238.1	103.1	131.9	172	2.7	3.1	4	0.9	1.1	1.3
Atmel ATmega128L	210.9	244.8	303	129.4	147.7	199.5	3.3	3.9	4.8	1.1	1.2	1.6
STM32F7	11.8	13.7	16.8	7.9	9.2	11.6	0.2	0.2	0.3	0.07	0.08	0.1
STM32F4	24.3	28.2	40.7	14.2	18.3	26.7	0.4	0.4	0.6	0.2	0.2	0.3
STM32F3	36.5	42.4	61.1	25	30.1	40.5	0.6	0.7	1	0.2	0.3	0.4
STM32L4	54.8	63.6	91.7	34.3	40.7	59.8	0.9	1	1.4	0.3	0.4	0.5
STM32F2	60.3	70.6	101.9	39.5	43.1	63.7	1	1.2	1.7	0.3	0.4	0.6
STM32F1	89.9	104.2	150.4	59.2	71.3	101	1.4	1.7	2.4	0.5	0.6	0.9
STM32F0	144.6	167.4	211.5	90.8	104.6	139.8	2.3	2.7	3.4	0.8	0.9	1.2
STM32L1	165.3	184.4	231.9	102.5	124.3	162.1	2.7	3	3.9	0.9	1	1.3
STM32L0	187.4	225.2	278.9	114.6	133.4	178.2	3	3.3	4.5	1	1.1	1.5

irregular and sometimes hard to be detected. Compared to the normal ECG signals, abnormal signals are more chaotic and have larger variation resulting in less reliable ECG features. For normal ECG signals, the IPI and SEF approaches have in average the entropy of about 0.98, the IPI-PRNG and SEF-PRNG approaches, have in average the entropy of about 0.99, and the IPI-AES and SEF-AES approaches offer the entropy of ~ 1. The results of the test of randomness revealed that there is no significant difference between the results of entropy nor the NIST pass rates of any two different cryptographic keys generated using the strengthened IPI-based and the SEF approaches. The cryptographic keys generated using the IPI-PRNG, SEF-PRNG, IPI-AES and SEF-AES approaches provide better randomness in terms of entropy as well as NIST pass rates compared to the IPI approach and the SEF approaches. We have found out that the cryptographic keys which are generated utilizing the strengthened ECG features (IPI or SEF) offer better results in terms of randomness, that is ~ 1 entropy, as well as in terms of NIST pass rates than just utilizing singleton ECG features. A high level of randomness prevents the cryptographic keys from being easily predicted by any malicious activity. As a result, cryptographic keys generated using our proposed approaches meet the design goal of randomness.

C. TEMPORAL VARIANCE

Being different for the same subject at different time intervals is another main requirement of a binary sequence to be used as a cryptographic key. Temporal variance measures the resemblance between two cryptographic keys that are generated using a bio-signal (i.e., the ECG signal in this context) of the same subject at different time intervals. The analysis of the temporal variance also indicates that medical data of one subject which is encrypted using a robust cryptographic key cannot be decrypted effortlessly using a non-real time ECG signal from the same subject.

We evaluated the temporal variance of different 128-bit cryptographic keys which are generated using the IPI, SEF, IPI-PRNG, SEF-PRNG, IPI-AES and SEF-AES approaches. This is to ensure that a new measurement of a subject's ECG will not lead to the same key. We have sampled ECG signals of each subject over 100 random start-times. The average HDs between the keys of the same subject generated at different start-times are then calculated. To compute temporal variance, the average HD between cryptographic keys that are generated utilizing the ECG signal of the same subject at different start-times is computed.

The HD equation being utilized for computing the temporal variance of the generated keys can be written as [5]:

$$HD_s = \sum_{P_1=P_2} \frac{(\mid ECG^{t_1}_{i,P_1} - ECG^{t_2}_{i,P_2} \mid)}{\binom{\mid sig \mid}{2}} \tag{16}$$

HD_s is the hamming distance computed between the cryptographic keys generated from the ECG signal of the same subject at different time intervals. t_1 and t_2 define different start-times.

The results of our experiment show that the average HD between the cryptographic keys which are generated via the ECG signal of the same subject at different time intervals using IPI, SEF, IPI-PRNG, SEF-PRNG, IPI-AES and SEF-AES are 47.71% ($\approx$ 62 bits), 48.02% ($\approx$ 62 bits), 48.96% ($\approx$ 63 bits), 49.33% ($\approx$ 63 bits), 49.79% ($\approx$ 64 bits), and 49.9% ($\approx$ 64 bits), respectively. Similar to the computed results presented in the distinctiveness section, when employing strengthened ECG features (either IPI-based or SEF approach), the distribution of HDs of any two binary sequences generated from the ECG signal of the same subject does not change significantly. The normalized distribution of HDs of two cryptographic keys that are generated using strengthened IPI-AES and SEF-AES approaches are centered at 64. Similarly, the normalized distribution of HDs of two cryptographic keys that are generated using strengthened IPI-PRNG and SEF-SEF approaches are centered at 63. For IPI and SEF approaches, the normalized distribution of HDs of two cryptographic keys are centered at 62. The main reason for such similarities between the HD results (with just negligible percentage differences) is due to the fact that our main goal is to alleviate the key generation execution time while preserving the achieved high security level in terms of temporal variance. The average HD between the cryptographic keys of the same subject generated using the IPI-PRNG, SEF-PRNG, IPI-AES, and SEF-AES approaches present better results compared to the IPI and SEF approaches. This is because ECG feature based cryptographic key generation approaches which are strengthened using the PRNG and AES algorithms appear to better distinguish the same subject's cryptographic key. Particularly, ECG feature based cryptographic key generation approaches which are strengthened using the PRNG and AES algorithms can increase the security level of the generated keys as the correct keys cannot be easily obtained via a brute-force attack. Therefore, the cryptographic keys which are generated using our proposed approaches meet the design goal of temporal variance.

D. KEY GENERATION EXECUTION TIME

To investigate the feasibility and key generation execution overhead of our approaches compared to the conventional IPI approach, we have examined the execution time required to generate 128-bit ECG-based cryptography keys. For this purpose, we utilized different processors ranging from tiny micro-controllers (e.g., STM32L0 with 32 MHz operating frequency) to reasonably powerful embedded microprocessors (ARM Cortex-A7). The considered processors are widely used in different medical domains depending on the power-performance requirements. Our experiments are carried out on ECG recordings obtained from the mentioned MIT-BIH Arrhythmia dataset, sampled at 360 Hz.

Table 2 presents the computed key generation execution times of our IPI-PRNG, IPI-AES, SEF, SEF-PRNG, and SEF-AES approaches as well as the conventional IPI approach. The execution times are presented in both single iteration and total times. Single iteration execution time indicates the time required to produce an x-bit binary sequence from one heartbeat cycle. Total execution time means the sum of single iteration execution times until successive iterations of the operations yields the desired result, that is, generates the desired 128-bit ECG-based cryptographic keys. To give an example, considering a subject with the ECG heartrate of 60 bpm, the specific STM32L0 microcontroller requires about 187.4 ms, 225.2 ms and 278.9 ms execution times per iteration for the IPI, IPI-PRNG, and IPI-AES approaches, respectively. These are the times these three approaches require to produce an 8-bit binary sequence from one ECG heartbeat cycle. As discussed earlier, to generate 128-bit ECG-based cryptographic keys, it is required for IPI, IPI-PRNG and IPI-AES approaches to compute 16 heartbeat cycles from a subject's ECG signal. Thus, the total key generation execution times of IPI, IPI-PRNG, and IPI-AES approaches are computed as: $187.4 * 16 = 3$ (s), $225.2 * 16 = 3.3$ (s), and $278.9 * 16 = 4.5$ (s), respectively. The same microcontroller requires about 114.6 ms, 133.4 ms, and 178.2 ms execution times for the SEF, SEF-PRNG, and SEF-AES approaches to produce 16-bits binary sequences from one ECG heartbeat cycle. However, as presented earlier, to generate 128-bit ECG-based cryptographic keys, the SEF, SEF-PRNG and SEF-AES approaches need to compute 8 heartbeat cycles from a subject's ECG signal. As a result, the total key generation execution times of SEF, SEF-PRNG, and SEF-AES approaches are calculated as $114.6 * 8 = 1$ (s), $133.4 * 8 = 1.1$ (s), and $178.2 * 8 = 1.5$ (s), respectively, which are considerably lower than their counterparts. The key generation execution times of SEF, SEF-PRNG and SEF-AES are in average 1.8 times times faster than IPI, IPI-PRNG and IPI-AES approaches. This is due to the fact that in IPI, IPI-PRNG and IPI-AES in total 8 bits can be extracted from one ECG heartbeat cycle, while in SEF, SEF-PRNG and SEF-AES approaches in total 16 bits can be extracted from the same heartbeat cycle. Thus, by utilizing additional ECG features, the latency of ECG-based key generation approaches can be significantly reduced. As can be seen from the results of distinctiveness, test of randomness, temporal variance and execution time, there is a clear trade-off between execution time and security level for different approaches. the IPI-AES and SEF-AES approaches show higher security levels in comparison to the SEF, IPI-PRNG, SEF-PRNG and the conventional IPI approach. However, such a high security level increases the execution time on average by 41.2% and 38.8% compared to the IPI-based and the SEF approaches, respectively. In this context, the IPI-PRNG and SEF-PRNG better balance the trade-off as they offer a higher security level while imposing a much lower execution time overhead, that is, on average 12.3% and 9.6% compared to the IPI-based and the SEF approaches, respectively. It should be mentioned that the efficiency of the proposed approaches highly depends on the application domain in which the approaches are utilized. As generating keys is performed in an on-demand way and not in every message transaction, the delay imposed by it might be more tolerable for some applications compared to others. Therefore, the IPI-AES and SEF-AES approaches can be a better alternative for applications where high security level is demanded and the latency can be tolerated. Another observation which can be made from Table 2 is the significant difference in execution time for different processors. This is mainly due to the difference in the processing power and memory available for each processor. This can guide designers and developers to adjust their demanded security level with the available processing power or vice versa.

VI. CONCLUSIONS

We presented a low-latency approach for generating secure ECG feature based cryptographic keys. Most existing key generation approaches are not directly applicable to BANs. The reason is that sensors used in BANs are extremely resource-constrained and demand a low-latency key generation time as well as a high security level. To alleviate these limitations, we proposed a robust key generation approach employing several ECG features, called SEF. Our SEF approach utilizes 4 main reference-free ECG features comprising of PR, RR, PP, QT, and ST. A dynamic technique is used to specify the optimum number of bits that can be extracted from each main ECG feature. We consolidated and strengthened the SEF approach with cryptographically secure pseudo-random number generator techniques. The Fibonacci linear feedback shift register and the AES algorithm are implemented as pseudo-random generators to enhance the security level of our approach. The security evaluation of the generated keys was made in terms of distinctiveness, test of randomness, temporal variance, as well as using the NIST benchmark. Our approach is applied to normal and abnormal ECG signals. The analyses showed that the strengthened key generation approach offers a higher security level in comparison to existing approaches which rely only on singleton ECG features. Our analyses also reveal that the normal ECG signals have slightly better randomness compared to the abnormal ones. Cryptographic keys which are generated from normal ECG signals using the SEF approach have in average the entropy of about 0.98. Cryptographic keys that are produced using the strengthened SEF approach offer the entropy of ~ 1. In addition, the reinforced key generation approach has also better P-value NIST pass rates compared to state-of-the-art approaches which rely only on singleton ECG features. We also found out that our approach is approximately 1.8 times faster than existing IPI-based key generation approaches. Future work includes investigating and analysis of other physiological signals within a BAN. This is to realize how the generated cryptographic keys can also be used by other bio-sensors to provide intra-BAN communication security.

REFERENCES

[1] R. J. Anderson, "A security policy model for clinical information systems," in *Proc. IEEE Symp. Secur. Privacy*, May 1996, pp. 30–43.

[2] M. S. Siddiqui and C. Hong, "Security issues in wireless mesh networks," in *Proc. Int. Conf. Multimedia Ubiquitous Eng.*, 2007, pp. 717–722.

[3] A. Bhargava and M. Zoltowski, "Sensors and wireless communication for medical care," in *Proc. Int. Workshop Database Expert Syst. Appl.*, 2003, pp. 956–960.

[4] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 73–81, Apr. 2006.

[5] D. K. Altop, A. Levi, and V. Tuzcu, "Towards using physiological signals as cryptographic keys in body area networks," in *Proc. Int. Conf. Pervasive Comput. Technol. Healthcare*, 2015, pp. 92–99.

[6] F. Agrafioti, J. Gao, and D. Hatzinakos, "Heart biometrics: Theory, methods and applications," in *Biometrics*, J. Yang, Ed. Rijeka, Croatia: InTech, 2011. [Online]. Available: https://www.intechopen.com/books/biometrics/heart-biometrics-theory-methods-and-applications, doi: 10.5772/18113.

[7] G.-H. Zhang, C. C. Y. Poon, and Y.-T. Zhang, "Analysis of using interpulse intervals to generate 128-bit biometric random binary sequences for securing wireless body sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 1, pp. 176–182, Jan. 2012.

[8] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Comput.*, vol. 55, no. 9, pp. 1081–1088, Sep. 2006.

[9] A. Ali and F. A. Khan, "Key agreement schemes in wireless body area networks: Taxonomy and state-of-the-art," *J. Med. Syst.*, vol. 39, no. 10, p. 115, 2015.

[10] K. V. R. Ravi, R. Palaniappan, C. Eswaran, and S. Phon-Amnuaisuk, "Data encryption using event-related brain signals," in *Proc. Int. Conf. Comput. Intell. Multimedia Appl.*, vol. 1. 2007, pp. 540–544.

[11] A. Leier, C. Richter, W. Banzhaf, and H. Rauhe, "Cryptography with dna binary strands," *Biosystems*, vol. 57, no. 1, pp. 13–22, 2000.

[12] S. D. Bao, C. C. Y. Poon, Y. T. Zhang, and L. F. Shen, "Using the timing information of heartbeats as an entity identifier to secure body sensor network," *IEEE Trans. Inf. Technol. Biomed.*, vol. 12, no. 6, pp. 772–779, Nov. 2008.

[13] G. H. Zhang, C. C. Y. Poon, and Y. T. Zhang, "A fast key generation method based on dynamic biometrics to secure wireless body sensor networks for p-health," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol.*, Aug./Sep. 2010, pp. 2034–2036.

[14] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2011, pp. 1862–1870.

[15] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): Authentication for implanted medical devices," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 1099–1112.

[16] G. Zheng, G. Fang, R. Shankaran, and M. A. Orgun, "Encryption for implantable medical devices using modified one-time pads," *IEEE Access*, vol. 3, pp. 825–836, 2015.

[17] S. R. Moosavi, E. Nigussie, S. Virtanen, and J. Isoaho, "Cryptographic key generation using ECG signal," in *Proc. 14th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2017, pp. 1024–1031.

[18] M. Goresky and A. M. Klapper, "Fibonacci and Galois representations of feedback-with-carry shift registers," *IEEE Trans. Inf. Theory*, vol. 48, no. 11, pp. 2826–2836, Nov. 2002.

[19] J. Daemen and V. Rijmen, "Specification of Rijndael," in *The Design of Rijndael*. Berlin, Germany: Springer, 2002, pp. 31–50.

[20] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 1, pp. 60–68, Jan. 2010.

[21] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Plethysmogram-based secure inter-sensor communication in body area networks," in *Proc. IEEE Military Commun. Conf.*, Nov. 2008, pp. 1–7.

[22] F. Miao, L. Jiang, Y. Li, and Y.-T. Zhang, "Biometrics based novel key distribution solution for body sensor networks," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Sep. 2009, pp. 2458–2461.

[23] A. Banerjee, K. Venkatasubramanian, and S. K. S. Gupta, "Challenges of implementing cyber-physical security solutions in body area networks," in *Proc. Int. Conf. Body Area Netw.*, 2009, Art. no. 18.

[24] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1070–1078, Nov. 2012.

[25] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems," in *Proc. IEEE Annu. Conf. Eng. Med. Biol. Soc.*, Jan. 2005, pp. 2455–2458.

[26] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-22 Rev 1a, 2001.

[27] G. Zheng *et al.*, "Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks," *IEEE J. Biomed. Health Inform.*, vol. 21, no. 3, pp. 655–663, May 2017.

[28] N. Karimian, Z. Guo, M. Tehranipoor, and D. Forte, "Highly reliable key generation from electrocardiogram (ECG)," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 6, pp. 1400–1411, Jun. 2017.

[29] P. Li *et al.*, "High-performance personalized heartbeat classification model for long-term ECG signal," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 1, pp. 78–86, Jan. 2017.

[30] L. Sun, Y. Lu, K. Yang, and S. Li, "ECG analysis using multiple instance learning for myocardial infarction detection," *IEEE Trans. Biomed. Eng.*, vol. 59, no. 12, pp. 3348–3356, Dec. 2012.

[31] S. Kiranyaz, T. Ince, and M. Gabbouj, "Real-time patient-specific ECG classification by 1-D convolutional neural networks," *IEEE Trans. Biomed. Eng.*, vol. 63, no. 3, pp. 664–675, Mar. 2016.

[32] K. N. Plataniotis, D. Hatzinakos, and J. K. M. Lee, "ECG biometric recognition without fiducial detection," in *Proc. Biometrics Symp., Special Session Res. Biometric Consortium Conf.*, 2006, pp. 1–6.

[33] Y. Wang, F. Agrafioti, D. Hatzinakos, and K. N. Plataniotis, "Analysis of human electrocardiogram for biometric recognition," *EURASIP J. Adv. Signal Process.*, vol. 2008, p. 148658, Dec. 2007.

[34] H.-S. Choi, B. Lee, and S. Yoon, "Biometric authentication using noisy electrocardiograms acquired by mobile sensors," *IEEE Access*, vol. 4, pp. 1266–1273, 2016.

[35] F. Porée, G. Kervio, and G. Carrault, "ECG biometric analysis in different physiological recording conditions," *Signal, Image Video Process.*, vol. 10, no. 2, pp. 267–276, 2016.

[36] Y. N. Singh and P. Gupta, "ECG to individual identification," in *Proc. IEEE Conf. Biometrics, Theory, Appl. Syst.*, Sep./Oct. 2008, pp. 1–8.

[37] D. F. Dickinson, "The normal ECG in childhood and adolescence," *Heart*, vol. 91, no. 12, pp. 1626–1630, 2005.

[38] H. C. Bazett, "An analysis of the time-relations of electrocardiograms," *Ann. Noninvasive Electrocardiol.*, vol. 2, no. 2, pp. 177–194, 1997.

[39] S. R. Moosavi *et al.*, "End-to-end security scheme for mobility enabled healthcare Internet of Things," *Future Generat. Comput. Syst.*, vol. 64, pp. 108–124, Nov. 2016.

[40] S. R. Moosavi *et al.*, "SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways," *Procedia Comput. Sci.*, vol. 52, pp. 452–459, Jan. 2015.

[41] A. M. Rahmani *et al.*, "Smart e-health gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems," in *Proc. 12th Annu. IEEE Conf. Consum. Commun. Netw.*, Jan. 2015, pp. 826–834.

[42] J. Granados, A.-M. Rahmani, P. Nikander, P. Liljeberg, and H. Tenhunen, "Towards energy-efficient HealthCare: An Internet-of-Things architecture using intelligent gateways," in *Proc. Int. Conf. Wireless Mobile Commun. Healthcare*, 2014, pp. 279–282.

[43] J. S. Sahambi, S. N. Tandon, and R. K. P. Bhatt, "Using wavelet transforms for ECG characterization. An on-line digital signal processing system," *IEEE Eng. Med. Biol. Mag.*, vol. 16, no. 1, pp. 77–83, Jan./Feb. 1997.

[44] A. A. R. Bsoul, S.-Y. Ji, K. Ward, and K. Najarian, "Detection of P, QRS, and T components of ECG using wavelet transformation," in *Proc. IEEE Int. Conf. Complex Med. Eng.*, Apr. 2009, pp. 1–6.

[45] S. Z. Mahmoodabadi, A. Ahmadian, and M. D. Abolhasani, "ECG feature extraction using Daubechies wavelets," in *Proc. Int. Conf. Vis., Imag., Image Process.*, 2005, pp. 343–348.

[46] A. L. Goldberger *et al.*, "PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. e215–e220, 2000.

[47] H. S. Black and J. O. Edson, "Pulse code modulation," *Trans. Amer. Inst. Electr. Eng.*, vol. 66, no. 1, pp. 895–899, Jan. 1947.

[48] *MATLAB, R2016a*. MathWorks Inc., Natick, MA, USA, 2016.

[49] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul./Oct. 1948.

SANAZ RAHIMI MOOSAVI (S'15) received the M.Sc. (Tech.) degree in information technology, networked systems security from the Department of Information Technology and Communication Systems, University of Turku, Finland, in 2013, where she is currently pursuing the Ph.D. degree with the Department of Future Technologies. Her research interests include security and privacy, Internet of Things, smart healthcare systems, and lightweight cryptography techniques.

ETHIOPIA NIGUSSIE (S'06–M'11–SM'15) received the B.Sc. degree in electrical engineering from Addis Ababa University, Ethiopia, in 2000, the M.Sc. degree in electrical engineering from the KTH Royal Institute of Technology, Sweden, in 2004, and the D.Sc. (Tech.) degree in communication systems from the University of Turku, Finland, in 2010. She is currently an Adjunct Professor of self-aware networked systems with the University of Turku. Her current research interests are self-aware and adaptive systems design, security for low-power wireless networks, including hardware-enabled and smart healthcare systems.

MARCO LEVORATO (S'06–M'09) received the B.S. and M.S. degrees in electrical engineering (*summa cum laude*) from the University of Ferrara, Italy, in 2003 and 2005, respectively, and the Ph.D. degree in electrical engineering from the University of Padova, Italy, in 2009. He held post-doctoral appointments with Stanford University, the University of Southern California, and the KTH Royal Institute of Technology, Stockholm, Sweden. He is currently an Assistant Professor in computer science with the University of California at Irvine. He was a recipient of the Best Paper Award at the IEEE Globecom 2012, the UC Hellman Foundation Award, and has been twice nominated for the Best Young Researcher Award, Department of Information Engineering, University of Padova.

SEPPO VIRTANEN (S'00–M'04–SM'09) received the M.Sc. degree in electronics and information technology and the D.Sc. (Tech.) degree in communication systems from the University of Turku, Finland, in 1998 and 2004, respectively. Since 2009, he has been an Adjunct Professor of embedded communication systems with the University of Turku, where he also Heads the Master's Degree Programme in Information Security. His research currently focuses on information security issues in the communication and network technology domain, specifically focusing on design and methodological aspects of reliable and secure communication systems, and secure communication for IoT.

JOUNI ISOAHO received the M.Sc. (Tech.) degree in electrical engineering and the Lic.Tech. and Dr.Tech. degrees in signal processing from the Tampere University of Technology, Finland, in 1989, 1992, and 1995, respectively. Since 1999, he has been a Professor of communication systems with the University of Turku, Finland, where he is currently the Head of the Communication Systems Laboratory. His research interests include future communication system concepts, applications, and implementation techniques. His current special interests are in dynamically reconfigurable self-aware systems for future communication and interdisciplinary applications, including information security and dependability aspects.

Publication IV

End to-End Security Scheme for Mobility Enabled healthcare Internet of Things

Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Ethiopia Nigussie, Amir-Mohammad Rahmani, Seppo Virtanen, Hannu Tenhunen, Jouni Isoaho

Original published in Elsevier Future Generation Computer Systems (FGCS-2016), 2016, pages 108-124

Future Generation Computer Systems 64 (2016) 108–124

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

End-to-end security scheme for mobility enabled healthcare Internet of Things

Sanaz Rahimi Moosavi [a,*], Tuan Nguyen Gia [a], Ethiopia Nigussie [a], Amir M. Rahmani [a], Seppo Virtanen [a], Hannu Tenhunen [a,b], Jouni Isoaho [a]

[a] *Department of Information Technology, University of Turku, Turku, Finland*

[b] *Department of Industrial and Medical Electronics, KTH Royal Institute of Technology, Stockholm, Sweden*

ARTICLE INFO

Article history:
Received 1 October 2015
Received in revised form
15 February 2016
Accepted 24 February 2016
Available online 3 March 2016

Keywords:
End-to-end security
Internet of Things
Smart healthcare
Mobility
Session resumption

ABSTRACT

We propose an end-to-end security scheme for mobility enabled healthcare Internet of Things (IoT). The proposed scheme consists of (i) a secure and efficient end-user authentication and authorization architecture based on the certificate based DTLS handshake, (ii) secure end-to-end communication based on session resumption, and (iii) robust mobility based on interconnected smart gateways. The smart gateways act as an intermediate processing layer (called fog layer) between IoT devices and sensors (device layer) and cloud services (cloud layer). In our scheme, the fog layer facilitates ubiquitous mobility without requiring any reconfiguration at the device layer. The scheme is demonstrated by simulation and a full hardware/software prototype. Based on our analysis, our scheme has the most extensive set of security features in comparison to related approaches found in literature. Energy-performance evaluation results show that compared to existing approaches, our scheme reduces the communication overhead by 26% and the communication latency between smart gateways and end users by 16%. In addition, our scheme is approximately 97% faster than certificate based and 10% faster than symmetric key based DTLS. Compared to our scheme, certificate based DTLS consumes about 2.2 times more RAM and 2.9 times more ROM resources. On the other hand, the RAM and ROM requirements of our scheme are almost as low as in symmetric key-based DTLS. Analysis of our implementation revealed that the handover latency caused by mobility is low and the handover process does not incur any processing or communication overhead on the sensors.

1. Introduction

Recent advances in information and communication technologies have given rise to a new technology: Internet of Things (IoT) [1–3]. IoT enables people and objects in the physical world as well as data and virtual environments to interact with each other, hence realizing smart environments such as smart transport systems, smart cities, smart healthcare, and smart energy. The rising cost of healthcare, and the prevalence of chronic diseases around the world urgently demand the transformation of healthcare from a hospital-centered system to a person-centered environment, with a focus on citizens' disease management as well as their wellbeing [4]. It has been predicted that in the following decades, the way healthcare is currently provided will be transformed from hospital-centered, first to hospital-home-balanced in the 2020's, and then ultimately to home-centered in 2030's [5]. This essential transformation necessitates the fact that the convergence and overlap of the IoT architectures and technologies for smart spaces and healthcare domains should be more actively considered [4,6–8].

Security is a major concern wherever networks are deployed at large scales. IoT-based healthcare systems deal with human-related data. Although collected from innocuous wearable sensors, such data is vulnerable to top privacy concerns [9–12]. In IoT-based healthcare applications, security and privacy are among major areas of concern as most devices and their communications are wireless in nature [13]. An IP-enabled sensor in a Medical Sensor Network (MSN), for instance, can transmit medical data of patients to a remote healthcare service. However, in such scenarios, the conveyed medical data may be routed through an untrusted network infrastructure, e.g. the Internet. Hence, in healthcare IoT, security and privacy of patients are among major areas of concern. In this regard, the authentication and authorization of remote healthcare centers/caregivers and end-to-end data protection are

[*] Corresponding author.
E-mail address: saramo@utu.fi (S.R. Moosavi).

http://dx.doi.org/10.1016/j.future.2016.02.020
0167-739X/© 2016 Elsevier B.V. All rights reserved.

critical requirements as eavesdropping on sensitive medical data or malicious triggering of specific tasks can be prevented [14]. Due to direct involvement of humans in IoT-based healthcare applications, providing robust and secure data communication among healthcare sensors, actuators, patients, and caregivers are crucial. Misuse or privacy concerns may restrict people to utilize IoT-based healthcare applications.

Conventional security and protection mechanisms including existing cryptographic solutions, secure protocols, and privacy assurance cannot be re-used due to resource constrains, security level requirements, and system architecture of IoT-based healthcare systems [15]. To mitigate the aforementioned risks, strong network security infrastructures for a short and long-range communication are needed. There are significant security solutions to current wireless networks which are not directly applicable to IoT-based healthcare applications due to the following challenges [16]: (i) security solutions must be resource-efficient as medical sensors have limited processing power, memory, and communication bandwidth. (ii) Medical sensors can be easily lost or abducted as they are tiny in terms of size.

To deal with the mentioned challenges, Constrained Application Protocol (CoAP) [17] proposes Datagram Transport Layer Security (DTLS) [18] to be used for resource-constrained services/applications. DTLS is a complete security protocol as it offers authentication, key exchange, and protection of application data. An IoT-enabled application may be in one of the following four security modes: (i) *NoSec*, meaning that the DTLS is disabled and there is no protocol level security. However, the use of *IPsec* as network layer security is recommended. (ii) *Symmetric Key-based DTLS*, meaning that DTLS is enabled and symmetric key-based authentication is utilized. (iii) *Public Key-based DTLS*, meaning that DTLS is enabled and the resource constrained device has an asymmetric key pair. The public key is not embedded in an X.509 certificate. (iv) *Certificate-based DTLS*, meaning that DTLS is enabled and the constrained device has an asymmetric key pair. The X.509 certificate is signed by a Certificate Authority (CA). Medical sensors used in healthcare IoT have limited ROM, RAM, CPU and energy resources. Thus, new challenges arise when using certificates on such resource-constrained devices.

In [19], as shown in Fig. 1, we presented a secure and efficient authentication and authorization architecture for IoT-based healthcare systems using smart e-health gateways in a distributed fashion. More precisely, we proposed to exploit the smart gateways' advantageous property of being non-resource constrained for outsourcing the processing burden of end-user authentication and authorization from tiny medical sensors. The system architecture of our proposed IoT-enabled healthcare system includes the following main components: (i) *Device Layer*: enabled with ubiquitous identification, sensing, and communication capacity, in which bio-medical and context signals are captured from home/hospital room(s) or patients' body to be used for treatment and diagnosis of medical states. (ii) *Fog Layer*: consists of a network of distributed smart e-health gateways where those gateways support various communication protocols and acts as a touching point between the device layer and cloud layer. (iii) *Cloud Layer*: this layer is composed of the remote healthcare server and patients' classified health data. (iv) *Web Interface*: as a graphical user interface to be used by remote caregivers for final visualization and apprehension.

Recently, there have been efforts in designing *Smart e-Health Gateways* for Healthcare Internet of Things (Health-IoT) systems [4]. In a smart home/hospital, where the mobility and location of patients are confined to hospital facilities or buildings, gateways can play a key role. The stationary nature of such gateways enables them with the exclusivity of being non-resource constrained in terms of power consumption, memory, and communication bandwidth. By providing the necessary security context to the medical sensors, smart gateways remove the need to authenticate and authorize remote healthcare centers/caregivers from the sensors. Therefore, any malicious activity can be blocked before entering to a medical constrained domain. For this purpose, we employed the certificate-based DTLS handshake as it is the main transport layer security solution for IoT.

In healthcare IoT systems, improving patients' quality of life is important to mitigate the negative effects of being hospitalized. Providing patients with the possibility to walk around the medical environments knowing that the monitoring of their health condition is not interrupted is an important feature. Enabling mobility support for patient monitoring systems offers a high quality of medical service as it allows patients to move around freely within the premises. Patients do not need to be worried about moving around as the system can enable mobility while monitoring their vital signs continuously.

In our previous work [19], the main focus was on the analysis and development of authentication and authorization between peers rather than end-to-end security. In [20], we proposed a session resumption-based end-to-end security scheme for healthcare IoT systems to securely and efficiently manage the communication between medical sensors and remote healthcare centers/ caregivers. The proposed scheme relied on the certificate-based DTLS handshake between non-resource-constrained distributed smart gateways and end-users at the start of the communication (initialization phase). To provide end-to-end security, the session resumption technique without server-side state is utilized. The session resumption technique has an abbreviated form of the DTLS handshake and it neither requires heavy-weight certificate-related nor public-key operations as it relies on the previously established DTLS connection.

In this article, an end-to-end security scheme for mobility enabled healthcare IoT is proposed. The main contributions of this article, which is a major extension of our recent works published in [19,20], are twofold. First, we propose an end-to-end security scheme for healthcare IoT with the explicit consideration of mobility for medical sensors. We exploit the concept of fog layer in IoT for realizing efficient and seamless mobility since fog extends the cloud paradigm to the edge of the network. Second, we analyze the characteristics of the proposed scheme in terms of security and energy-performance on a prototype of a healthcare IoT system through simulation and hardware/software prototype.

The remainder of the article is organized as follows: in Section 2, the related work and motivation are discussed. Section 3 presents our proposed system architecture for healthcare IoT. In Section 4, the requirements of secure and efficient communication for healthcare IoT system are presented and discussed. Section 5 presents the proposed end-to-end security scheme for healthcare IoT systems. Fog layer-based mobility for our proposed end-to-end security scheme is presented in Section 6. Experimental results including energy-performance and security evaluations are provided and discussed in Section 7. Finally, Section 8 concludes the article.

2. Related work and motivation

For the discussion of related work, we recognize three main research directions: (i) IoT-based Healthcare Security, (ii) Smart Gateways, and (iii) Mobility solutions for IoT systems.

2.1. IoT-based healthcare security

CodeBlue is one of the most popular healthcare research projects that has been developed at the Harvard sensor network Lab [21]. In this approach, several medical sensors are placed on a patients' body. CodeBlue has been expected to be deployed in in-hospital emergency care, stroke patient rehabilitation and

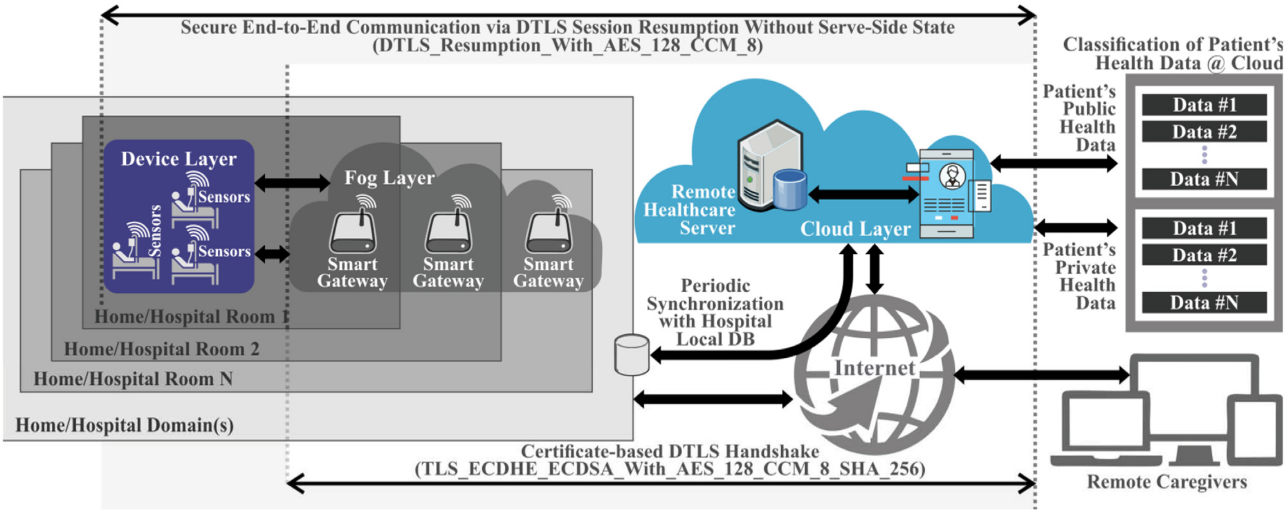

Secure End-to-End Communication via DTLS Session Resumption Without Serve-Side State
(DTLS_Resumption_With_AES_128_CCM_8)
Classification of Patient's Health Data @ Cloud
Patient's Public Health Data
Data #1
Data #2
Data #N
Patient's Private Health Data
Data #1
Data #2
Data #N
Device Layer
Sensors
Sensors
Sensors
Fog Layer
Smart Gateway
Smart Gateway
Smart Gateway
Remote Healthcare Server
Cloud Layer
Periodic Synchronization with Hospital Local DB
Internet
Home/Hospital Room 1
Home/Hospital Room 2
Home/Hospital Room N
Home/Hospital Domain(s)
Certificate-based DTLS Handshake
(TLS_ECDHE_ECDSA_With_AES_128_CCM_8_SHA_256)
Remote Caregivers

Fig. 1. The architecture of a healthcare IoT system with secure end-to-end communication.

disaster response. The authors of CodeBlue admit the necessity of security for IoT-based medical applications. However, the security aspects of CodeBlue are still left as future work. Lorincz et al. [22] suggest that Elliptic Curve Cryptography (ECC) [23] and TinySec [24] are efficient solutions to be used for key generation and symmetric encryption in the CodeBlue project, respectively. Kambourakis et al. discuss some attack models and security threats concerning the CodeBlue project: denial-of-service attack, snooping attack, grey-hole attack, sybil attack, and masquerading attacks [25]. An in-hospital patient monitoring system called MEDiSN has been developed at Johns Hopkins University [26]. It consists of multiple physiological motes which are battery powered and equipped with medical sensors in order to collect patients' medical and physiological health information. The MEDiSN architecture focuses on reliable communication, routing, data rate, and QoS [26]. In their proposed architecture, the authors of MEDiSN acknowledged the necessity of having encryption for the physiological monitors. However, they did not mention which cryptosystems have been used for the data confidentiality and integrity. Although the authors claim that security is provided by the MEDiSN architecture, their study did not reveal much information regarding the security implementation. An architecture called Sensor Network for Assessment of Patients (SNAP) [13] has been proposed to address the security challenges concerning the wireless health monitoring systems. However, the main problem of the aforementioned architecture is that it does not authenticate users when providing medical data. Furthermore, the data collected from medical sensors are conveyed to a controller in plaintext format. Hence, the medical data of the patients can be modified or intercepted by a malicious user. In [27], a lightweight identity-based cryptography solution called IBE-Lite has been proposed. The basic idea of IBE-Lite is to balance security and privacy with availability. Nevertheless, several security and privacy issues as well as efficiency problems are recognized in IBE-Lite. First, in their work, Tan et al. do not consider sensor to base station/end-user data authentication. Therefore, falsified medical information can be introduced or treated as authentic due to the lack of authentication schemes. Second, IBE-Lite cannot resist against replication attacks. Consequently, an adversary can insert malicious medical sensors into the network.

To establish interoperable network security between end-peers from independent network domains, variants of conventional end-to-end security protocols have been recently proposed among which Datagram Transport Layer Security (DTLS) is one of the most relevant protocols [18]. In this regard, Hummen et al. [14] present an implementation of a delegation architecture based on an off-path delegation server. Their proposed delegation-based architecture relies on a centralized delegation server. Due to this, their proposed architecture lacks scalability and reliability. More precisely, their architecture cannot be extended to be employed for multi-domain infrastructures, e.g. large in-home/hospital domains. Also, their proposed architecture suffers from a considerable network transmission overhead resulting to a long transmission latency. Moreover, if an adversary performs a Denial of Service (DoS) attack or compromises the delegation server, a large quantity of stored security context of a constrained domain can be retrieved.

2.2. *Smart e-health gateway*

There have been many efforts in designing gateways for one or several specific applications and architectural layers. Muller et al. [6] present a gateway called SwissGate which handles and optimizes the operation of sensor networks. They transparently employ their proposed gateway on home automation applications. Shen et al. [7] propose a prototype of a smart 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) border router that makes local decisions of users' health states based on a Hidden Markov Model. Finally, Rahmani et al. [4] present a smart e-health gateway called *UT-GATE* in order to bring intelligence into IoT-based ubiquitous healthcare systems. These gateways are intelligent in the sense that they have been empowered to autonomously perform local data storage and processing, to learn, and to make decisions at the edge of the network (i.e., in a distributed fashion), thanks to the provided embedded processing power and storage capabilities of the gateways. A smart gateway can rapidly provide preliminary results and reduce the redundant remote communication to cloud servers by using data aggregation, embedded machine learning, and inferences, thus offering the basic services at the edge of the network. In this way, remote cloud computers will just provide premium services which are often computationally intensive and require access to the central database.

In a smart home/hospital, gateway is in a unique position between Body/Patient/Local Area Network (BAN/PAN/LAN) and Wide Area Network (WAN). This promising opportunity can be exploited by different means such as collecting health and context information from those networks and providing different services accordingly. As mentioned above, compared to the conventional gateways which often just perform basic functions such as translating between the protocols used in the Internet and sensor networks, smart e-health gateways are empowered with the property of being non-resource constrained in terms of processing power, memory, power consumption, and communication bandwidth. In [19,20], we demonstrated the use of a smart gateway to handle medical sensors' main computation and communication overhead that results from end-user authentication and authorization.

2.3. Mobility solutions for IoT systems

In [28], Valenzuela et al. propose a solution to support mobility for in-home health monitoring systems using wearable sensors. This approach utilizes a coordinator sensor attached to patients' body that is responsible for all the communications between wearable sensors and network Access Points (APs). Jara et al. in [29–31], propose a solution to support the mobility of sensors employed to monitor patients in hospital environments. This approach supports intra-mobility exploiting elements such as sink nodes and gateways in their proposed architecture. This proposal supposes that each mobile node has a base network and can move into other networks. Fotouhi et al. [32] present a handover approach for mobility support in Wireless Sensor Networks (WSNs) which can be easily employed for Body Sensor Networks (BSNs) [33,34]. In their work, different parameters are utilized to specify the time for handover, but the most important ones are the Received Signal Strength (RSS) and the sensor velocity. To verify the quality of the link as well as to decide handover mechanism, this solution requires a continuous exchange of probe or acknowledge messages between the sensor and the corresponding access point. However, this continuous messages exchange weaken the network in terms of transmission overhead, memory, and energy consumption.

In [19], our main focus was on the development and analysis of a secure and efficient authentication and authorization architecture, while in [20] we proposed a secure end-to-end communication scheme via session resumption for healthcare IoT system. In these works patients' mobility support was not considered. This article essentially extends our previous works by incorporating enhanced mobility while providing secure end-to-end communication. Our proposal is motivated by the fact that to enable mobility for healthcare IoT systems, an intermediate computing layer, that is the fog layer [35], can be exploited between the device layer and the cloud layer. More precisely, the mobility support can be provided to the medical sensors ubiquitously from the fog layer so that no more reconfiguration is needed in the resource-constrained device layer.

3. Healthcare IoT system architecture

Healthcare IoT systems are distinct in that they are built to serve human beings, which inherently raises the requirements of safety, security, and reliability. Moreover, they have to provide real-time notifications and responses regarding the status of patients. In a typical healthcare IoT system, to monitor patients' activities and vital signs, the system has to ensure the safety of patients. In addition, physicians, patients, and other caregivers demand a dependable system in which the results are accurate and timely, and the service is reliable and secure. To guarantee these requirements, the smart components in the system require a predictable latency and reliable communication with the upper computing layer. The conventional cloud-based approaches cannot assure the requirements of healthcare IoT systems, as the connection to the cloud is less reliable and may incur additional latency. In this article, we utilize a novel system architecture as a suitable paradigm to address the aforementioned requirements.

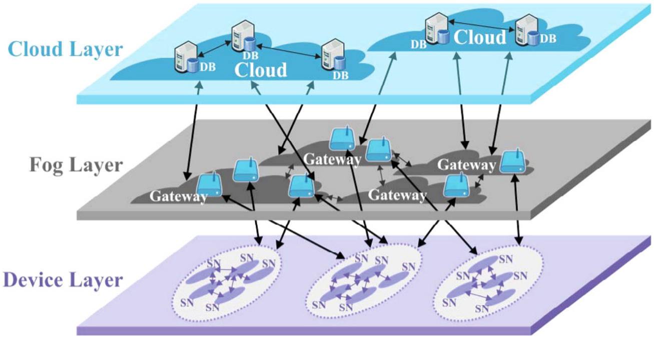


Fig. 2. The three-tier system architecture of the healthcare IoT system (SN and DB stand for Sensor Node and Database, respectively).

Fog computing is a paradigm extending cloud computing and its services to the edge of the network. Fog distinguishes from cloud in its proximity to end-users/devices, dense geographical distribution, real-time interaction, support for mobility, heterogeneity, interoperability and pre-processing along with interplay with the cloud. Fog devices are heterogeneous in nature, ranging from end-user devices and access points to edge routers and switches allowing their use in wide variety of environments. Fog services can be implemented in a variety of devices ranging from smart phones to edge routers and access points with a reasonable support of local storage and processing.

The three-tier system architecture of the healthcare IoT system on which we apply our end-to-end security scheme is shown in Fig. 2. In such a system, patients' health-related information is recorded by implanted or wearable medical sensors with which the patient is equipped for personal monitoring of multiple parameters. This health-related data may also be supplemented with context information, i.e. time, date, location, and relevant environment information which enables the recognition of abnormal patterns and the making of more precise inferences. The functionality of each layer in this architecture is as follows:

(i) **Device layer**: the lowest layer consisting of several physical devices including implantable or wearable medical sensors that are integrated into a tiny wireless module to collect contextual and medical data. Enabled by the ubiquitous identification, sensing, and communication capacity, biomedical and context signals are captured from the body and/or the room. The signals are used for managing the treatment and diagnosis of medical conditions. The signal is then transmitted to the upper layer (i.e., smart gateways in the Fog layer) via wireless or wired communication protocols such as IEEE 802.15.4, Bluetooth LE, Wi-Fi, etc.

(ii) **Fog layer**: the middle layer consists of a network of interconnected smart gateways. Cloud computing paradigm is an efficient alternative to establishing and maintaining private servers and data centers. Particularly, due to its "pay-as-you-go" business model, it gives more efficiency and freedom to web applications. However, these features demand high computation and storage as well as batch processing. This model enables developers and end-users to exploit cloud services with a minimum knowledge of the underlying hardware and infrastructure. However, this becomes an issue in applications which require low latency (emergency care). Such challenges are addressed in the Fog computing paradigm by extending the cloud services to the edge of the network. As mentioned before, we exploit Smart e-Health gateways which support different communication protocols, act as a touching point between a sensor network and the local switch/Internet. A smart gateway receives data from different sub-networks, performs protocol conversion, and provides other higher level services. It acts as repository (local database) to temporarily store sensors' and users' information, and provides intelligence at the edge of the network. In addition, by taking responsibility for handling some computational and processing burdens of the sensors and the cloud, a smart gateway at the fog layer can cope with many challenges such as energy efficiency, scalability, and reliability issues [35].

(iii) **Cloud layer**: The cloud layer includes broadcasting, data warehousing and big data analysis servers, and a hospital local database that periodically performs data synchronization with the remote healthcare database server in the cloud. In the cloud layer, accessibility to patients-related health data is classified as public data (e.g., patients' ID or blood type) and private data (e.g., DNA).

4. Requirements of secure and efficient communication for healthcare IoT system

In this section, various criteria that represent desirable characteristics of secure communication for a healthcare IoT system are presented.

Data confidentiality: All relevant data being transmitted between communicating peers remains unknown for others. To prevent patients' health data from the leakage attack, such data needs to be kept confidential. This can be achieved using strong encryption schemes meaning that even if an adversary eavesdrops on transmitted packets, he/she cannot easily get access to them. Data confidentiality should also be resistant to any device compromise attack, for example, medical sensor or smart gateway compromise attack.

Data integrity: Ensures that patients' health data is received in the exact way as it was sent and it has not been manipulated in transit. Since in healthcare IoT systems most devices and their communications are wireless in nature, maintaining data integrity is a necessary task. To provide data integrity, a Cyclic Redundancy Checksum (CRC), that is used to detect random errors during packet transmission, or a Message Authentication Code (MAC) are usually employed.

Mutual authentication and authorization: Allows the communication peers to ensure and validate the identity of each other. Mutual authentication needs to be done in the whole system so that private medical information cannot be accessed by any unauthorized user. This way, an adversary cannot claim to be a valid user to obtain patients' health data or inject invalid information. Authentication can be achieved by sending a MAC along with the message. On the other hand, authorization indicates that only authorized users/sensors can access resources and services in an IoT-enabled healthcare system.

Data freshness and forward security: Data freshness indicates that patients' health data is fresh and an adversary has not replayed the previously transmitted data. The property of forward security ensures that the revelation of current encrypted medical sensors' data does not threaten the security of the previously transmitted health data.

Availability: Ensures that medical sensors and all services utilized in an IoT-enabled healthcare system can constantly provide services to authorized users whenever required (despite of possible Denial of Service (DoS) attacks). Fulfilling availability, however, is a difficult task as DoS attacks can exhaust the power supplies of the medical sensors or heavily reduce the network performance by jamming the radio channel.

Scalability and lightweight solutions: Scalability refers to the capability of an IoT-enabled healthcare system to continue functioning well even if such a system may be modified in terms of size (e.g. sensors, hardware or services may be added/removed). In emergency situations, an IoT-enabled healthcare system should have the capability of fast reaction without compromising the patients' security and privacy. It is necessary to minimize communication, computation, and memory overhead of medical sensors due to the low capabilities of these sensors. Hence, cryptographic solutions being proposed should be lightweight to fulfill the aforementioned requirements.

Data access control: In healthcare IoT systems, caregivers (i.e. doctors, pharmacists, nurses, etc.) are directly involved with patients' physiological and medical data. Thus, a real-time role-based access control needs to be available to restrict caregivers' access based on their privileges.

Patient consent: Patients' consents are always essential when caregivers decide to circulate their medical records to another healthcare sector/hospital in order to provide higher quality of healthcare. Informed consent refers to the process of getting patients' permission before conducting medical procedures/ interventions (e.g. medical treatment's nature, consequences, harms, risks, and benefits). Informed consent is a fundamental principle of healthcare and it is collected according to the guidelines of medical and research ethics.

Mobility support: Mobility is one of the most important challenges in healthcare IoT systems which increases the applicability of these technologies. The mobility support enables patients to go for a walk around the medical domain(s) while he/she is continuously monitored. Furthermore, mobility allows the patient to move from his/her base MSN to other rooms for medical tests without losing the continuous monitoring.

End-to-end security: End-to-end security is one of the major requirements in healthcare IoT systems. This feature enables the end-points of a healthcare IoT system, that is caregivers and medical sensors, to securely communicate with each other beyond the independent network.

5. End-to-end security scheme for healthcare IoT system

In [19], we presented a secure and efficient authentication and authorization architecture for healthcare IoT system using smart e-health gateways called *SEA* (lower black arrow shown in Fig. 1). In [20], we presented a comprehensive end-to-end security scheme for healthcare IoT systems using the session resumption technique (upper black arrow shown in Fig. 1). Before presenting the fog layer-based mobility for our proposed end-to-end security scheme, we briefly explain our previous work in this section.

5.1. Secure and efficient authentication and authorization architecture

In the paradigms of healthcare IoT, not only data can be collected by smart devices (medical sensors) and transmitted to end-users (caregivers), but end-users can also access, control, and manage medical sensors through the Internet. Since patients' health data is the basis for enabling applications and services in healthcare IoT, it becomes imperative to provide secure end-to-end communication between end-users and medical sensors to protect the exchange of health data. In addition, privacy of patients and key negotiation materials should be protected to prevent anyone other than the negotiation peers from learning the contents of the negotiations. It is also important that malicious activities be blocked at the entrance to MSNs. Hence, mutual authentication and authorization of end-users and devices used in healthcare IoT systems is a crucial task.

Our proposed architecture called *SEA* exploits the role of smart e-health gateways in the fog layer to perform the authentication and authorization of remote end-users securely and efficiently on behalf of the medical sensors [19]. By providing the established

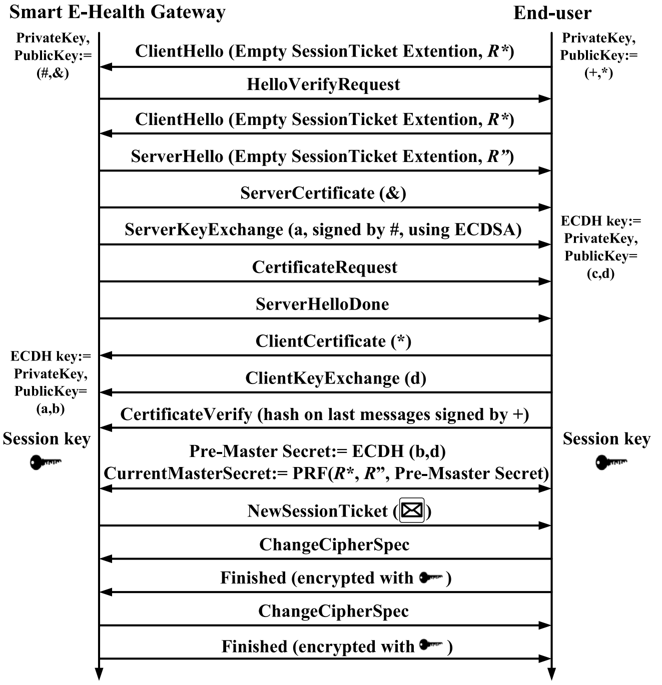

Smart E-Health Gateway
End-user
PrivateKey, PublicKey:= (#,&)
PrivateKey, PublicKey:= (+,*)
ClientHello (Empty SessionTicket Extention, R*)
HelloVerifyRequest
ClientHello (Empty SessionTicket Extention, R*)
ServerHello (Empty SessionTicket Extention, R”)
ServerCertificate (&)
ServerKeyExchange (a, signed by #, using ECDSA)
ECDH key:= PrivateKey, PublicKey= (c,d)
CertificateRequest
ServerHelloDone
ClientCertificate (*)
ECDH key:= PrivateKey, PublicKey= (a,b)
ClientKeyExchange (d)
CertificateVerify (hash on last messages signed by +)
Session key
Session key
Pre-Master Secret:= ECDH (b,d)
CurrentMasterSecret:= PRF(R*, R”, Pre-Msaster Secret)
NewSessionTicket (✉)
ChangeCipherSpec
Finished (encrypted with)
ChangeCipherSpec
Finished (encrypted with)

Fig. 3. Message flights for the full certificate-based DTLS handshake while issuing a session ticket [19].

connection context to the medical sensor nodes, these devices no longer need to authenticate and authorize a remote healthcare center or a caregiver. Thus, any malicious activity can be blocked before entering to a constrained medical domain. The architecture of our proposed healthcare IoT monitoring system in home/hospital domain(s) is shown in Fig. 1. In such an architecture, patient health-related information is recorded by body-worn or implanted sensors, with which the patient is equipped for personal monitoring of multiple parameters. This health data can be also supplemented with context information (e.g., date, time, location, and temperature) which enables to identify unusual patterns and make more precise inferences about the situation. Our proposed SEA focuses on a fact that the smart e-health gateway and the remote end-user have sufficient resources to perform various heavy-weight security protocols as well as certificate validation. To provide end-to-end communication between a remote end-user and a constrained medical device, distributed smart e-health gateways are introduced to build a transport layer security protocol that is Datagram Transport Layer Security (DTLS) [18].

DTLS handshake protocol is the main transport layer security solution for IoT. As Fig. 3 presents, a full handshake begins with a *ClientHello* message, that includes the security parameters for the connection which is used later during the handshake to compute the pre-master secret key. Flight 3 contains additional cookie from *ClientHelloVerify*. Flight 4 includes several messages and starts with *ServerHello* message which contains the negotiated cipher suite for the current handshake and the smart gateway's random value which is utilized later during the handshake to compute the master secret key. The agreed cipher suite relies on supported cipher suites by the end-user. If the smart gateway and the end-user cannot agree on a common cipher suite, the handshake is canceled with a *HandshakeFailure* alert message. The next message of flight 4 is smart gateway's *Certificate* message which holds gateway's certificate-chain. The first certificate in the chain includes the smart gateway's public key which is created using *OpenSSL* in version of 1.0.1.j. OpenSSL is an open source project for implementing SSL, TLS and various cryptography libraries such as symmetric key, public key, and hash algorithms. It is commonly utilized for creating and managing keys and certificates. Once the certificate is validated, the end-user can extract the smart gateway's public key. The *CertificateRequest* is only sent in a mutual handshake and includes the lists of the smart gateway's valid certificates. The *ServerKeyExchange* message is only sent with specific cipher suites that need more parameters in order to compute a master secret key. The cipher suite employed in this work is *TLS_ECDHE_ECDSA_WITH_AES*_128_*CCM*_8_*SHA*_256. The name indicates the use of elliptic cryptography, particularly-*Elliptic Curve Diffie-Hellman* (*ECDH*) and *Elliptic Curve Digital Signature Algorithm* (*ECDSA*). Furthermore, for encryption AES-based CCM with an IV of 8 bytes is used. With this cipher suite, ServerKeyExchange message contains the ECDH public key of the smart gateway and the detail of the associated elliptic curve. The *ServerHelloDone* message announces the end of flight 4 messages. The first message of flight 5 is the end-user's certificate in case mutual authentication is run. *ClientKeyExchange* includes additional parameters utilized to compute the master secret key. In this case, the ECDH public key of the smart gateway is conveyed. *CertificateVerify* is a message which enables the end-user to prove to the smart gateway that it carries the private key which corresponds to the public key contained in the certificate. Thus, it is only transmitted in the mutual authentication. With the *ChangeCipherSpec* message, the end-user informs the smart gateway that next messages will be encrypted using the agreed cipher suites and secret keys. The *Finished* message includes the encrypted hash over all flight messages which ensure that both peers have been performing handshake based on unmodified flight messages and the handshake is performed successfully. In flight 6, the smart gateway responds with its own ChangeCipherSpec and Finished messages. With the Finished messages both peers agree to send and receive securely protected application information over this connection. Upon this connection setup, as shown in Fig. 4, the remote end-point and the smart e-health gateway mutually authenticate each other.

It is supposed that within the certificate-based DTLS handshake, from one hand, the smart gateway authenticates (*Auth-req.1*) the remote end-user through certificates. In this regard, similar to current web browsers, smart gateways hold a pool of trusted certificates. On the other hand, the smart gateway either authenticates (*Auth-req.2*) to the remote end-user through certificates within the DTLS handshake or based on an application-level password once the handshake is terminated. Once the mutual authentication between the end-user and the smart gateway is done successfully, the end-user authorizes (*Authz.*) as a trusted entity so that a data query from the end-users' side is transmitted to the medical sensor through the smart gateway. To facilitate the security and authorization of communication, it is required that both entities, the constrained medical sensor and the smart gateway, also mutually authenticate (*Mut-auth.*) one another once during the initialization phase. In SEA, this is done by performing a public key-based DTLS handshake between both entities. Although symmetric key-based DTLS handshake provides an efficient alternative to public key-based DTLS handshake, the symmetric key-based handshake needs secret keys to be pre-shared and readily available at both communication end-points. Moreover, compared to the symmetric key-based DTLS handshake, obtaining secret points in a public key-based handshake implies the computation of elliptic curve discrete logarithm problem. Since solving the discrete logarithm problem is as hard as integer factorization, this problem cannot be solved effortlessly [23].

Once mutual authentication and key exchange protocol is done, it is required that both peers agree upon a common key. This shared common key can be generated using an already agreed elliptic curve between the both peers. Using the shared common key, one peer (i.e., constrained medical sensor) encrypts the gathered

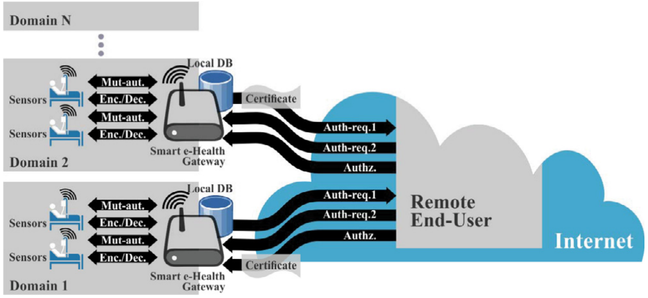


Fig. 4. The proposed SEA architecture overview using distributed smart e-health gateways.

patients' medical data applying the efficient *Advanced Encryption Standard* (*AES-CCM*) [36] algorithm and transmits the encrypted medical information (*Enc./Dec.*) to the smart e-health gateway and vice versa. AES-CCM offers confidentiality, integrity, and authentication of payload compared to other commonly known symmetric encryption/decryption algorithms (e.g., RC5, and Triple-DES), it is known as one of the most efficient ones. Moreover, AES is supported by many constrained devices used for IoT platforms. This make AES-CCM a desirable encryption/decryption algorithm choice for constrained devices.

Our SEA architecture achieved the following benefits: (i) network transmission overhead and latency were reduced compared to the most recently proposed architectures. This is because a great part of the work, that is authentication and authorization of a remote end-user/healthcare center, is shifted to be performed by distributed smart e-health gateways. (ii) the privacy of patients, vital certificates, and key negotiation materials were effectively protected, and (iii) the scalability and reliability of the system were enhanced as the architecture was changed from centralized to distributed.

5.2. The proposed end-to-end security scheme

In SEA [19], our main focus was on the development and analysis of an authentication and authorization architecture for IoT-enabled healthcare systems rather than end-to-end secure communication. In [20], we enabled end-to-end secure communication between end-points of a healthcare IoT system (i.e., medical sensors and end-users) by developing a session resumption-based scheme which offloads the encrypted session states of DTLS towards a non-resource-constrained end-user. The main motivation to employ the DTLS session resumption is to mitigate the overhead on resource-constrained sensors. Because, transmitting and processing of messages in the certificate-based DTLS handshake are resource intensive tasks. The session resumption technique is an extended form of the DTLS handshake which enables a client/server to continue the communication with a previously established session state without compromising the security properties. The session resumption approach improves the performance of the DTLS handshake in terms of required bandwidth, computational overhead, and number of transmitted messages. The main idea to employ session resumption is to perform heavy-weight operations only once, during an initial DTLS handshake connection (initialization) phase. Thus, the peers need to keep minimal session state, even after the session is terminated. The session resumption enables the peers to resume the secure connection without the need for running expensive operations and transmitting long certificates.

Two types of DTLS session resumption techniques have been proposed by IETF for constrained network environments [17]. (i) *Abbreviated DTLS handshake* where both peers have similar resources and both peers maintain session state through connections. (ii) *DTLS session resumption without server-side state* which is an extension of DTLS handshake that allows a server to offload the encrypted session state towards a non-resource-constrained client [37]. In [20], we employed the second type of session resumption (i.e. without server-side state) that offloads the encrypted session state of the tiny sensors towards the non-resource-constrained end-users/caregivers [18,37]. This is due to the asymmetry in resources between medical sensors and end-users/caregivers considering the constrained nature of sensors.

Before enabling secure end-to-end communication, as we presented earlier, a full certificate-based DTLS handshake needs to be performed once by the end-user and the smart e-health gateway (initialization phase). The protocol flow of the full certificate-based DTLS handshake while issuing a session ticket (to be used later in DTLS session resumption) is shown in Fig. 3. Here, the client (i.e. end-user) indicates its support for session resumption with an empty session resumption extension in the *ClientHello* message. On the other hand, the server (i.e. medical sensor) indicates its support for session resumption with an empty session resumption extension in the *ServerHello* message. In addition, during the handshake procedure, the smart gateway needs to build a new session ticket which holds: (i) the key name that recognizes the key utilized to encrypt the state, (ii) the validation of the ticket, and (iii) the encrypted state. Once the full certificate-based DTLS handshake between the aforementioned end-points is done successfully, the smart gateway updates the medical sensor about the validity of the end-user as well as the status of the DTLS handshake. This is done by encrypting the respective information using AES-CCM encryption algorithm. The AES-CCM algorithm ensures the confidentiality, integrity and authentication of the transmitted payloads. Here, the encryption key is used as secret key, which is shared between the smart gateway and the medical sensor and generated by utilizing the mutually agreed elliptic curve cryptographic algorithm. More details regarding the shared secret key generation can be found in [19]. This enables medical sensors to perform the session resumption with authorized and validated end-users.

To provide secure end-to-end communication between an end-user and a medical sensor, the end-user needs to initiate the session resumption mechanism with the sensor by sending a *ClientHello* message (Fig. 5). This time, the *ClientHello* message comprises a session resumption extension maintaining the session ticket and a random value R^*. During this step, the medical sensor uses the received encrypted and authorized session update from the smart gateway in order to resume the DTLS connection which has previously been established between the end-user and the smart gateway. The protocol flow for the DTLS session resumption without server-side state used in this work is shown in Fig. 5. Upon receiving the *SessionTicket* extension, the medical sensor which acts as a server needs to decrypt and verify the correctness of the ticket using the corresponding key which is the pre-master secret. When the session ticket is completely verified, the sensor responds with a *ServerHello* message holding an empty session resumption extension and a random value R''. In the same flight, the sensor also issues a new session ticket, which contains the information of the current state, that is, the current master secret. The current master secret is computed using the Pseudo Random Function (PRF), that is, a HMAC-based secret expansion function, over the previous master secret key (pre-master secret) and the exchanged random values R^* and R'', respectively. The random values provide the property of forward secrecy meaning that revelation of the current single key just allows access to the information of that session and does not threaten the security of the previous DTLS sessions. The new session ticket is conveyed through the *NewSessionTicket* message

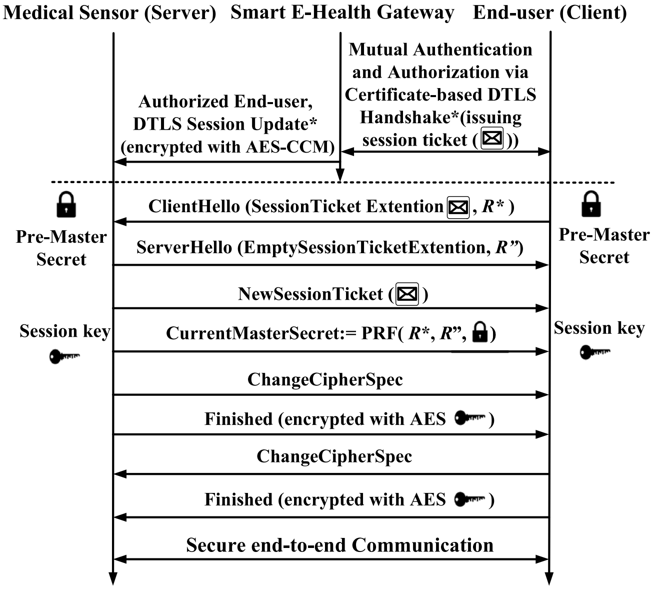

Medical Sensor (Server)
Smart E-Health Gateway
End-user (Client)
Mutual Authentication and Authorization via Certificate-based DTLS Handshake*(issuing session ticket (☒))
Authorized End-user, DTLS Session Update* (encrypted with AES-CCM)
Pre-Master Secret
ClientHello (SessionTicket Extention ☒, R*)
Pre-Master Secret
ServerHello (EmptySessionTicketExtention, R")
NewSessionTicket (☒)
Session key
CurrentMasterSecret:= PRF(R*, R", 🔒)
Session key
ChangeCipherSpec
Finished (encrypted with AES 🔑)
ChangeCipherSpec
Finished (encrypted with AES 🔑)
Secure end-to-end Communication

Fig. 5. The proposed session resumption based end-to-end security for healthcare Internet of Things [20].

and kept by the end-user for a possible subsequent session resumption. This way the resource-constrained sensor offloads the computational and processing burden of its state towards the non-resource-constrained end-user. Later, by exchanging the *ChangeCipherSpec* messages, the new keying material is utilized in order to secure the communication channel. Finally, by exchanging the *Finished* messages the correctness of the agreed keys and the integrity of all exchanged messages are verified. This concludes the handshake and provides the exchange of secured application data.

In this work, to generate the *SessionTicket*, the revised version of recommended ticket construction proposed in [37] is used. This is because the recommended ticket construction leads to an excessive ticket size for resource-constrained network environments. Therefore, it is necessary to provide a revised version of the recommended ticket construction that will take the constraints of the device/network into account with respect to the transmission overheads. The *NewSessionTicket* message includes a lifetime value and a session ticket. The lifetime value represents the number of seconds until the session ticket expires. The structure of the session ticket is opaque to the communicating peers and only the ticket issuer can access the session ticket information. The recommended ticket structure presented in [37] suggests to use AES-CCM for encryption with a 12 byte Initialization Vector (IV) and a 32 byte MAC based on HMAC-SHA-256. However, in this work, an 8-byte MAC based on HMAC-SHA-256 and a 12-byte IV are utilized, as they are the recommended cipher suites for secure CoAP over DTLS [17].

The major advantages offered by our scheme compared to the conventional end-to-end security solution [38] can be found in [20]. We applied our proposed session resumption-based end-to-end security scheme for healthcare IoT to the full system architecture shown in Fig. 1. As can be seen from the architectural viewpoint, the end-to-end security is fulfilled by (i) using the full initial certificate-based DTLS between end-users and smart gateways and (ii) utilizing session resumption technique which enables end-users and sensors to directly communicate and transmit the encrypted health-related information. The full procedure considerably alleviates the processing load on tiny sensors in terms of authentication, authorization, certificate related functionalities, and public key cryptography operations.

6. Fog layer-based mobility for the proposed end-to-end security scheme

Mobility support is one of the most important issues in healthcare IoT systems. In such systems, improving patients' quality of life is essential. Providing patients with the possibility to walk around the hospital wards knowing that the monitoring of their health condition is not interrupted is an essential feature. Using a portable patient monitoring system offers a high quality of medical service by providing freedom of movement to patients. Mobility enables patients to go for a walk around the medical domain(s) while they are monitored. In addition, mobility allows the patient to move from his/her base MSN to other rooms for medical tests without losing the continuous monitoring. This scenario can also be extended to other environments such as a nursing house or in-home patient monitoring. The main goal of the continuous monitoring in the healthcare IoT systems is to achieve a knowledge base from the patient which enables the remote server and the Knowledge Base System (KBS) to detect symptoms, predict, and manage the illnesses. Mobility can be categorized into two main topics denoted as macro-mobility and micro-mobility. The movement of medical sensors between various medical network domains distinguishes the macro-mobility. Micro-mobility assumes that medical sensors move between different MSNs within the same domain.

To achieve a continuous monitoring of patients considering the mobility support, it is essential to develop self-configuration or handover mechanisms which are capable of handling secure and efficient data transfers among different MSNs. A data handover mechanism is defined as the process of changing or updating the registration of a mobile sensor from its associated base MSN to the visited MSN, for example, when moving across the hospital's wards. Data handover solutions should enable the ubiquity when they need to work autonomously without human intervention. The handover mechanism should also offer medical sensors continuous connectivity, if there exist several gateways in the hospital or nursing/home environments.

Medical sensors carried by patients are utilized to collect various biological or physiological parameters. Healthcare IoT services are supposed to serve patients in a seamless and continuous way when they are moving in a hospital a nursing facility or at home. More precisely, the mobility support should be provided to the medical sensors ubiquitously from the upper layer (i.e. Fog layer) so that zero reconfiguration is needed in the sensor layer. Fog layer-based handover solutions try to endow healthcare IoT systems with ubiquitous features and provide continuous patient monitoring as well as mobility support.

6.1. Requirements of mobility support for a healthcare IoT system

In this subsection, we present different requirements that need to be fulfilled while offering mobility support for a healthcare IoT system.

(1) In healthcare IoT, mobility must be supported in both star and mesh topologies including single- and multi-hop routing. Mesh networks are mostly formed by nodes with a high degree of mobility.
(2) Signaling must be minimized by removing the use of broadcast/multicast flooding as well as the frequency of link scope broadcast/multicast messages. Reduction of the mentioned mobility signaling messages mitigates the transmission overhead.
(3) Mobility solutions should be compatible and interoperable with the current IPv6 protocols such as Internet Control Message Protocol version 6 (ICMPv6) and Mobile Internet Protocol version 6 (MIPv6).

(4) In the fog layer, a local gateway must notify other available gateways about the presence of mobile sensors in its domain. The reason is that binding necessary updates about the network must be performed by gateways rather than the mobile sensors to unburden tiny sensors from performing heavy tasks.

(5) Global addressing must be supported in mobility solutions. Medical sensors must be addressable anytime needed independent of their current locations. In healthcare IoT, it is one of the main challenges to accomplish global connectivity with the devices using the current Internet infrastructure.

(6) Header information and payloads regarding data messages should be optimized carefully. This reduces fragmentation, the transmission overhead of data messages, and latency while roaming.

(7) Mobility solutions must be based on distributed storage of patients' medical information rather than conventional centralized approaches to support fault tolerance.

(8) The authentication and authorization of medical sensors, smart gateways and caregivers must be performed to ensure the protection of resources, confidentiality, and integrity of the medical information.

(9) Robust security solutions must be provided as healthcare IoT requires ensuring the protection of patients' medical information. Security support can be provided by the AES algorithm which is provided in the data link layer. However, stronger mechanisms to guarantee patients' privacy as well as the security of their medical data can be offered by IPSec in the network layer and DTLS in the transport layer.

(10) In real-time healthcare IoT, mobility detection must be agile so that it avoids delays, jitter, and interruptions of the communication during the data handover process. Data handover procedures (on the evaluation of specific metrics) can be categorized into two main groups: movement parameters and communication parameters. The movement parameters are based on the node position, and movement direction, and velocity. Such parameters are difficult to capture in resource-constrained sensors made to collect just physiological parameters. The second group utilizes the communication parameters in order to handle the requirements for the handover task. The wireless link between two devices can be evaluated using two different metrics: the Received Signal Strength Indicator (RSSI) and the Link Quality Indicator (LQI).

According to [39], the most frequently monitored parameter utilized to evaluate the handover decisions is the Received Signal Strength Indicator (RSSI). The RSSI represents the signal power of a message received by a node which is mostly measured in decibels (dB). The alteration of this value should be directly related to the distance between a sender and a receiver. However, the value of this metric suffers from interference from the surrounding environment and, thereby, this relation is not linear in most situations. The evaluation of RSSI can be performed in two different ways:

(i) Choosing the best value: In this approach, if a patient carrying medical sensors moves to an overlapped coverage area of two or more smart gateways, the one with the higher RSSI value is the one with which the medical sensor chooses to communicate. Due to the oscillation of the RSSI, this model can lead to unnecessary data handovers when a sensor is under several smart gateways' coverage zones. Despite this unpleasant behavior, this model is easy to be deployed and if optimized, it can minimize the data handover costs.

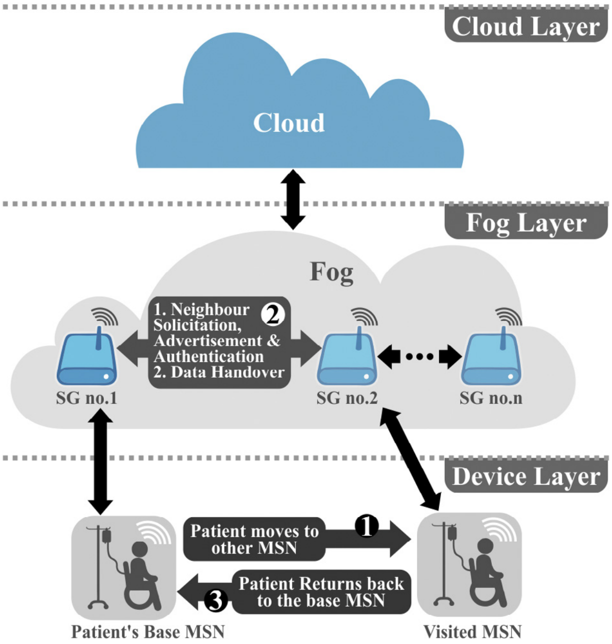

Cloud Layer
Cloud
Fog Layer
Fog
1. Neighbour Solicitation, Advertisement & Authentication
2. Data Handover
2
SG no.1
SG no.2
SG no.n
Device Layer
Patient moves to other MSN
1
Patient Returns back to the base MSN
3
Patient's Base MSN
Visited MSN

Fig. 6. Mobility scenario.

(ii) Making a decision based on comparison against a threshold value: To mitigate the number of unnecessary data handovers performed by the previous approach, this model recommends the use of a threshold value to decide the proper moment to switch to a new gateway. If a sensor moves out from the registered smart gateway's coverage area, the RSSI value will be decreased. If this value undershoots to a predefined threshold value, the sensor needs to be registered to another nearby smart gateway which can receive signals with satisfactory signal strength.

It should be noted that proposing an efficient policy for mobility support in fog-based architectures is beyond the scope of this article. Instead, the key contribution of this work is to present how our proposed session resumption-based end-to-end security scheme can be extended to be efficiently maintained and managed when mobility takes place. In other words, it can be considered as a sub-process of a full mobility procedure to address security aspects after it is decided by a policy making module that roaming should be performed from a smart gateway to another.

6.2. Mobility scenario

Fig. 6 presents the scenario where a patient wearing medical sensors decides to move from its room (base network) to other rooms (visited networks). We assume a mobility scenario which consists of several MSNs for remote patient monitoring in a hospital or nursing/home environment. In the considered scenario, patients may roam through the hospital wards or move to other rooms due to some medical tests (e.g., Laboratory or X-ray).

In the case that a moving sensor loses its connection with one of the smart gateways, he/she will stop being monitored by the caregivers. This condition is not favorable in situations where real-time and continuous monitoring is necessary. To enable seamless transitions of medical sensors, providing an efficient and robust data handover mechanism among smart gateways, considering the limitations of sensors, is of essential importance. The mobility scenario is discussed in three phases in the following subsections.

6.2.1. Message exchange in patients' base MSN

This phase presents the initial state of the medical sensors where each sensor is connected to its base MSN via smart e-health gateway and exchange the required messages. These messages may consist of data frames requests, responses, and acknowledgments of data transmission between the medical sensors and the smart gateways.

The data frames include: (1) information regarding the DTLS session states for the subsequent DTLS session resumption and (2) information about the validity of remote caregivers. Information is exchanged between both peers using the aforementioned AES-CCM algorithm. Request messages are queries to the medical sensor to either get or change some values. Response messages include replies to the request messages where the results of the operation can be obtained. In addition, the request and response messages include information that needs to be transmitted between the sensor and the gateway during the DTLS handshake to perform mutual authentication.

6.2.2. Entering to a new medical subnetwork

Healthcare IoT services are supposed to be offered to patients in a seamless and continuous way when they are moving. When a patient moves out of his/her base MSN, the sensor detects that the quality of its connection with the associated smart gateway is reduced below a pre-defined threshold. We propose to provide mobility support to the sensors from the fog layer to alleviate processing and computation burden of the sensors. To do so, the smart gateway located in the base network needs to check, through the fog layer, whether the medical sensor is accessible from other gateways. This type of mobility (micro-mobility) is just provided to those sensors that are in the same domain/sub-network and their IP addresses do not change. This type of scenario is desirable for MSNs of a hospital as the entire network relies on the same domain.

To provide continuous monitoring of patients, efficient and seamless data handover mechanisms between smart e-health gateways are needed. These mechanisms should take the following features into consideration: (1) Data handover between smart gateways should be quick and seamless considering that the connection to the sensor needs to be preserved during the whole process. (2) After a successful data handover, the changes of routes to the moving medical senor should be spread quickly by the entire healthcare IoT system. (3) The number of messages which need to be exchanged among gateways should be kept minimal (transmission overhead). As a result, to enable mobility for healthcare IoT systems, the following functions need to be performed in the fog layer between smart gateways:

(i) Neighbor Solicitation, Advertisement, and Authentication: Neighbor solicitation and advertisement functions need to be done between the smart gateways in the fog layer to enable seamless mobility. The successful integration of multiple smart gateways on a shared backbone (i.e. fog layer) offers an efficient mobility support. To facilitate the security and the authorization of communication between available smart gateways, it is also required that gateways mutually authenticate one another. As presented earlier, smart gateways are non-resource-constrained devices and they are intelligent in the sense that they have been empowered to autonomously perform local data storage and processing, to learn, and to make decisions at the edge of the network. Hence, the mutual authentication between gateways can be done securely and efficiently using the ECDSA algorithm which was previously presented and analyzed in *SEA* [19].

(ii) Data Handover: Data handover is defined and considered as the process of changing/updating the registration of a sensor from one smart gateway to another one. For example, when moving across hospitals' different rooms. This mechanism enables the mobility support of medical sensors in healthcare IoT domains. In a case that a moving medical sensor loses its connection with one of the smart gateways or if it takes too long to be registered/updated by a new one, the desirable continuous communication and monitoring cannot be ensured. Thus, the smart gateway located in patients' base network needs to periodically send update messages to other gateways in the same domain (e.g., hospital). These messages may include information about the authorized sensors as well as caregivers. Thereby, when a patient enters to another MSN, due to some medical tests, no authentication needs to be done between the sensor and the new gateway. The reason is that the gateway located in the visited network has already been updated, with all necessary information regarding the communication, by the gateway in the base MSN. However, in the case that a new mobile sensor is detected in an MSN, the authentication needs to be performed. As a result, any malicious activity can be discovered and blocked before entering to an MSN.

6.2.3. Returning back to the base MSN

When the patient returns back to his/her base network, the medical sensor sends a re-association request to inform the home smart gateway regarding its new location.

As can be noticed from Fig. 7, mobility is enabled in our proposed end-to-end security scheme using the fog concept. It is shown that by exploiting the fog layer, the mobility support can be provided to the medical sensors ubiquitously without compromising the end-to-end security.

7. Implementation and evaluation

The system architecture illustrated in Fig. 1 is implemented for experimental evaluation, with the main goal of secure and efficient authentication and authorization as well as providing mobility for the proposed end-to-end security scheme. To Implement our proposed architecture, we setup a platform that consists of medical sensors, UT-GATE smart e-health gateways, a remote server, and end-users. UT-GATE is constructed from the combination of a Pandaboard [40] and a Texas Instruments (TI) SmartRF06 board that is integrated with a CC2538 module [41]. The Pandaboard is a low-power and low-cost single-board computer development platform based on the TI OMAP4430 system-on-chip (SoC) following the OMAP architecture and fabricated using 45 nm technology. The OMAP4430 processor is composed of a Cortex-A9 microprocessor unit (MPU) subsystem including dual-core ARM cores with symmetric multiprocessing at up to 1.2 GHz each. In our configuration, UT-GATE uses 8 GB of external memory and is powered by Ubuntu OS which allows to control devices and services such as local storage and notification. To investigate the feasibility of our proposed architecture, the *Wismote* [42] platform, which is a common resource-limited sensor, is utilized in Contiki's network simulation tool Cooja [14]. Wismote is equipped with a 16 MHz MSP430 micro-controller, an IEEE 802.15.4 radio transceiver, 128 kB of ROM, 16 kB of RAM, and supports 20-bit addressing. For the evaluation, we use the open source tool *OpenSSL* version 1.0.1.j to create elliptic curve public and private keys from the NIST P-256 (prime256v1) and X.509 certificates. X.509 certificates are the prevailing form of certificates and are employed in the certificate-based mode of DTLS [43]. The server association to the end-user is created using OpenSSL API

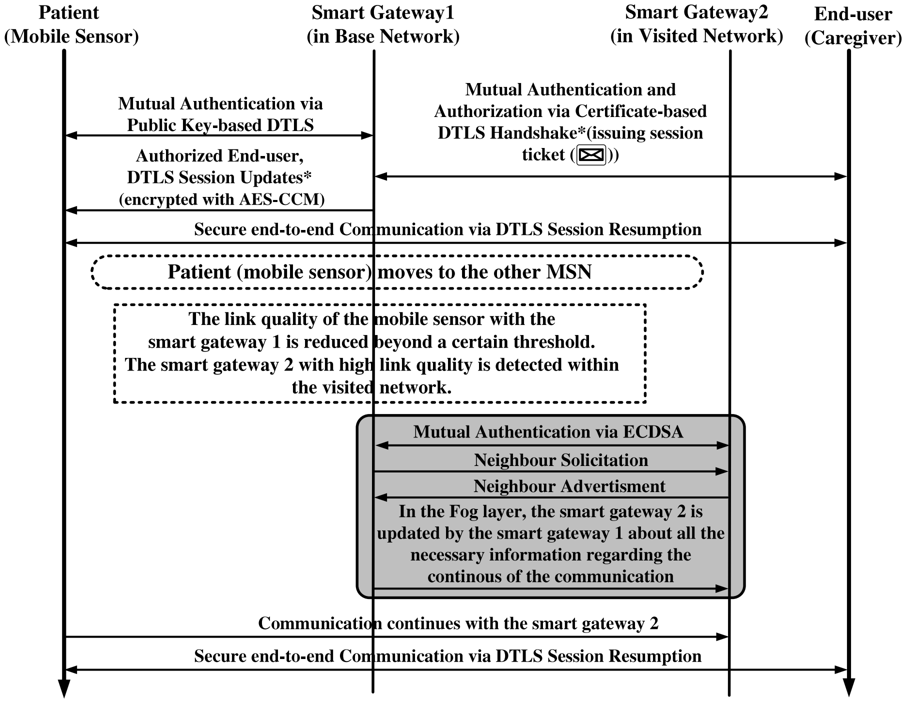

Patient
(Mobile Sensor)
Smart Gateway1
(in Base Network)
Smart Gateway2
(in Visited Network)
End-user
(Caregiver)
Mutual Authentication via
Public Key-based DTLS
Mutual Authentication and
Authorization via Certificate-based
DTLS Handshake*(issuing session
ticket (✉))
Authorized End-user,
DTLS Session Updates*
(encrypted with AES-CCM)
Secure end-to-end Communication via DTLS Session Resumption
Patient (mobile sensor) moves to the other MSN
The link quality of the mobile sensor with the
smart gateway 1 is reduced beyond a certain threshold.
The smart gateway 2 with high link quality is detected within
the visited network.
Mutual Authentication via ECDSA
Neighbour Solicitation
Neighbour Advertisment
In the Fog layer, the smart gateway 2 is
updated by the smart gateway 1 about all the
necessary information regarding the
continous of the communication
Communication continues with the smart gateway 2
Secure end-to-end Communication via DTLS Session Resumption

Fig. 7. The handshaking procedures of the proposed end-to-end security scheme for mobility enabled healthcare IoT.

which provides all necessary functions related to end-users including configuration, certificate, handshake, session state, and cipher suites to support session resumption. *TinyDTLS* [44] is used as the code-base of the proposed scheme, in this work. TinyDTLS is an open-source implementation of DTLS in symmetric key-based mode. We extend it with support for the certificate-based DTLS as well as session resumption. For the public-key functions, we utilize the *Relic-toolkit* [45] that is an open source cryptography library tailored for specific security levels with emphasis on efficiency and flexibility. The MySQL database is set up for static and non-static records. Static records which are managed by system administrators, include white tables, essential data required by the DTLS handshake, and an end-user authentication mechanism. Non-static records store up-to-date bio-signals that are synchronized between the Pandaboard database and a cloud server database. The cloud server database is processed using xSQL Lite which is the third party tool for data synchronization. With respect to the cryptographic primitives and to make a fair comparison, we followed similar cipher suites (which are current security recommendations for constrained network environments [17]) as employed in the most recently proposed authentication and authorization architecture for IP-based IoT [45]. In this regard, we utilize elliptic curve NIST-256 for public-key operations, *AES_128_CCM_8* (with an IV of 8 bytes) for symmetric-key, and SHA256 for hashing operations.

7.1. Energy-performance evaluation

In this subsection, we analyze our proposed end-to-end security scheme from the energy-performance point of view.

Transmission overhead: To perform the certificate-based DTLS handshake, as shown in Fig. 3, all message flights need to be transmitted to establish a DTLS connection. When transmitted over size-constrained IEEE 802.15.4 radio links, these messages must additionally be split into several packet fragments due to their extensive message size [14]. As Table 1 presents, the transmission overhead of the proposed SEA approach to the most recently proposed architecture for a successful certificate-based DTLS connection is compared. As the baseline for this evaluation, a simulation environment is implemented using Cooja. Then, the transmission overheads of the certificate-based DTLS protocol between two wirelessly connected WiSMotes is measured. To quantify the transmission overhead, the *pcap* tool in combination with the Cooja simulator is employed. The presented results signify averages over 100 measurement runs. In a delegation-based architecture, the measured transmission overhead of the certificate-based DTLS handshake is 1609 bytes which causes in total 24 fragments for the transmission of all handshake messages from the delegation server to the end-user [14]. In contrast, the proposed SEA architecture requires transmission of 1190 bytes and it causes 18 fragments totally. As a result, the transmission overhead in our proposed architecture is reduced by 26% compared to the delegation-based architecture.

Latency: Latency is defined as the time needed for a data packet to travel from one designated point to another. It is an essential metric for real-time applications. In this work, we calculate the latency from two perspectives: (i) The communication latency from a smart gateway to an end-user for the authentication and authorization process, and (ii) Data handover latency between two smart gateways for the proposed mobility enabled end-to-end security scheme. The communication latency and the data handover latency are estimated on a 20 Mb/s broadband Internet connection (see Table 2).

(i) *Communication latency*: To estimate the communication latency, the processing time which is spent from sensor node to the end-user (NE) is calculated. This processing time deduced from the summation of communication latency from sensor node to smart gateway (NG) and smart gateway to end-user can be written as: $Latency_{NE} = Latency_{NG} + Latency_{GE}$. In this work, to compute the communication latency from the UT-Gate to the end-user, a proxy server is adjoined to the network. Through the proxy server, the transmission latency between the end-user and the UT-Gate can be easily measured as the proxy server listens to requests transmitted from the end-user to the UT-Gate and vice versa without tampering or modifying them. To compute the communication latency of GE, the

Table 1
Performance comparison with the most recently proposed authentication and authorization approach for IoT.

	Transmission-overhead (byte)	Latency-GE (s)	Latency-NG (s)
SEA approach (this work)	1190	5.001	∼15
Hummen et al. [14]	1609	6.08	∼15
SEA approach improvements (%)	26	16	0

Table 2
Data handover latency between two smart gateways with different packet size.

Packet size (byte)	Data handover latency (ms)
10	2.288
30	2.410
50	2.517
100	2.884
200	3.113
500	3.342
1k	3.685
5k	4.588

Fiddle [4] proxy server, which is a desktop application, is employed to track requests and responses. Fiddle offers a large number of services including security testing and HTTP/HTTPS traffic recoding. According to our analysis, the proposed SEA architecture achieves an almost equivalent *NG* processing time to the delegation-based architecture [14]. However, the proposed SEA approach considerably reduces the processing time required for *GE* compared to the delegation-based architecture. As shown in Table 1, in SEA, the processing time required for *GE* is about 5.001 s whereas this time increases to about 6.08 s in the delegation-based architecture. Thus, regarding the latency from the gateway to the end-user, the proposed architecture obtains about 16% improvement compared to the delegation-based architecture.

(ii) *Data handover latency*: To demonstrate how our proposed end-to-end security scheme enables mobility, we implemented a real system in which two UT-GATE gateways with the configuration described above are employed. We assume that these gateways are connected through the fog layer where one of the gateways acts as a client and the other one acts as a server. In the experiments, we created a 100-byte lookup table for each gateway that consists of: (i) control data which consists of the DTLS session resumption state, information about the authorized caregivers, medical sensors' IDs, and patients' IDs. (ii) Patients' health data that includes heart rate, body temperature, and oxygen saturation. In our analysis, we calculated the latency of the data handover process between the gateways. To show the scalability of our method, we considered messages with different sizes which may need to be exchanged between the gateways for the data handover process. The results are shown in Table 6. As can be deduced from the Table, the data handover latency between two gateways is negligible and mobility is supported in an agile way without any computational and processing burden to the sensors. In addition, by increasing the packet size, latency marginally increases showing the scalability of our scheme. As mentioned before, seamless mobility is a necessity in healthcare IoT systems. The experiments show that our proposed end-to-end security scheme also provides support for this feature. It should be noted that proposing a novel mobility approach is orthogonal to the proposed idea. It means that any fog-based mobility solution can be combined with our security scheme.

Sensor-side processing time: For the evaluation, in Cooja, we configured two Wismotes as a client and a server. Once the booting process is performed, the client initiates the handshake by sending the *ClientHello* message. After a successful handshake, we measured the total processing time at the sensor-side (server). The results of our measurements using three different approaches are shown in Table 4. As can be seen from the Table, the symmetric key-based mode and our session resumption-based scheme require almost similar processing time. The proposed scheme requires 20 ms less processing time than the symmetric key-based mode. This is due to the fewer message flights needed to be exchanged in the session resumption (compared to the full symmetric key-based DTLS), resulting in less computations at the sensor-side. The processing time for the certificate-based DTLS handshake is considerably higher than both the symmetric key-based and the session resumption-based modes. The certificate-based DTLS requires about 5690 ms at the sensor-side which is mainly due to the expensive public key-based operations (i.e. ECDSA and ECDH).

Client-side processing time: The total processing time at the client (end-user) side using three different approaches is shown in Table 4. For the client-side, we used a machine with *IntelCore*$^{\text{TM}}$*i*5 — 4570 CPU operating at 2.2 GHz and having 6 GB of RAM. The processing time of the proposed scheme using DTLS session resumption is 45 ms, where as the conventional symmetric key-based requires 49 ms. This is due to the lesser number of control messages needed for session resumption, compared to the full symmetric key-based DTLS. The processing time for certificate-based DTLS handshake, is considerably higher than both the symmetric key-based and the session resumption-based modes. The certificate-based DTLS requires approximately 3744 ms at the client-side which is mainly due to the expensive public key-based operations. Compared to symmetric key-based and certificate-based DTLS, our session resumption-based scheme has 8.1% and 98.7% improvements in terms of client-side processing time, respectively.

Run-time performance: In this work, run-time refers to the time it takes for the handshake between the medical sensor and the end-user to be done successfully. To provide end-to-end security, we calculate the total run-time performance of three different DTLS modes. The results are presented in Table 3. As can be seenfrom the Table, our scheme which utilizes the DTLS session resumption technique is about 97% and 10% faster than certificate-based and symmetric key-base DTLS handshake, respectively.

Energy consumption: To measure the consumed energy of each sensor, we utilize the equation: E (mJ) $= U(V) \times I$ (mA) $\times$ t (ms) where U represents the supply voltage, I is the current draw of the hardware, and t is the time. We calculate the energy consumption of the Wismote sensor when performing the DTLS session resumption, the symmetric key-based DTLS handshake, and the certificate-based DTLS handshake. According to the datasheet available in [42], the Wismote has a current consumption of 18.5 mA and a supply voltage of 3 V. The results are presented in Table 4. As can be seen from the Table, our techniques are considerably more energy efficient in comparison to the certificate-based DTLS handshake technique. It saves 11% of energy compared to the symmetric key-based DTLS.

Table 3
Client-side processing time and total run-time performance of different DTLS modes to provide end-to-end security.

	Client-side processing time (ms)	Run-time performance (ms)
DTLS session resumption without server-side state (*DTLS_Session_Resumption_WITH_AES*_128) (this work)	45	205
Certificate-based DTLS (*DTLS_ECDHE_ECDSA_WITH_AES*_128_*CCM*_8_*SHA*_256)	3744	9434
Symmetric key-based DTLS (*DTLS_PSK_WITH_AES*_128_*CCM*_8)	49	229

Table 4
Sensor-side processing time and energy consumption of different DTLS modes to provide end-to-end security.

	Sensor-side processing time (ms)	Energy consumption (mJ)
DTLS session resumption without server-side state (*DTLS_Session_Resumption_WITH_AES*_128) (this work)	160	8.87
Certificate-based DTLS (*DTLS_ECDHE_ECDSA_WITH_AES*_128_*CCM*_*SHA*_256)	5690	315.79
Symmetric key-based DTLS (*DTLS_PSK_WITH_AES*_128_*CCM*_8)	180	9.99

Table 5
Memory footprint of different DTLS modes to provide end-to-end security.

	RAM overhead (kB)	ROM overhead (kB)
DTLS session resumption without server-side state (*DTLS_Session_Resumption_WITH_AES*_128) (this work)	3.51	14.29
Certificate-based DTLS (*DTLS_ECDHE_ECDSA_WITH_AES*_128_*CCM*_8_*SHA*_256)	7.8	41.1
Symmetric Key-Based DTLS (*DTLS_PSK_WITH_AES*_128_*CCM*_8)	2.96	13.49

Memory requirement: To calculate total RAM and ROM requirements of the utilized session resumption technique, we used the msp430-size tool which is provided by the MSP430-gcc compiler. We evaluated RAM and ROM requirements using three different modes of DTLS handshake: (i) DTLS session resumption used in our proposed scheme, (ii) symmetric key-based DTLS handshake, and (iii) certificate-based DTLS handshake. As shown in Table 5, the certificate-based DTLS consumes about 2.6 times more RAM and 3 times more ROM resources than what is required by the symmetric key-based DTLS handshake. These overheads are considerable for devices having limited resources particularly in terms of memory. In [19], we presented that our proposed IoT-enabled healthcare architecture enables the constrained medical sensor to unburden all certificate-related and public-key operations to the distributed smart e-health gateway. Thus, the memory burden of the medical sensors is considerably alleviated. Compared to the symmetric key-based mode, our proposed session resumption-based scheme adds a negligible memory overhead (RAM and ROM overheads are only increased by 0.5 kB and 0.8 kB, respectively). This minor increase is due to the session resumption extension and the storage of the session tickets.

7.2. Security evaluation

In this section, we analyze our proposed end-to-end security scheme from the security perspective. We conclude this section by comparing our work with the most recently proposed schemes found in the literature.

Data confidentiality: In this work, to provide confidentiality, 128-bit AES-CCM with a 16 byte initialization vector is employed to protect patients' information that needs to be transmitted between communicating peers. In the proposed scheme, even if an adversary eavesdrops on some or all of the transmitted patients' health data, he/she cannot access those data easily as they are encrypted using the secure and robust 128-bit AES encryption algorithm. A brute force attack on 128-bit AES would require $3.4 * 10^{38}$ years [36].

Data integrity: In this work, to ensure that the transmitted data is received in the exact same way as it is sent, a 8 byte Message Authentication Code (MAC) based on HMAC-SHA-256 is employed. This is done by creating the MAC of a message m (that needs to be transmitted) using the SHA-256 hash function and a shared secret key K (*SessionKey*) over m which can be written as: $HMAC(m) = SHA256(K, m) = HMAC(K, m) = D$. The MAC is a cryptographic checksum on message m that uses the *SessionKey* to detect both accidental and intentional modifications of the message. Based on the above equation, the secure HMAC generates a fixed length hash digest D from the message m. It has the characteristics of being simple to compute, while infeasible to retrieve the m from the given hash digest D. The small changes in m result in a different hash value. Such features are specified as preimage and collision resistant, respectively. Thus, our proposed scheme ensures the property of data integrity.

Mutual authentication and authorization: In SEA [19], we presented that sensors used in medical applications are highly resource-constrained for which reason they cannot cope with cryptography techniques demanding heavy computations. To overcome this limitation, we proposed to employ non-resource-constrained smart e-health gateways in distributed fashion to perform the authentication and authorization of end-users mutually on behalf of the sensors. The proposed architecture relied on the certificate-based DTLS handshake and the employed cipher suite was *TLS_ECDHE_ECDSA_WITH_AES*_128_*CCM*_8_*SHA*_256. The name indicates the use of elliptic cryptography, particularly-*Elliptic Curve Diffie-Hellman* (*ECDH*) and *Elliptic Curve Digital Signature Algorithm* (*ECDSA*). We proved that, within the certificate-based DTLS handshake, from one hand, the smart e-health gateway authenticates the remote end-user through certificates. On the other hand, the smart gateway either authenticates to the remote end-point through certificates within the DTLS handshake mechanism or based on an application-level password once the handshake is terminated. Therefore, mutual authentication and authorization of peers is fulfilled in our work.

Forward security: As mentioned earlier, the property of forward security ensures that the revelation of current encrypted patients' health data should not threaten the security of previously transmitted data. In this work, using the certificate-based DTLS handshake, the shared *SessionKey* between peers is derived using ECDH. For this, as Fig. 3 presents, each of the peers, the smart gateway and the end-user, produce their own pair of private and public keys on an already agreed elliptic curve. (a, b) for the smart gateway and (c, d) for the end-user. Then, the peers exchange their public keys and the DTLS session key over the elliptic curve is calculated as: $a \times b = SessionKey = c \times d$ where × is the scalar multiplication on elliptic curve. Elliptic Curve Cryptography (ECC) relies on the general hypothesis that the elliptic curve discrete logarithm problem is infeasible or at least it cannot be solved in a reasonable time. Once the *SessionKey* is derived using ECDH, the x-coordinate value of *SessionKey* serves as a shared secret between the end-user and the smart gateway. The derived shared secret is utilized further to protect the communication/data transmitted between the peers. As shown in Fig. 3, since b and d are public values of the peers, their exchange through an unencrypted channel does not compromise or provide any information concerning the *SessionKey*. This is because obtaining the *SessionKey* implies the computation of elliptic curve discrete logarithm problem (ECDLP). Solving this problem is not easily possible. The reason is that ECDLP is believed to be much harder to solve than its counterpart over finite fields (DLP) or the integer factorization problem (FP), the two main alternatives for public key cryptography.

Scalability and reliability: In SEA [19], we proposed a new architecture for IoT-enabled healthcare system (i.e. in-home/hospital environments) which relies on distributed smart e-health gateways. In our proposed architecture, we also discussed that in a multi-domain smart home/hospital environment, if an attacker runs a DoS attack or compromises one of the smart gateways, only the associated medical sub-domain is disrupted. However, in most of the recently proposed delegation-based architectures, if an attacker performs a Denial of Service (DoS) attack or compromises the delegation server, a large quantity of stored patients' health data can be retrieved. Specifically, in multi-domain networks, a DoS attack can disrupt all the available constrained medical domains as the functionality of those IoT-based domains depends on the centralized delegation server. Hence, compared to most recently proposed delegation-based architectures [14,38,46], our proposed IoT-enabled healthcare architecture is more scalable and reliable as the architecture is changed from being centralized to distributed.

Lightweight solutions: In the previous section, we noted that conventional security and protection mechanisms including existing cryptographic solutions, secure protocols, and privacy assurance cannot be re-used due to resource constraints, security level requirements, and system architecture of IoT-based healthcare systems. To alleviate the constrained medical sensors from all heavy processing burdens: (i) we exploit the non-resource-constrained distributed smart gateways to perform the authentication and authorization of remote end-users securely and efficiently on behalf of medical sensors. (ii) to provide secure end-to-end communication between the end-user and the tiny medical sensor, we used the lightweight DTLS session resumption technique. This is because session resumption has an abbreviated form of a full DTLS handshake that relies on the previously established security context, which neither requires heavy-weight certificate-related nor public-key cryptography operations.

Access control: In our scheme, as we discussed earlier in the mutual authentication and authorization section, the validation and authorization of data and end-user access control are handled by smart e-health gateways instead of the resource-constrained medical sensors. Thus, any malicious activity is blocked at the smart gateway before an unauthorized users get access to the medical network domain(s).

Smart gateway and sensor spoofing: In the proposed architecture, if an adversary pretends to be a trusted smart e-health gateway/medical sensor, from one hand, he/she can get access to all information related to the DTLS sessions. On the other hand, patients' encrypted health data can also be revealed to the attacker. In this work, as Figs. 3 *and* 5 present, the smart e-health gateway and the end-user as well as the medical sensor and the smart e-health gateway share a symmetric *SessionKey* between each other. As it was presented earlier in the forward security section, this shared *SessionKey* is generated using ECDH and solving this algorithm is not easily possible [23]. Thus, by spoofing the smart gateway/sensor, an attacker cannot deceive the end-user for access to data concerning the DTLS session.

Denial of service attack (DoS): In SEA [19], we discussed in more detail about the drawbacks of the state-of-the-art architectures proposed for IoT-based systems. To give an example, in the most recently proposed delegation-based architecture developed by Hummen et al. [47], if an adversary performs a DoS attack or compromises the centralized delegation server, a large number of stored security context related to constrained domains can be retrieved. Specifically, in multi-domain networks, a DoS attack can disrupt all the available medical domains as the functionality of the IoT-based healthcare systems still relies on the centralized delegation server. However, in our proposed IoT-enabled healthcare system, in a multi-domain smart home/hospital network, if an attacker runs a DoS attack or compromises one of the smart e-health gateways, just the associated medical sub-domain can be disrupted. The reason is that in our proposed architecture, the authentication and authorization tasks of a centralized delegation server is broken down to be performed by distributed smart e-health gateways.

Stolen DTLS session tickets: In a DTLS handshake, an eavesdropper may attempt to obtain the ticket and to utilize it to establish a session with the server. However, a stolen ticket does not help the adversary to resume the session as the session ticket is encrypted and the adversary does not have any knowledge about the secret key. To minimize the feasibility of success of this attack, in this work (as proposed by IETF [17]), the lightweight 128-bit AES in CCM mode and the HMAC-SHA-256 algorithms are used by the DTLS server to provide confidentiality and integrity, respectively. This prevents an adversary from successfully executing a brute force attack to obtain the tickets' contents.

Forged DTLS session tickets: A malicious adversary can alter or forge the session ticket in order to resume a DTLS session, to impersonate as a valid user, to extend the lifetime of a session, or to obtain additional privileges. To avoid the forged ticket attack, we used the strong integrity protection algorithm HMAC-SHA-256 to protect the session ticket. In the data integrity section, we

Table 6
Security comparison of different schemes providing end-to-end security ("✓" indicates that the scheme supports the mentioned security feature, and "✗" indicates that the scheme does not support the feature).

Security features	Hummen et al. [14]	Granjal et al. [38]	Kang et al. [46]	This work
Data confidentiality	✓	✓	✓	✓
Data integrity	✓	✓	✓	✓
Mutual authentication and authorization	✓	✓	✓	✓
Forward security	✓	✓	✗	✓
Architecture scalability	✗	✗	✗	✓
Lightweight solutions	✓	✓	✓	✓
Access control	✗	✗	✓	✓
Smart gateway and sensor spoofing	✗	✗	✓	✓
Denial of Service (DoS) attack	✗	✗	✓	✓
End-to-end security	✓	✗	✗	✓

described in detail more how the integrity requirements can be fulfilled using HMAC-SHA-256.

End-to-end security: In our proposed scheme, during the initialization phase, the smart e-health gateways' main tasks are transmitting the information related to the DTLS sessions as well as the necessary security contexts to the medical sensors. However, the only performers of both the encryption and decryption of patients' health data (in DTLS session resumption) are the end-user and the medical sensor. Thus, both end points directly communicate with each other without the necessity of a smart gateway as an intermediary node. Thus, end-to-end security is ensured in our scheme.

The security comparisons of our proposed end-to-end security scheme and the most recently proposed approaches are presented in Table 6. The state-of-the-art end-to-end security approaches proposed for IoT are presented by Hummen et al. [14], Granjal et al. [38], and Kang et al. [46]. However, we distinguish the following major advantages offered by our scheme compared to their approaches. We believe that the approaches presented by Granjal et al. [38] and Kang et al. [46] do not provide comprehensive end-to-end security. Rather, they can be considered *semi end-to-end* security. The main reason is that in these works, the 6LoWPAN Border Router (6LBR) acts as an intermediary node located between the sensor and the end-user. Every time these two end-points try to communicate with each other, all the secret information related to the communication needs to pass through the 6LBR. Whilst, the smart gateway utilized in our work is only used during the initialization phase (Fig. 5), and then afterwards, both end-points directly communicate with each other through a channel secured by the DTLS session resumption. Therefore, *end-to-end* security is guaranteed in our work.

The approaches presented by Granjal et al. [38] and Kang et al. [46] also lack scalability and reliability as their proposed system architectures rely on the centralized 6LBR. The main reason is that their proposed architectures cannot be extended to be utilized in multi-domain infrastructures, such as large hospital environments. For example, if a malicious adversary performs a DoS attack or compromises the 6LBR, a large quantity of stored information concerning the constrained domain can be retrieved. More precisely, in multi-domain networks, a DoS attack can disrupt all the available medical networks as the functionality of the IoT-based healthcare system still depends on the centralized 6LBR. However, these issues are solved in our proposed scheme as the architecture is distributed. To be more specific, in our scheme, in a multi-domain smart home/hospital environment, if an attacker runs a DoS attack or compromises one of the smart gateways, only the associated medical sub-domain is disrupted. Although Hummen et al.'s [14] proposed delegation-based architecture offers end-to-end security, it is still not secure against the DoS attack due to the use of a centralized delegation server. Their presented architecture also suffers from shortcomings in scalability and reliability which is mainly due to the reasons mentioned above.

Based on the discussion above, our proposed scheme fulfills the aforementioned requirements of secure and efficient communication for healthcare IoT systems and can efficiently provide end-to-end security.

8. Conclusions

We presented an end-to-end security scheme for mobility enabled healthcare IoT systems. Based on literature, we determined that our scheme has the most extensive set of security features in comparison to related approaches. Our three-tier system architecture consists of the device layer, the fog layer, and the cloud layer. We leveraged the strategic position and the distributed nature of smart gateways in the fog layer to provide seamless mobility for medical sensors and to alleviate the sensors' processing loads. In our scheme, ubiquitous mobility is possible without requiring any reconfiguration at the device layer. The end-to-end security scheme was specified and designed by employing the certificate-based DTLS handshake between end-users and smart gateways as well as utilizing the session resumption technique. Our testbed platform demonstration showed that, compared to existing end-to-end security approaches, our scheme reduces the communication overhead by 26% and the communication latency between smart gateways and end users by 16%. Our scheme performed approximately 97% faster than certificate-based and 10% faster than symmetric key-based DTLS. In terms of memory requirements, certificate-based DTLS consumes about 2.2 times more RAM and 2.9 times more ROM resources than our approach. In fact, the RAM and ROM requirements of our scheme are almost as low as in symmetric key-based DTLS. Taking into account that the handover latency caused by mobility is low and the handover process does not incur any processing or communication overhead on the sensors, we summarize that our scheme is a very promising solution for ensuring end-to-end security and secure ubiquitous sensor-level mobility for healthcare IoT.

Acknowledgments

The authors wish to acknowledge the financial support by the Finnish Cultural Foundation, HPY Foundation, Nokia Foundation, Ulla Tuominen Foundation, and University of Turku Graduate School (UTUGS) during the course of this project.

References

[1] European Commission Information Society. Internet of Things Strategic Research Roadmap, 2009.

[2] L. Da Xu, W. He, S. Li, Internet of things in industries: A survey, IEEE Trans. Ind. Inf. 10 (4) (2014) 2233–2243.

[3] S. Li, L. Da Xu, S. Zhao, The Internet of things: A survey, Inf. Syst. Front. 17 (2) (2015) 243–259.

[4] A.-M. Rahmani, N.K. Thanigaivelan, Tuan Nguyen Gia, J. Granados, B. Negash, P. Liljeberg, H. Tenhunen, Smart e-health gateway: Bringing intelligence to IoT-based ubiquitous healthcare systems, in: 12th Annual IEEE Consumer Communications and Networking Conference, 2015, pp. 826–834.

[5] C.E. Koop, R. Mosher, L. Kun, J. Geiling, E. Grigg, S. Long, C. Macedonia, R. Merrell, R. Satava, J. Rosen, Future delivery of health care: Cybercare, IEEE Eng. Med. Biol. Mag. 27 (6) (2008) 29–38.

[6] R. Mueller, Demo: A generic platform for sensor network applications, in: IEEE International Conference on Mobile Adhoc and Sensor Systems, 2007, pp. 1–3.

[7] W. Shen, Y. Xu, D. Xie, T. Zhang, A. Johansson, Smart border routers for ehealthcare wireless sensor networks, in: 7th International Conference on Wireless Communications, Networking and Mobile Computing, 2011, pp. 1–4.

[8] Intel® IoT Gateway, 2014. http://www.intel.com/content/products [accessed 22.01.2014].

[9] S. Kumar, C. Paar, Are standards compliant elliptic curve cryptosystems feasible on RFID? in: Workshop on RFID Security, 2006.

[10] B. Xu, L. Da Xu, H. Cai, C. Xie, J. Hu, F. Bu, Ubiquitous data accessing method in IoT-based information system for emergency medical services, IEEE Trans. Ind. Inf. 10 (2) (2014) 1578–1586.

[11] G. Yang, L. Xie, M. Mantysalo, X. Zhou, Z. Pang, L. Da Xu, S. Kao-Walter, Q. Chen, L. Zheng, A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box, IEEE Trans. Ind. Inf. 10 (4) (2014) 2180–2191.

[12] H. Yan, L. Da Xu, Z. Bi, Z. Pang, J. Zhang, Y. Chen, An emerging technology—Wearable wireless sensor networks with applications in human health condition monitoring, J. Manage. Anal. 2 (2) (2015) 121–137.

[13] K. Malasri, L. Wang, Addressing security in medical sensor networks, in: Proceedings of the 1st International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments, 2007, pp. 7–12.

[14] R. Hummen, H. Shafagh, S. Raza, T. Voig, K. Wehrle, Delegation-based authentication and authorization for IP-based Internet of things, in: 11th IEEE International Conference on Sensing, Communication, and Networking, 2014, pp. 284–292.

[15] X. Hung, M. Khalid, R. Sankar, S. Lee, An efficient mutual authentication and access control scheme for WSN in healthcare, J. Netw. 6 (3) (2011) 355–364.

[16] R. Chakravorty, MobiCare: A programmable service architecture for mobile medical care, in: Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, 2006.

[17] C. Bormann, Z. Shelby, K. Hartke, Constrained Application Protocol (CoAP), draft-ietf-core-coap-18, IETF. 2013.

[18] N. Modadugu, E. Rescorla, Datagram Transport Layer Security (DTLS) Version 1.2, in: RFC 5238, 2012.

[19] S. Rahimi Moosavi, T. Nguyen Gia, A.M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, H. Tenhunen, SEA: A secure and efficient authentication and authorization approach for IoT-based healthcare systems using smart gateways, in: The 6th International Conference on Ambient Systems, Networks and Technologies, 2015, pp. 452–459.

[20] S. Rahimi Moosavi, T. Nguyen Gia, E. Nigussie, A.M. Rahmani, S. Virtanen, H. Tenhunen, J. Isoaho, Session resumption-based end-to-end security for healthcare Internet-of-things, in: IEEE International Conference on Computer and Information Technology, 2015.

[21] D. Malan, T. Fulford-Jones, M. Welsh, S. Moulton, CodeBlue: An Ad hoc sensor network infrastructure for emergency medical care, in: Wearable and Implantable Body Sensor Networks, 2004, pp. 12–14.

[22] K. Lorincz, D. Malan, T. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, S. Moulton, Sensor networks for emergency response: Challenges and opportunities, IEEE Pervasive Comput. 3 (4) (2004) 16–23.

[23] N. Koblitz, Elliptic curve cryptosystems, Math. Comp. 48 (1987) 203–209.

[24] C. Karlof, N. Sastry, D. Wagner, TinySec: A link layer security architecture for wireless sensor networks, in: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, 2004, pp. 162–175.

[25] G. Kambourakis, E. Klaoudatou, S. Gritzalis, Securing medical sensor environments: The codeblue framework case, in: The Second International Conference on Availability, Reliability and Security, 2007, pp. 637–643.

[26] J. Ko, J. Lim, Y. Chen, R. Musvaloiu, A. Terzis, G. Masson, T. Gao, W. Destler, L. Selavo, R. Dutton, MEDiSN: Medical emergency detection in sensor networks, ACM Trans. Embedded Comput. Syst. 10 (2010) 11:1–11:29.

[27] C. Tan, H. Wang, S. Zhong, Q. Li, IBE-Lite: A lightweight identity-based cryptography for body sensor networks, IEEE Trans. Inf. Technol. Biomed. 13 (6) (2009) 926–932.

[28] S. valenzuela, M. Chen, V. Leung, Mobility support for health monitoring at home using wearable sensors, IEEE Trans. Inf. Technol. Biomed. 15 (4) (2011) 539–549.

[29] A. Jara, M. Zamora, A. Skarmeta, An initial approach to support mobility in hospital wireless sensor networks based on 6LoWPAN (HWSN6), J. Wirel. Mob. Netw., Ubiquitous Comput., Dependable Appl. 1 (2–3) (2010) 107–122.

[30] A. Jara, M. Zamora, A. Skarmeta, HWSN6: Hospital wireless sensor networks based on 6LoWPAN technology: Mobility and fault tolerance management, in: International Conference on Computational Science and Engineering, Vol. 2, August 2009, pp. 879–884.

[31] A. Jara, M. Zamora, A. Skarmeta, Intra-mobility for hospital wireless sensor networks based on 6LoWPAN, in: 6th International Conference on Wireless and Mobile Communications, September 2010, pp. 389–394.

[32] H. Fotouhi, M. Alves, M. Zuniga Zamalloa, A. Koubaa, Reliable and fast hand-offs in low-power wireless networks, IEEE Trans. Mob. Comput. 13 (11) (2014) 2620–2633.

[33] S. Li, L. Da Xu, X. Wang, Compressed sensing signal and data acquisition in wireless sensor networks and Internet of things, IEEE Trans. Ind. Inf. 9 (4) (2013) 2177–2186.

[34] S. Li, L. Da Xu, X. Wang, A continuous biomedical signal acquisition system based on compressed sensing in body sensor networks, IEEE Trans. Ind. Inf. 9 (3) (2013) 1764–1771.

[35] F. Bonomi, R. Milito, J. Zhu, S. Addepalli, Fog computing and its role in the Internet of things, in: Proceedings of the Workshop on Mobile Cloud Computing, 2012, pp. 13–16.

[36] J. Daemen, V. Rijmen, Specification of Rijndael, 2002, pp. 31–50.

[37] R. Hummen, J. Gilder, Extended DTLS session resumption for constrained network environments. Technical Report, 2013.

[38] J. Granjal, E. Monteiro, J. Sa Silva, End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication, in: International Conference on Networking, 2013, pp. 1–9.

[39] J. Caldeira, J. Rodrigues, P. Lorenz, Intra-mobility support solutions for healthcare wireless sensor networks, handover issues, IEEE Sens. 13 (11) (2013) 4339–4348.

[40] PandaBoard Platform Information. http://pandaboard.org/ [accessed 27.09.2015].

[41] SmartRF06 Evaluation Board. http://www.ti.com/lit/ug/swru321a [accessed 27.09.2015].

[42] Arago Systems. Wismote. http://www.aragosystems.com/en/document-center [accessed 27.09.2015].

[43] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, Internet X.509 Public Key Infrastructure Certificate Profile. http://tools.ietf.org/html/rfc5280 [accessed 27.09.2015].

[44] O. Bergmann, TinyDTLS. http://sourceforge.net/p/tinydtls [accessed 27.09.2015].

[45] D. Aranha, C. Gouv, RELIC is an Efficient Library for Cryptography. http://code.google.com/p/relic-toolkit/ [accessed 27.09.2015].

[46] N. Kang, J. Park, H. Kwon, S. Jung, ESSE: Efficient secure session establishment for Internet-integrated wireless sensor networks, Int. J. Distrib. Sens. Netw. (2015) 1–12.

[47] R. Hummen, J. Ziegeldorf, H. Shafagh, S. Raza, K. Wehrle, Towards viable certificate-based authentication for the Internet of things, in: Proceedings of the 2nd Workshop on Hot Topics on Wireless Network Security and Privacy, 2013, pp. 37–42.

Sanaz Rahimi Moosavi received her B.Sc. (Tech.) degree in Computer Software Engineering from the Department of Electrical and Computer Engineering, University of Imam Reza, Mashhad, Iran in 2006, and M.Sc. (Tech.) degree in Information Technology, Networked Systems Security from the Department of Information Technology and Communication Systems, University of Turku, Finland in 2013. She is currently working towards her Ph.D. degree at University of Turku, Finland. Her research interests include security and privacy, Internet of Things (IoT), smart healthcare systems, and lightweight cryptography techniques. She is a student member of IEEE.

Tuan Nguyen Gia received his B.Sc. (Tech.) degree in Information technology from Department of Information Technology, Helsinki Metropolia University of Applied Sciences, Helsinki, Finland in 2012, and M.Sc. (Tech) degree in Information Technology, Embedded Computing from the Department of Information Technology and Communication Systems, University of Turku, Finland in 2014. He is currently working towards his Ph.D. degree at the University of Turku, Finland. His research interests include Internet of Things (IoT), Smart Healthcare, and Medical Cyber–Physical System, FPGA and Wireless Body Sensor Networks.

Ethiopia Nigussie is a University Lecturer at the University of Turku, Finland. She obtained her Ph.D. degree in Communication Systems from University of Turku in 2010 and M.Sc. degree in Electrical Engineering from Royal Institute of Technology (KTH), Sweden in 2004. Her current research interests are energy saving strategies, adaptive design approaches and security for low-power wireless networks, self-aware design, and cognitive radio networks. Dr. Nigussie is the author of "Variation Tolerant On-Chip Interconnects" book (Springer) and she has about 50 international peer-reviewed journal and conference articles. She is senior member of IEEE since March 2015.

Amir M. Rahmani received his Master's degree from Department of Electrical and Computer Engineering, University of Tehran, Iran, in 2009 and Ph.D. degree from Department of Information Technology, University of Turku, Finland, in 2012. He also received his M.B.A. jointly from Turku School of Economics and European Institute of Innovation & Technology (EIT) ICT Labs, in 2014. He is currently a University Teacher (Faculty Member) at the University of Turku, Finland, and visiting researcher at KTH Royal Institute of Technology, Sweden. He is the author of more than 100 peer-reviewed publications, is supervising eight Ph.D. students. He is currently co-leading three Academy of Finland projects entitled "MANAGE", "SPA", and "InterSys".

Seppo Virtanen received his M.Sc. in electronics and information technology in 1998 and D.Sc. (Tech.) in Communication Systems in 2004 from the University of Turku, Finland. Since 2009, he has been an adjunct professor of Embedded Communication Systems at University of Turku where he also heads the Master's Programme in Information Security and Cryptography. He is a senior member of the IEEE. Currently the focus in his research is on information security issues in the communication and network technology domain, specifically focusing on design and methodological aspects of reliable and secure communication systems and networks.

Hannu Tenhunen received the diplomas from the Helsinki University of Technology, Finland, 1982, and the Ph.D. degree from Cornell University, Ithaca, NY, 1986. In 1985, he joined the Signal Processing Laboratory, Tampere University of Technology, Finland, as an associate professor and later served as a professor and department director. Since 1992, he has been a professor at the Royal Institute of Technology (KTH), Sweden, where he also served as a dean. He has more than 600 reviewed publications and 16 patents internationality. He is a member of the IEEE.

Jouni Isoaho received his M.Sc. (Tech.) in Electrical Engineering, and his Lic. Tech. and Dr. Tech. in signal processing from Tampere University of Technology, Finland in 1989, 1992 and 1995, respectively. Since 1999 he has been the professor of communication systems at University of Turku, Finland, where he heads the communication systems laboratory. His research interests include future communication system concepts, applications and implementation techniques. His current special interests are in dynamically reconfigurable self-aware systems for future communication and interdisciplinary applications including information security and dependability aspects.

Publication V

Performance Analysis of End-to-End Security Schemes in Healthcare IoT

Sanaz Rahimi Moosavi, Ethiopia Nigussie, Marco Levorato, Seppo Virtanen, Jouni Isoaho

Original published in Elsevier International Conference on Ambient Systems, Networks and Technologies (ANT-2018), pages 327-334, 2018, Portugal.

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 130 (2018) 432–439

Procedia Computer Science

www.elsevier.com/locate/procedia

9th International Conference on Ambient Systems, Networks and Technologies, ANT-2018 and the 8th International Conference on Sustainable Energy Information Technology, SEIT 2018, 8-11 May, 2018, Porto, Portugal

Performance Analysis of End-to-End Security Schemes in Healthcare IoT

Sanaz Rahimi Moosavi*, Ethiopia Nigussie, Marco Levorato, Seppo Virtanen, Jouni Isoaho

Department of Future Technologies, University of Turku, 20014 Turku, Finland

Abstract

In this paper, we analyze the performance of the state-of-the-art end-to-end security schemes in healthcare Internet of Things (IoT) systems. We identify that the essential requirements of robust security solutions for healthcare IoT systems comprise of (i) low-latency secure key generation approach using patients' Electrocardiogram (ECG) signals, (ii) secure and efficient authentication and authorization for healthcare IoT devices based on the certificate-based datagram Transport Layer Security (DTLS), and (iii) robust and secure mobility-enabled end-to-end communication based on DTLS session resumption. The performance of the state-of-the-art security solutions including our end-to-end security scheme is tested by developing a prototype healthcare IoT system. The prototype is built of a Pandaboard, a TI SmartRF06 board and WiSMotes. The Pandaboard along with the CC2538 module acts as a smart gateway and the WisMotes act as medical sensor nodes. Based on the analysis, we found out that our solution has the most extensive set of performance features in comparison to related approaches found in the literature. The performance evaluation results show that compared to the existing approaches, the cryptographic key generation approach proposed in our end-to-end security scheme is on average 1.8 times faster than existing key generation approaches while being more energy-efficient. In addition, the scheme reduces the communication overhead by 26% and the communication latency between smart gateways and end users by 16%. Our scheme is also approximately 97% faster than certificate based and 10% faster that symmetric key-based DTLS. Certificate based DTLS requires about 2.9 times more ROM and 2.2 times more RAM resources. On the other hand, the ROM and RAM requirements of our scheme are almost as low as in symmetric key-based DTLS.

Keywords: Smart Home/Hospital; Cryptographic Key Generation; Bio-Electrical Signal; Authentication and Authorization; End-to-End Security

1. Introduction

IoT enables physical objects in the physical world as well as virtual environments to interact and exchange information with each other in an autonomous way so as to create smart environments. Healthcare IoT systems are distinct in that they are built to deal directly with the data of human health conditions, which inherently raises the requirements of security, safety and reliability. In addition, they have to offer real-time notifications and responses about the status of patients. In healthcare IoT systems, security and privacy of individuals are among major areas of concern as most devices and their communications are wireless in nature. This is to prevent manipulating and eavesdropping on sensitive medical data or malicious triggering of specific tasks. Key security requirements for healthcare IoT systems consist

* Corresponding author. Tel.: +3-582-333-8647.
E-mail address: saramo@utu.fi

1877-0509 © 2018 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2018.04.064

of three main phases: (1) secure cryptographic key generation, (2) authentication and authorization of each healthcare IoT component, (3) and robust and secure end-to-end communication between sensor nodes and health caregivers are critical requirements[1]. Existing security and protection techniques including cryptographic key generation solutions, secure authentication and authorization, robust end-to-end communication protocols, and privacy assurance cannot be re-used due to the following main reasons: (i) proposed security solutions must be resource-efficient as medical sensor nodes used in healthcare IoT systems have limited memory, processing power, and communication bandwidth, and (ii) medical sensor nodes can be easily abducted or lost since they are tiny in terms of size. To mitigate the above-mentioned risks, robust and lightweight security solutions are needed.

In this paper, we analyze the performance of the state-of-the-art end-to-end security solutions in healthcare IoT systems. The main contributions of this paper are twofold. First, we identify and present the essential requirements of robust security solutions for healthcare IoT systems which include (i) secure ECG-based cryptographic key generation, (ii) authentication and authorization of each healthcare IoT component based on certificate-based Datagram Transport Layer Security (DTLS), and (iii) secure mobility-enabled end-to-end communication based on session resumption technique as well as the concept of fog layer in IoT for realizing efficient and seamless mobility.

The remainder of this paper is organized as follows: Section 2 provides an overview of related work. Section 3 discusses the architecture and requirements of healthcare IoT systems. Section 4 presents our healthcare IoT security solutions. Section 5 provides a comprehensive performance analysis of different security solutions. In this section, the comparison of our work with similar existing approaches is also presented. Finally, Section 6 concludes the paper.

2. Related Work

To establish an efficient inter-operable network security between end-points, variants of end-to-end security protocols have been proposed, among which DTLS is one of the most relevant protocols[2]. DTLS comprises of four main protocols: Handshake, Alert, Change Cipher Spec, and Record. The most recently DTLS-based solutions are proposed by Hummen *et al.*[3], Zack *et al.*[4], Granjal *et al.*,[5] and Kang *et al.*[6]. In[4], authors proposed symmetric key-based DTLS solution as the basic cipher suite of DTLS to reduce packet fragmentation, loss and delay in a low-power and lossy network. However, there is a limitation in the fact that the sensor devices cannot utilize this cipher suite without a pre-shared key (PSK). In[7], authors present a certificate-based raw public key cipher suite. This cipher suite comprises of six flight messages which are fragmented into 27 datagram packets. Nevertheless, packet fragmentation causes issues such as high data loss rate and packet re-transmission delays. To reassemble a fragmented message packet, sensor devices have to keep fragmented pieces of the message in the buffer until all the pieces arrive. This is a considerable burden to the resource-constrained sensor devices. In other works presented in[3,5,6], the authors present an implementation of delegation-based architecture which relies on a delegation server/certificate authority. Their solutions, however, lack scalability and architecture reliability as their proposed architectures are based on a centralized delegation server/certificate authority or on the centralized 6LoWPAN Borader Router (6LBR). The main reason is that their proposed architectures cannot be extended to be utilized in multi-domain infrastructures, such as large hospital environments. If a malicious adversary performs a DoS attack or compromises the 6LBR, a large quantity of stored information concerning the constrained domain can be retrieved. These issues are solved in our scheme as the architecture is distributed. To be more specific, in our scheme, in a multi-domain smart home/hospital environment, if an attacker runs a DoS attack or compromises one of the smart gateways, only the associated medical sub-domain is disrupted. We believe that the approaches presented by Granjal *et al.*[5] and Kang *et al.*[6] do not provide comprehensive end-to-end security. Rather, they can be considered *semi end-to-end* security. This is beacuse in these works, the 6LBR acts as an intermediary node located between the sensor and the end-user. Every time these two end-points try to communicate with each other, all the secret information related to the communication needs to pass through the 6LBR. Whilst, the smart gateway utilized in our work is only used during the initialization phase, and then afterwards, both end-points directly communicate with each other through a channel secured by the DTLS session resumption. Although Hummen *et al.*s'[3] proposed delegation-based architecture offers end-to-end security, it is still not secure against the DoS attack due to the use of a centralized delegation server. Their presented architecture also suffers from shortcomings in architecture reliability and scalability which is mainly due to the reasons mentioned above.

3. Healthcare IoT: Architecture and Requirements

In a typical healthcare IoT system, to monitor patients' vital signs and activities, the system has to ensure the security and privacy of patients. Physicians and other caregivers demand a dependable system in which the results are accurate, timely and the service is reliable and secure. To guarantee these requirements, the smart components in the system require a predictable latency, reliable and robust communication with other components of healthcare IoT systems[8]. The 3-layer system architecture of our proposed healthcare IoT system on which the security solutions can be applied is shown in Figure 1. In such a system, patients' health-related information is recorded by wearable or implantable medical sensor nodes with which the patient is equipped for personal monitoring of multiple parameters. The functionality of each layer is as follows: (1) *Device Layer*, the lowest layer consisting of several physical devices

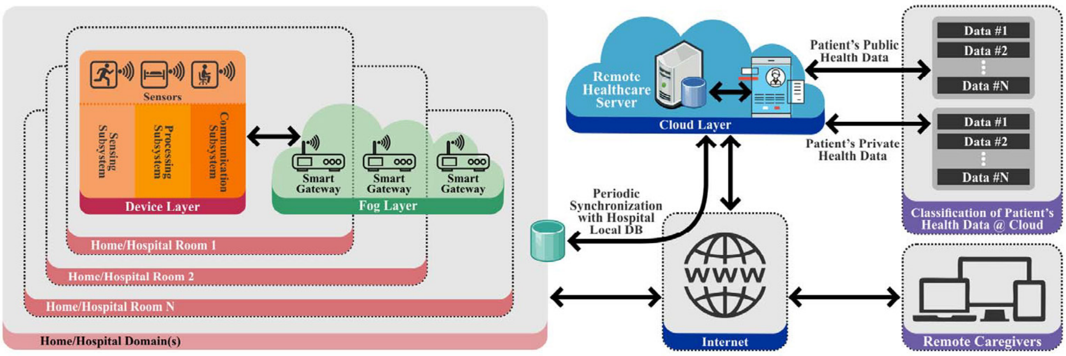


Fig. 1: The system architecture of our healthcare IoT system with secure end-to-end communication

including implantable or wearable medical sensor nodes that are integrated into a tiny wireless module to collect contextual and medical data. (2) *Fog Layer*, the middle layer consists of a network of interconnected smart gateways. A smart gateway receives data from different sub-networks, performs protocol conversion, and provides other higher level services. It acts as repository (local database) to temporarily store sensors' and users' information, and provides intelligence at the edge of the network. (3) *Cloud Layer*, the cloud layer includes broadcasting, data warehousing and big data analysis servers, and a hospital local database that periodically performs data synchronization with the remote healthcare database server in the cloud.

4. Healthcare IoT Security Solutions

As we comprehensively discussed in[1], key security requirements for healthcare IoT systems consist of three main phases: (i) secure and efficient cryptographic key generation for healthcare IoT devices, (ii) authentication and authorization of each healthcare IoT component, and (iii) and robust and secure end-to-end communication between medical sensor nodes and health caregivers. In the following, we briefly present our healthcare IoT security solutions.

4.1. ECG Feature-Based Cryptographic Key Generation

Since medical sensor nodes deal with patients' vital health data, securing their communication is an absolute necessity. Without robust security features not only patients' privacy can be breached but also adversaries can potentially manipulate actual health data resulting in inaccurate diagnosis and treatment. Medical sensor nodes rely on cryptography to secure their communications[9]. Proper application of cryptography requires the use of secure keys and robust key generation methods. Key generation approaches that are proposed for wireless networks in general are not directly applicable to tiny medical sensors as they are highly resource-constrained and demand a higher security level. Given the constrained nature of medical sensor nodes used in healthcare Iot systems, conventional key generation approaches may potentially involve reasonable computations as well as latency during network or any subsequent adjustments, due to their need for pre-deployment. In[10], we presented two different ECG-based cryptographic key generation approaches. The first approach is integrating interpulse interval (IPI) sequence of ECG signal with pseudorandom number that is generated using Fibonacci linear feedback shift register. The generated key is called IPI-PRNG. An alternative key generation approach that utilized the Advanced Encryption Standard (AES) algorithm and IPI sequences as the seed generator for the AES, called IPI-AES. IPI-PRNG and IPI-AES offer higher security levels compared to conventional key generation approaches. In[11], we further improved the ECG-based key generation approach by introducing the use of several ECG Features (SEF) that reduce the key generation execution time overhead significantly while preserving the achieved high security levels. The proposed approach is applied to both normal and abnormal ECG signals. The SEF approach uses 4 main reference-free [1] features of the ECG signal (being extracted from every ECG heartbeat cycle) along with consecutive IPI sequences to generate ECG-based cryptographic keys. To reinforce and enhance the security level of our approach, we consolidate the SEF key generation approach with two different cryptographically secured pseudo random number generators, called, SEF-PRNG and SEF-AES. We evaluated the efficiency of our IPI-PRNG, IPI-AES, SEF, SEF-PRNG, and SEF-AES approaches by simulations on real ECG data from different subjects having various heart health conditions.

4.2. Mutual Authentication and Authorization of Healthcare IoT Components

In the paradigms of healthcare IoT, not only data can be collected by medical sensor nodes and transmitted to end-users, but end-users can also access, control, and manage medical sensors through the Internet. As a result, mutual authentication and authorization of end-users and devices used in healthcare IoT systems is a crucial task. Our proposed architecture, called *SEA*, exploits the role of smart e-health gateways in the fog layer to perform the

[1] In this context, the reference-free property indicates a dynamic technique in which no ECG fiducial point is fixed as reference.

authentication and authorization of remote end-users securely and efficiently on behalf of the medical sensors[12]. *SEA* focuses on a fact that the smart e-health gateway and the remote end-user have sufficient resources to perform various heavy-weight security protocols as well as certificate validation. By providing the established connection context to the medical sensor nodes, these devices no longer need to authenticate and authorize a remote caregiver. It is supposed that within the certificate-based DTLS handshake, from one hand, the smart gateway authenticates the remote end-user through certificates. In this regard, similar to current web browsers, smart gateways hold a pool of trusted certificates. On the other hand, the smart gateway either authenticates to the remote end-user through certificates within the DTLS handshake or based on an application-level password once the handshake is terminated. Once the mutual authentication between the end-user and the smart gateway is done successfully, the end-user authorizes as a trusted entity so that a data query from the end-users' side is transmitted to the medical sensor nodes through the smart gateway. To facilitate the security and authorization of communication, it is required that both entities, the constrained medical sensor node and the smart gateway, also mutually authenticate one another during the initialization phase.

4.3. Secure End-to-End Communication for Mobility Enabled Healthcare IoT

In[1], we enabled secure end-to-end communication between end-points of a healthcare IoT system by developing a session resumption-based scheme which offloads the encrypted session states of DTLS towards a non-resource-constrained end-user. The main motivation to employ the DTLS session resumption is to mitigate the overhead on resource-constrained medical sensors. The session resumption technique is an extended form of the DTLS handshake which enables a client/server to continue the communication with a previously established session state without compromising the security properties. The major advantages offered by our scheme compared to the conventional end-to-end security solution can be found in[1]. We applied our proposed session resumption-based end-to-end security scheme for healthcare IoT to the full system architecture shown in Figure 1. Providing patients with the possibility to walk around the hospital wards knowing that the monitoring of their health condition is not interrupted is an essential feature. To achieve a continuous monitoring of patients considering the mobility support, in[1] , we developed self-configuration/handover mechanisms which are capable of handling secure and efficient data transfers among different medical sensor networks. A fog layer-based data handover mechanism is defined as the process of changing or updating the registration of a mobile sensor from its associated base MSN to the visited MSN, for example, when moving across the hospital's wards. Data handover solutions should enable the ubiquity when they need to work autonomously without human intervention. The handover mechanism should also offer medical sensor nodes continuous connectivity, if there exist several gateways in the hospital or nursing/home environments.

Table 1: Execution time comparison of different ECG-based key generation approaches to produce 128-bit cryptographic keys

Approach	Execution Time Single Iteration (ms)	Execution Time Total (s)	Energy Consumption Single Iteration (μJ)	Energy Consumption Total (mJ)
IPI[9,13]	181.3	2.9	9507.1	527.6
IPI-PRNG	198.6	3.2	11022.3	611.7
IPI-AES	244	3.9	13542	751.5
SEF	104.3	0.9	5788.6	321.2
SEF-PRNG	136.9	1.1	7598	421.6
SEF-AES	168.1	1.3	9884.5	548.5

5. Implementation and Performance Analysis

The system architecture illustrated in Figure 1 is implemented for experimental evaluation for two different scenarios: in-home and hospital room(s). To Implement the proposed healthcare IoT system architecture, we setup a platform that consists of medical sensor nodes, UT-GATE smart e-health gateways, a remote server, and end-users. UT-GATE is constructed from the combination of a Pandaboard and a Texas Instruments (TI) SmartRF06 board that is integrated with a CC2538 module[14]. In our configuration, UT-GATE uses 8GB of external memory and is powered by Ubuntu OS which allows to control devices and services such as local storage and notification. To investigate the feasibility of our proposed architecture, the *Wismote*[15] platform, which is a common resource-limited sensor nodes, is utilized in Contiki's network simulation tool Cooja[3]. For the evaluation, we use the open source tool *OpenSSL* version 1.0.1.j to create elliptic curve public and private keys from the NIST P-256 and X.509 certificates. The server association to the end-user is created using OpenSSL API which provides all necessary functions related to end-users including configuration, certificate, handshake, session state, and cipher suites to support session resumption. *TinyDTLS*[16] is used as the code-base of the proposed scheme. For the public-key functions, we utilize the *Relic-toolkit*[17] that is an open source cryptography library tailored for specific security levels with emphasis on efficiency and flexibility. The MySQL database is set up for static and non-static records. The cloud server database is processed using xSQL Lite which is the third party tool for data synchronization. With respect to the cryptographic primitives and to make a fair comparison, we followed similar cipher suites as employed in the most recently proposed authentication and authorization architecture for IP-based IoT[17]. In this regard, we utilize elliptic curve NIST-256 for public-key operations, $AES\_128\_CCM\_8$ (with an IV of 8 bytes) for symmetric-key, and SHA256 for hashing operations. To asses the performance of different ECG-based cryptographic key generation approaches in terms of execution time, we conduct the experiments on ECG signals of 48 subjects with Arrhythmia obtained from the publicly available database, that is, Physiobank[18]. The recordings are digitized at 360 samples per second with 11-bit resolution over a 10 mV range per patient with 16 bit resolution over a range of 16 mV. We have captured 100 different samples of 5 minute long ECG data for each subject. We have implemented the key generation approaches utilizing MATLAB.

5.1. Cryptographic Key Generation Performance Analysis

In this section, we analyze and compare the performance of different ECG-based cryptographic key generation approaches to produce 128-bit cryptographic keys from the execution time and energy consumption point of views.

5.1.1. Cryptographic Key Generation Execution Time

To investigate the generation execution overhead of our approaches compared to the conventional IPI approach, we have examined the execution time required to generate 128-bit ECG-based cryptography keys. For this purpose, we utilized the *Wismote*[15] platform, which is equipped with a 16MHz MSP430 micro-controller, an IEEE 802.15.4 radio transceiver, 128KB of ROM, 16KB of RAM, and supports 20-bit addressing. Our experiments are carried out on ECG recordings obtained from the MIT-BIH Arrhythmia dataset, sampled at 360 Hz.

Table 1 presents the computed key generation execution times of our IPI-PRNG, IPI-AES, SEF, SEF-PRNG, and SEF-AES approaches as well as the conventional IPI approach. The execution times are presented in both single iteration and total times. Single iteration execution time indicates the time required to produce an *8*-bit binary sequence from one heartbeat cycle. Total execution time means the sum of single iteration execution times until successive iterations of the operations yields the desired result, that is, generates the desired 128-bit ECG-based cryptographic keys. Considering a subject with the ECG heartrate of 60 bpm, the specific MSP430 micro-controller requires about 181 ms, 198 ms and 244 ms execution times per iteration for the IPI, IPI-PRNG, and IPI-AES approaches, respectively. These are the times these three approaches require to produce an 8-bit binary sequence from one ECG heartbeat cycle. To generate 128-bit ECG-based cryptographic keys, it is required for IPI, IPI-PRNG and IPI-AES approaches to compute 16 heartbeat cycles from a subject's ECG signal. The same microcontroller requires about 104.3 ms, 136.9 ms, and 178.1 ms execution times for the SEF, SEF-PRNG, and SEF-AES approaches to produce 16-bits binary sequences from one ECG heartbeat cycle. To generate 128-bit ECG-based cryptographic keys, the SEF, SEF-PRNG and SEF-AES approaches need to compute 8 heartbeat cycles from a subject's ECG signal. As a result, the total key generation execution times of SEF, SEF-PRNG, and SEF-AES approaches are calculated as 104.3 * 8=0.9 (s), 136.9 * 8=1.1 (s), and 168.1 * 8=1.3 (s), respectively, which are considerably lower than their counterparts. The key generation execution times of SEF, SEF-PRNG and SEF-AES are in average 1.8 times times faster than IPI, IPI-PRNG and IPI-AES approaches. This is due to the fact that in IPI, IPI-PRNG and IPI-AES in total 8 bits can be extracted from one ECG heartbeat cycle, while in SEF, SEF-PRNG and SEF-AES approaches in total 16 bits can be extracted from the same heartbeat cycle. Thus, by utilizing additional ECG features, the latency of ECG-based key generation approaches can be significantly reduced. It should be mentioned that, generating these cryptographic keys are performed in an on-demand way and not in every message transaction, for example, once the key is revoked.

5.1.2. Energy Consumption Due to ECG-based Key Generation

To measure the consumed energy of each Wismote sensor node due to key generation, we utilize the following equation: $E = U \times I \times t$ where U represents the supply voltage in Volt (V), I is the current draw of the hardware in milliAmperes (mA) , and t is the key generation execution time in milliseconds (ms). According to the Wismote datasheet that is available in[15], the Wismote sensor node has a current consumption of 18.5 mA and a supply voltage of 3 V. The energy consumption comparison of different ECG-based cryptographic key generation approaches are presented in Table 1. According to the results, SEF, SEF-PRNG and SEF-AES have in average better energy consumption than IPI, IPI-PRNG and IPI-AES approaches. This is due the fact that SEF, SEF-PRNG and SEF-AES approaches require lower execution time. Hence, the energy consumption of the Wismote sensor nodes can be considerably reduced.

5.2. Mutual Authentication and Authorization Performance Analysis

In this section, we analyze the performance of different mutual authentication and authorization approaches from the transmission overhead and latency points of views.

5.2.1. Transmission Overhead

The required number of packet fragments has a direct impact on energy consumption of the healthcare IoT devices. In the following, we analyze the transmission overhead in more detail. As we presented in[10], to perform the certificate-based DTLS handshake, all 15 messages are needed to establish a DTLS connection. When transmitted over size-constrained IEEE 802.15.4 radio links, these messages must additionally be split into several packet fragments due to their extensive message size[3]. As Table 2 presents, we compared the transmission overhead of the proposed SEA approach to the most recent architecture for a successful certificate-based DTLS connection. In delegation-based

Table 2: Performance comparison with the most recently proposed authentication and authorization approach for IoT

	SEA Approach (This Work)	Hummen *et al.*[3]	SEA Approach Improvements (%)
Transmission-overhead (byte)	1190	1609	26
6LoWPAN Fragments (#)	18	24	26
Latency-GE (s)	$\sim$ 15	$\sim$ 15	0
Latency-NG (s)	5.001	6.08	5
Latency-NE (Total) (s)	20.001	21.08	5

architecture, the measured transmission overhead of the certificate-based DTLS handshake is 1609 bytes which cause in total 24 fragments for the transmission of all handshake messages from the delegation server to the end-user[3]. In contrast, our purposed architecture requires transmission of 1190 bytes and it cause 18 fragments totally. As a result, the transmission overhead in our architecture reduces by 26% compared to the delegation-based architecture.

5.2.2. Authentication and Authorization Latency

Latency in this context is defined as the time required from sending a request to confirming the shared session key between two peers. To estimate the authentication and authorization latency, the processing time which is spent from sensor node to the end-user, that is, NE is calculated. This processing time is deduced from the summation of communication latency from sensor node to smart gateway, that is, NG and smart gateway to end-user which can be written as: $Latency_{NE}(s) = Latency_{NG}(s) + Latency_{GE}(s)$. To compute the communication latency from the UT-Gate to the end-user, a proxy server is adjoined to the network. The proposed SEA approach achieves an almost equivalent NG processing time to the delegation-based architecture[3], which takes up to 15 s for the certificate-based DTLS. However, the proposed SEA approach considerably reduces the processing time required for GE compared to the delegation-based architecture. As shown in Table 2, in SEA, the processing time required for GE is about 5.001 s whereas this time increases to about 6.08 s in the delegation-based architecture. Regarding the latency from the gateway to the end-user, the proposed SEA architecture obtains about 16% improvement compared to the delegation-based architecture. When utilizing public keys, the certificate-related processing overhead is no longer available. This is a remarkable advantage as the certificate-related overhead increases linearly with the depth of certificate hierarchy.

5.3. End-to-End Communication Performance Analysis

We analyze the performance of different end-to-end security schemes for mobility enabled healthcare IoT from (i) sensor-side processing time, (ii) sensor-side energy consumption, (iii) data handover latency between gateways, (iv) client-side processing time, (v) client-side run-time performance, and (vi) memory footprint point of views.

5.3.1. Sensor-side Processing Time

The total sensor-side processing time and energy consumption of different DTLS modes to provide end-to-end security is presented in Table 3. For the evaluation, in Cooja, we configured two Wismotes as a client and a server. When the booting process is performed, the client initiates the handshake by sending the *ClientHello* message. After a successful handshake, we measured the total processing time at the sensor-side. Results demonstrated that the symmetric key-based DTLS mode[4] and our session resumption-based scheme require almost similar processing time. The proposed scheme requires 20 ms less processing time than the symmetric key-based mode. This is due to the fewer message flights needed to be exchanged in the session resumption, resulting in less computations at the sensor-side. The processing time for the certificate-based DTLS handshake[7] is considerably higher than both the symmetric key-based and the session resumption-based modes. The certificate-based DTLS requires about 5690 ms at the sensor-side which is mainly due to the expensive public key-based operations. Public key-related operations are the main contributor of sensor-side processing. In this work, there are three classes of public key-related computations. Elliptic Curve Diffie-Hellman (ECDH), the key agreement protocol. ECDH is a key agreement protocol which allows two parties, each having a publicprivate key pair, to establish a shared secret over an insecure channel. ECDH requires in average 437 ms and the deriving of a shared key point requires with 863.2 ms. Elliptic Curve Digital Signature Algorithm (ECDSA) is used for signing the server key exchange message and verifying the certificate message. The

Table 3: Client-side and sensor-side performance analysis of different DTLS modes to provide end-to-end security

	Sensor-side Processing Time (ms)	Sensor-side Energy Consumption (mJ)	Client-side Processing Time (ms)	Client-side Run-time (ms)
DTLS Session Resumption Without Server-side State ($DTLS\_Session\_Resumption\_WITH\_AES\_128$) (This Work)	160	8.87	45	205
Certificate-Based DTLS[7] ($DTLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CCM\_SHA\_256$)	5690	315.79	3744	9434
Symmetric key-Based DTLS[4] ($DTLS\_PSK\_WITH\_AES\_128\_CCM\_8$)	180	9.99	49	229

Table 4: Data handover latency between smart gateways with different packet size

Packet Size (byte)	Data Handover Latency (ms)
10	2.288
50	2.517
100	2.884
500	3.342
1K	3.685
5K	4.588

ECDSA signature requires in average 508.3 ms, whereas the ECDSA signature verification requires with in average 1896.5 ms. This shows how important it is to delegate such expensive operations through session resumption.

5.3.2. Sensor-side Energy Consumption

Similar to the previous section, energy consumption of each Wismote sensor node when performing end-to-end communication is computed using the aforementioned equation. We calculate the energy consumption of the Wismote sensor when performing the DTLS session resumption, the symmetric key-based DTLS, and the certificate-based DTLS. Results presented in Table 3 show that our techniques are considerably more energy efficient in comparison to the certificate-based DTLS[7] technique. It saves 11% of energy compared to the symmetric key-based DTLS[4].

5.3.3. Client-Side Processing Time

The total processing time at the client-side (end-user) using three different approaches is shown in Table 3. For the client-side, we used a machine with $IntelCore^{TM}i5 - 4570$ CPU operating at 2.2 GHz and having 6 GB of RAM. The processing time of our scheme using DTLS session resumption is 45 ms, where as the conventional symmetric key-based[4] requires 49 ms. This is due to the lesser number of control messages needed for session resumption, compared to the full symmetric key-based DTLS. The processing time for certificate-based DTLS handshake[7], is considerably higher than both the symmetric key-based and the session resumption-based modes. The certificate-based DTLS requires approximately 3744ms at the client-side which is mainly due to the expensive public key-based operations. Compared to symmetric key-based and certificate-based DTLS, our session resumption-based scheme has 8.1% and 98.7% improvements in terms of client-side processing time, respectively.

5.3.4. Client-Side Run-time Performance

Run-time refers to the time it takes for the handshake between the medical sensor node and the end-user to be done successfully. To provide end-to-end security, we calculate the total run-time of three different DTLS modes. As can be seen from Table 3, our scheme which exploits the DTLS session resumption technique is about 97% and 10% faster than certificate-based[7] and symmetric key-based DTLS handshake[4], respectively.

5.3.5. Data Handover Latency Between Two Smart Gateways

To demonstrate how our end-to-end security scheme enables mobility, we implemented a real system in which two UT-GATE gateways are employed. It is assumed that these gateways are connected through the fog layer where one of the gateways acts as a client and the other one acts as a server. In the experiments, we created a 100-byte lookup table for each gateway that consists of: i) Control data including the DTLS session resumption state, information about the authorized caregivers, medical sensors' IDs, and patients' IDs, ii) Patients' health data We computed the latency of the data handover process between the gateways. To show the scalability of our method, we considered messages with different sizes which may need to be exchanged between the gateways for the data handover process. As Table 4 presents, data handover latency between two gateways is negligible and mobility is supported in an agile way. In addition, by increasing the packet size, latency marginally increases showing the scalability of our scheme.

5.3.6. Memory Footprint

The memory footprint for symmetric key based DTLS, DTLS session resumption and certificate-based DTLS approaches are analyzed using *msp430-size* tool. For a more detailed information regarding the contribution of each components to static RAM and ROM the tool *msp430-objdump* is used. The results of our evaluation show that the certificate-based DTLS handshake is very expensive for resource-constrained sensor nodes. While, our DTLS session resumption approach requires similar resources as the symmetric key-based DTLS mode. Symmetric key-based DTLS requires 7.79 KB of RAM and 47.23 KB of ROM and our DTLS session resumption approach requires 8.25 KB of RAM and 47.86 KB of ROM. In DTLS session resumption approach, the RAM is just about 0.46 KB higher than symmetric key-based DTLS. This is due to a somewhat larger packet buffer size of DTLS session resumption approach. The certificate-based DTLS approach has the highest memory footprint With 12.32 KB of RAM, that is, 4.53 KB higher than symmetric key-based DTLS mode and 75.98 KB of ROM. This additional value is composed of more RAM requirements for larger packet buffers, session security parameters, certificate and buffering ECDSA signature values. Relic, requires 20.82 KB byte of ROM and and 1.49 KB of RAM. Relic cryptographic toolkit only appears in the certificate-based DTLS approach which makes it the major ROM and RAM contributor of this approach.

Table 5: Detailed Memory footprint of the three different DTLS approaches

	Symmetric Key-Based DTLS[4]		DTLS Session Resumption (This Work)		Certificate-Based DTLS[7]	
Modules	RAM (KB)	ROM (KB)	RAM (KB)	ROM (KB)	RAM (KB)	ROM (KB)
Relic Toolkit	-	-	-	-	1.49	20.82
AES-CCM	0	3.79	0	3.79	0	3.79
SHA2	0.29	2.48	0.29	2.48	0.29	2.48
DTLS-Client	0.22	0.27	0.22	0.27	0.6	0.27
DTLS-Server	0.008	0.21	0.171	0.21	0.42	0.21
Certificate Handler	-	-	-	-	0.02	1.46
DTLS	2.11	9.71	2.75	10.34	5.14	15.91

Symmetric cryptographic primitives of the three approaches that comprises of AES-CCM and SHA2 requires for 6.27 byte of ROM and 0.29 KB of RAM. The similarity is due to the fact that all the three approaches, employ the same symmetric primitives without further modifications. The portion labeled as DTLS in Table 5 is comprises of DTLS handler, state machine and re-transmission modules. As for the DTLS, symmetric key-based DTLS requires 9.71 KB of ROM and 2.11 KB of RAM, our session resumption approach requires 10.34 KB of ROM and 2.75 KB of RAM and 15.91 KB of ROM and 5.14 KB of RAM are required in the certificate-based DTLS, respectively. Certificate handler also appears only in the certificate-based DTLS approach which requires 1.46 KB byte of ROM and and 0.02 KB of RAM. Finally, the rest of RAM and ROM memories are dedicated to stack sizes and the Contiki OS.

6. Conclusions

We analyzed the performance of end-to-end security schemes in healthcare IoT systems. Based on the analysis, we distinguished that our scheme has the most extensive set of performance features in comparison to state-of-the-art end-to-end security schemes. Our end-to-end security scheme was designed by generating ECG-based cryptographic keys for medical sensor devices, certificate-based DTLS handshake between end-users and smart gateways as well as employing the session resumption technique for the communications between medical sensor devices and end-users. Our performance evaluation revealed that, the ECG signal based cryptographic key generation method that is employed in our end-to-end security scheme is on average 1.8 times faster than existing similar key generation approaches while being more energy-efficient. Compared to existing end-to-end security approaches, our scheme reduces the communication overhead by 26% and the communication latency between smart gateways and end users by 16%. Our scheme performed approximately 97% faster than certificate-based and 10% faster than symmetric key-based DTLS. In terms of memory requirements, certificate-based DTLS needs about 2.9 times more ROM and 2.2 times more RAM resources than our approach. In fact, the ROM and RAM requirements of our scheme are almost as low as in symmetric key-based DTLS. Our scheme is a very promising solution for ensuring secure end-to-end communications for healthcare IoT systems with low overhead. Our future work focuses on the trade-off analysis between security level and cost of the end-to-end security schemes in terms of latency and energy consumption.

References

1. S. R. Moosavi et al. End-to-End Security Scheme for Mobility Enabled Healthcare IoT. *Future Generation Computer Systems*, 2016.
2. E. Rescorla et al. Datagram Transport Layer Security (DTLS) Version 1.2. 2012.
3. R. Hummen et al. Delegation-based Authentication and Authorization for IP-based Internet of Things. In *11th IEEE International Conference on Sensing, Communication, and Networking*, pages 284–292, 2014.
4. Z. Shelby et al. CoRE Resource Directory. Internet-draft, 2017.
5. J. Granjal et al. End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication. In *International Conference on Networking*, pages 1–9, 2013.
6. N. Kang et al. ESSE: Efficient Secure Session Establishment for Internet-integrated Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*, pages 1–11, 2016.
7. K. Hartke. Practical Issues with Datagram Transport Layer Security in Constrained Environments. Internet-draft, 2014.
8. A. M. Rahmani et al. Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems. In *12th Annual IEEE Conference on Consumer Communications and Networking*, pages 826–834, Jan 2015.
9. C. Poon et al. A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and m-Health. *IEEE Communications Magazine*, 44(4):73–81, 2006.
10. S. R. Moosavi et al. Cryptographic key generation using ECG signal. In *14th IEEE Annual Consumer Communications Networking Conference (CCNC)*, pages 1024–1031, 2017.
11. S. R. Moosavi et al. Low-latency Approach for Secure ECG Feature Based Cryptographic Key Generation, year=2017. *IEEE Access*.
12. S. R. Moosavi et al. SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways. *Procedia Computer Science*, 52:452 – 459, 2015.
13. G. Zhang et al. Analysis of Using Interpulse Intervals to Generate 128-Bit Biometric Random Binary Sequences for Securing Wireless Body Sensor Networks. *IEEE Transactions on Information Technology in Biomedicine*, 16(1):176–182, 2012.
14. SmartRF06 Evaluation Board. http://www.ti.com/lit/ug/swru321a [accessed 2017-12-24].
15. Arago Systems. Wismote. http://www.aragosystems.com/en/document-center [accessed 2017-12-24].
16. O. Bergmann. TinyDTLS. http://sourceforge.net/p/tinydtls [accessed 2017-12-24].
17. D. Aranha et al. RELIC is an Efficient Library for Cryptography. http://code.google.com/p/relic-toolkit/ [accessed 2017-12-24].
18. A. Goldberger et al. PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals. *Circulation*, 101(23):e215–e220, 2000.

Turku Centre for Computer Science
TUCS Dissertations

1. **Marjo Lipponen**, On Primitive Solutions of the Post Correspondence Problem
2. **Timo Käkölä**, Dual Information Systems in Hyperknowledge Organizations
3. **Ville Leppänen**, Studies on the Realization of PRAM
4. **Cunsheng Ding**, Cryptographic Counter Generators
5. **Sami Viitanen**, Some New Global Optimization Algorithms
6. **Tapio Salakoski**, Representative Classification of Protein Structures
7. **Thomas Långbacka**, An Interactive Environment Supporting the Development of Formally Correct Programs
8. **Thomas Finne**, A Decision Support System for Improving Information Security
9. **Valeria Mihalache**, Cooperation, Communication, Control. Investigations on Grammar Systems.
10. **Marina Waldén**, Formal Reasoning About Distributed Algorithms
11. **Tero Laihonen**, Estimates on the Covering Radius When the Dual Distance is Known
12. **Lucian Ilie**, Decision Problems on Orders of Words
13. **Jukkapekka Hekanaho**, An Evolutionary Approach to Concept Learning
14. **Jouni Järvinen**, Knowledge Representation and Rough Sets
15. **Tomi Pasanen**, In-Place Algorithms for Sorting Problems
16. **Mika Johnsson**, Operational and Tactical Level Optimization in Printed Circuit Board Assembly
17. **Mats Aspnäs**, Multiprocessor Architecture and Programming: The Hathi-2 System
18. **Anna Mikhajlova**, Ensuring Correctness of Object and Component Systems
19. **Vesa Torvinen**, Construction and Evaluation of the Labour Game Method
20. **Jorma Boberg**, Cluster Analysis. A Mathematical Approach with Applications to Protein Structures
21. **Leonid Mikhajlov**, Software Reuse Mechanisms and Techniques: Safety Versus Flexibility
22. **Timo Kaukoranta**, Iterative and Hierarchical Methods for Codebook Generation in Vector Quantization
23. **Gábor Magyar**, On Solution Approaches for Some Industrially Motivated Combinatorial Optimization Problems
24. **Linas Laibinis**, Mechanised Formal Reasoning About Modular Programs
25. **Shuhua Liu**, Improving Executive Support in Strategic Scanning with Software Agent Systems
26. **Jaakko Järvi**, New Techniques in Generic Programming – C++ is more Intentional than Intended
27. **Jan-Christian Lehtinen**, Reproducing Kernel Splines in the Analysis of Medical Data
28. **Martin Büchi**, Safe Language Mechanisms for Modularization and Concurrency
29. **Elena Troubitsyna**, Stepwise Development of Dependable Systems
30. **Janne Näppi**, Computer-Assisted Diagnosis of Breast Calcifications
31. **Jianming Liang**, Dynamic Chest Images Analysis
32. **Tiberiu Seceleanu**, Systematic Design of Synchronous Digital Circuits
33. **Tero Aittokallio**, Characterization and Modelling of the Cardiorespiratory System in Sleep-Disordered Breathing
34. **Ivan Porres**, Modeling and Analyzing Software Behavior in UML
35. **Mauno Rönkkö**, Stepwise Development of Hybrid Systems
36. **Jouni Smed**, Production Planning in Printed Circuit Board Assembly
37. **Vesa Halava**, The Post Correspondence Problem for Market Morphisms
38. **Ion Petre**, Commutation Problems on Sets of Words and Formal Power Series
39. **Vladimir Kvassov**, Information Technology and the Productivity of Managerial Work
40. **Frank Tétard**, Managers, Fragmentation of Working Time, and Information Systems

41. **Jan Manuch**, Defect Theorems and Infinite Words
42. **Kalle Ranto**, Z_4-Goethals Codes, Decoding and Designs
43. **Arto Lepistö**, On Relations Between Local and Global Periodicity
44. **Mika Hirvensalo**, Studies on Boolean Functions Related to Quantum Computing
45. **Pentti Virtanen**, Measuring and Improving Component-Based Software Development
46. **Adekunle Okunoye**, Knowledge Management and Global Diversity – A Framework to Support Organisations in Developing Countries
47. **Antonina Kloptchenko**, Text Mining Based on the Prototype Matching Method
48. **Juha Kivijärvi**, Optimization Methods for Clustering
49. **Rimvydas Rukšėnas**, Formal Development of Concurrent Components
50. **Dirk Nowotka**, Periodicity and Unbordered Factors of Words
51. **Attila Gyenesei**, Discovering Frequent Fuzzy Patterns in Relations of Quantitative Attributes
52. **Petteri Kaitovaara**, Packaging of IT Services – Conceptual and Empirical Studies
53. **Petri Rosendahl**, Niho Type Cross-Correlation Functions and Related Equations
54. **Péter Majlender**, A Normative Approach to Possibility Theory and Soft Decision Support
55. **Seppo Virtanen**, A Framework for Rapid Design and Evaluation of Protocol Processors
56. **Tomas Eklund**, The Self-Organizing Map in Financial Benchmarking
57. **Mikael Collan**, Giga-Investments: Modelling the Valuation of Very Large Industrial Real Investments
58. **Dag Björklund**, A Kernel Language for Unified Code Synthesis
59. **Shengnan Han**, Understanding User Adoption of Mobile Technology: Focusing on Physicians in Finland
60. **Irina Georgescu**, Rational Choice and Revealed Preference: A Fuzzy Approach
61. **Ping Yan**, Limit Cycles for Generalized Liénard-Type and Lotka-Volterra Systems
62. **Joonas Lehtinen**, Coding of Wavelet-Transformed Images
63. **Tommi Meskanen,** On the NTRU Cryptosystem
64. **Saeed Salehi**, Varieties of Tree Languages
65. **Jukka Arvo**, Efficient Algorithms for Hardware-Accelerated Shadow Computation
66. **Mika Hirvikorpi**, On the Tactical Level Production Planning in Flexible Manufacturing Systems
67. **Adrian Costea**, Computational Intelligence Methods for Quantitative Data Mining
68. **Cristina Seceleanu**, A Methodology for Constructing Correct Reactive Systems
69. **Luigia Petre**, Modeling with Action Systems
70. **Lu Yan**, Systematic Design of Ubiquitous Systems
71. **Mehran Gomari**, On the Generalization Ability of Bayesian Neural Networks
72. **Ville Harkke**, Knowledge Freedom for Medical Professionals – An Evaluation Study of a Mobile Information System for Physicians in Finland
73. **Marius Cosmin Codrea**, Pattern Analysis of Chlorophyll Fluorescence Signals
74. **Aiying Rong**, Cogeneration Planning Under the Deregulated Power Market and Emissions Trading Scheme
75. **Chihab BenMoussa**, Supporting the Sales Force through Mobile Information and Communication Technologies: Focusing on the Pharmaceutical Sales Force
76. **Jussi Salmi**, Improving Data Analysis in Proteomics
77. **Orieta Celiku**, Mechanized Reasoning for Dually-Nondeterministic and Probabilistic Programs
78. **Kaj-Mikael Björk**, Supply Chain Efficiency with Some Forest Industry Improvements
79. **Viorel Preoteasa**, Program Variables – The Core of Mechanical Reasoning about Imperative Programs
80. **Jonne Poikonen**, Absolute Value Extraction and Order Statistic Filtering for a Mixed-Mode Array Image Processor
81. **Luka Milovanov**, Agile Software Development in an Academic Environment
82. **Francisco Augusto Alcaraz Garcia**, Real Options, Default Risk and Soft Applications
83. **Kai K. Kimppa**, Problems with the Justification of Intellectual Property Rights in Relation to Software and Other Digitally Distributable Media
84. **Dragoş Truşcan**, Model Driven Development of Programmable Architectures
85. **Eugen Czeizler**, The Inverse Neighborhood Problem and Applications of Welch Sets in Automata Theory

86. **Sanna Ranto**, Identifying and Locating-Dominating Codes in Binary Hamming Spaces
87. **Tuomas Hakkarainen**, On the Computation of the Class Numbers of Real Abelian Fields
88. **Elena Czeizler**, Intricacies of Word Equations
89. **Marcus Alanen**, A Metamodeling Framework for Software Engineering
90. **Filip Ginter**, Towards Information Extraction in the Biomedical Domain: Methods and Resources
91. **Jarkko Paavola**, Signature Ensembles and Receiver Structures for Oversaturated Synchronous DS-CDMA Systems
92. **Arho Virkki**, The Human Respiratory System: Modelling, Analysis and Control
93. **Olli Luoma**, Efficient Methods for Storing and Querying XML Data with Relational Databases
94. **Dubravka Ilić**, Formal Reasoning about Dependability in Model-Driven Development
95. **Kim Solin**, Abstract Algebra of Program Refinement
96. **Tomi Westerlund**, Time Aware Modelling and Analysis of Systems-on-Chip
97. **Kalle Saari**, On the Frequency and Periodicity of Infinite Words
98. **Tomi Kärki**, Similarity Relations on Words: Relational Codes and Periods
99. **Markus M. Mäkelä**, Essays on Software Product Development: A Strategic Management Viewpoint
100. **Roope Vehkalahti**, Class Field Theoretic Methods in the Design of Lattice Signal Constellations
101. **Anne-Maria Ernvall-Hytönen**, On Short Exponential Sums Involving Fourier Coefficients of Holomorphic Cusp Forms
102. **Chang Li**, Parallelism and Complexity in Gene Assembly
103. **Tapio Pahikkala**, New Kernel Functions and Learning Methods for Text and Data Mining
104. **Denis Shestakov**, Search Interfaces on the Web: Querying and Characterizing
105. **Sampo Pyysalo**, A Dependency Parsing Approach to Biomedical Text Mining
106. **Anna Sell**, Mobile Digital Calendars in Knowledge Work
107. **Dorina Marghescu**, Evaluating Multidimensional Visualization Techniques in Data Mining Tasks
108. **Tero Säntti**, A Co-Processor Approach for Efficient Java Execution in Embedded Systems
109. **Kari Salonen**, Setup Optimization in High-Mix Surface Mount PCB Assembly
110. **Pontus Boström**, Formal Design and Verification of Systems Using Domain-Specific Languages
111. **Camilla J. Hollanti**, Order-Theoretic Mehtods for Space-Time Coding: Symmetric and Asymmetric Designs
112. **Heidi Himmanen**, On Transmission System Design for Wireless Broadcasting
113. **Sébastien Lafond**, Simulation of Embedded Systems for Energy Consumption Estimation
114. **Evgeni Tsivtsivadze**, Learning Preferences with Kernel-Based Methods
115. **Petri Salmela**, On Commutation and Conjugacy of Rational Languages and the Fixed Point Method
116. **Siamak Taati**, Conservation Laws in Cellular Automata
117. **Vladimir Rogojin**, Gene Assembly in Stichotrichous Ciliates: Elementary Operations, Parallelism and Computation
118. **Alexey Dudkov**, Chip and Signature Interleaving in DS CDMA Systems
119. **Janne Savela**, Role of Selected Spectral Attributes in the Perception of Synthetic Vowels
120. **Kristian Nybom**, Low-Density Parity-Check Codes for Wireless Datacast Networks
121. **Johanna Tuominen**, Formal Power Analysis of Systems-on-Chip
122. **Teijo Lehtonen**, On Fault Tolerance Methods for Networks-on-Chip
123. **Eeva Suvitie**, On Inner Products Involving Holomorphic Cusp Forms and Maass Forms
124. **Linda Mannila**, Teaching Mathematics and Programming – New Approaches with Empirical Evaluation
125. **Hanna Suominen**, Machine Learning and Clinical Text: Supporting Health Information Flow
126. **Tuomo Saarni**, Segmental Durations of Speech
127. **Johannes Eriksson**, Tool-Supported Invariant-Based Programming

128. **Tero Jokela**, Design and Analysis of Forward Error Control Coding and Signaling for Guaranteeing QoS in Wireless Broadcast Systems
129. **Ville Lukkarila**, On Undecidable Dynamical Properties of Reversible One-Dimensional Cellular Automata
130. **Qaisar Ahmad Malik**, Combining Model-Based Testing and Stepwise Formal Development
131. **Mikko-Jussi Laakso**, Promoting Programming Learning: Engagement, Automatic Assessment with Immediate Feedback in Visualizations
132. **Riikka Vuokko**, A Practice Perspective on Organizational Implementation of Information Technology
133. **Jeanette Heidenberg**, Towards Increased Productivity and Quality in Software Development Using Agile, Lean and Collaborative Approaches
134. **Yong Liu**, Solving the Puzzle of Mobile Learning Adoption
135. **Stina Ojala**, Towards an Integrative Information Society: Studies on Individuality in Speech and Sign
136. **Matteo Brunelli**, Some Advances in Mathematical Models for Preference Relations
137. **Ville Junnila**, On Identifying and Locating-Dominating Codes
138. **Andrzej Mizera**, Methods for Construction and Analysis of Computational Models in Systems Biology. Applications to the Modelling of the Heat Shock Response and the Self-Assembly of Intermediate Filaments.
139. **Csaba Ráduly-Baka**, Algorithmic Solutions for Combinatorial Problems in Resource Management of Manufacturing Environments
140. **Jari Kyngäs**, Solving Challenging Real-World Scheduling Problems
141. **Arho Suominen**, Notes on Emerging Technologies
142. **József Mezei**, A Quantitative View on Fuzzy Numbers
143. **Marta Olszewska**, On the Impact of Rigorous Approaches on the Quality of Development
144. **Antti Airola**, Kernel-Based Ranking: Methods for Learning and Performace Estimation
145. **Aleksi Saarela**, Word Equations and Related Topics: Independence, Decidability and Characterizations
146. **Lasse Bergroth**, Kahden merkkijonon pisimmän yhteisen alijonon ongelma ja sen ratkaiseminen
147. **Thomas Canhao Xu**, Hardware/Software Co-Design for Multicore Architectures
148. **Tuomas Mäkilä**, Software Development Process Modeling – Developers Perspective to Contemporary Modeling Techniques
149. **Shahrokh Nikou**, Opening the Black-Box of IT Artifacts: Looking into Mobile Service Characteristics and Individual Perception
150. **Alessandro Buoni**, Fraud Detection in the Banking Sector: A Multi-Agent Approach
151. **Mats Neovius**, Trustworthy Context Dependency in Ubiquitous Systems
152. **Fredrik Degerlund**, Scheduling of Guarded Command Based Models
153. **Amir-Mohammad Rahmani-Sane**, Exploration and Design of Power-Efficient Networked Many-Core Systems
154. **Ville Rantala**, On Dynamic Monitoring Methods for Networks-on-Chip
155. **Mikko Pelto**, On Identifying and Locating-Dominating Codes in the Infinite King Grid
156. **Anton Tarasyuk**, Formal Development and Quantitative Verification of Dependable Systems
157. **Muhammad Mohsin Saleemi**, Towards Combining Interactive Mobile TV and Smart Spaces: Architectures, Tools and Application Development
158. **Tommi J. M. Lehtinen**, Numbers and Languages
159. **Peter Sarlin**, Mapping Financial Stability
160. **Alexander Wei Yin**, On Energy Efficient Computing Platforms
161. **Mikołaj Olszewski**, Scaling Up Stepwise Feature Introduction to Construction of Large Software Systems
162. **Maryam Kamali**, Reusable Formal Architectures for Networked Systems
163. **Zhiyuan Yao**, Visual Customer Segmentation and Behavior Analysis – A SOM-Based Approach
164. **Timo Jolivet**, Combinatorics of Pisot Substitutions
165. **Rajeev Kumar Kanth**, Analysis and Life Cycle Assessment of Printed Antennas for Sustainable Wireless Systems
166. **Khalid Latif**, Design Space Exploration for MPSoC Architectures

167. **Bo Yang**, Towards Optimal Application Mapping for Energy-Efficient Many-Core Platforms
168. **Ali Hanzala Khan**, Consistency of UML Based Designs Using Ontology Reasoners
169. **Sonja Leskinen**, m-Equine: IS Support for the Horse Industry
170. **Fareed Ahmed Jokhio**, Video Transcoding in a Distributed Cloud Computing Environment
171. **Moazzam Fareed Niazi**, A Model-Based Development and Verification Framework for Distributed System-on-Chip Architecture
172. **Mari Huova**, Combinatorics on Words: New Aspects on Avoidability, Defect Effect, Equations and Palindromes
173. **Ville Timonen**, Scalable Algorithms for Height Field Illumination
174. **Henri Korvela**, Virtual Communities – A Virtual Treasure Trove for End-User Developers
175. **Kameswar Rao Vaddina**, Thermal-Aware Networked Many-Core Systems
176. **Janne Lahtiranta**, New and Emerging Challenges of the ICT-Mediated Health and Well-Being Services
177. **Irum Rauf**, Design and Validation of Stateful Composite RESTful Web Services
178. **Jari Björne**, Biomedical Event Extraction with Machine Learning
179. **Katri Haverinen**, Natural Language Processing Resources for Finnish: Corpus Development in the General and Clinical Domains
180. **Ville Salo**, Subshifts with Simple Cellular Automata
181. **Johan Ersfolk**, Scheduling Dynamic Dataflow Graphs
182. **Hongyan Liu**, On Advancing Business Intelligence in the Electricity Retail Market
183. **Adnan Ashraf**, Cost-Efficient Virtual Machine Management: Provisioning, Admission Control, and Consolidation
184. **Muhammad Nazrul Islam**, Design and Evaluation of Web Interface Signs to Improve Web Usability: A Semiotic Framework
185. **Johannes Tuikkala**, Algorithmic Techniques in Gene Expression Processing: From Imputation to Visualization
186. **Natalia Díaz Rodríguez**, Semantic and Fuzzy Modelling for Human Behaviour Recognition in Smart Spaces. A Case Study on Ambient Assisted Living
187. **Mikko Pänkäälä**, Potential and Challenges of Analog Reconfigurable Computation in Modern and Future CMOS
188. **Sami Hyrynsalmi**, Letters from the War of Ecosystems – An Analysis of Independent Software Vendors in Mobile Application Marketplaces
189. **Seppo Pulkkinen**, Efficient Optimization Algorithms for Nonlinear Data Analysis
190. **Sami Pyöttiälä**, Optimization and Measuring Techniques for Collect-and-Place Machines in Printed Circuit Board Industry
191. **Syed Mohammad Asad Hassan Jafri**, Virtual Runtime Application Partitions for Resource Management in Massively Parallel Architectures
192. **Toni Ernvall**, On Distributed Storage Codes
193. **Yuliya Prokhorova**, Rigorous Development of Safety-Critical Systems
194. **Olli Lahdenoja**, Local Binary Patterns in Focal-Plane Processing – Analysis and Applications
195. **Annika H. Holmbom**, Visual Analytics for Behavioral and Niche Market Segmentation
196. **Sergey Ostroumov**, Agent-Based Management System for Many-Core Platforms: Rigorous Design and Efficient Implementation
197. **Espen Suenson**, How Computer Programmers Work – Understanding Software Development in Practise
198. **Tuomas Poikela**, Readout Architectures for Hybrid Pixel Detector Readout Chips
199. **Bogdan Iancu**, Quantitative Refinement of Reaction-Based Biomodels
200. **Ilkka Törmä**, Structural and Computational Existence Results for Multidimensional Subshifts
201. **Sebastian Okser**, Scalable Feature Selection Applications for Genome-Wide Association Studies of Complex Diseases
202. **Fredrik Abbors**, Model-Based Testing of Software Systems: Functionality and Performance
203. **Inna Pereverzeva**, Formal Development of Resilient Distributed Systems
204. **Mikhail Barash**, Defining Contexts in Context-Free Grammars
205. **Sepinoud Azimi**, Computational Models for and from Biology: Simple Gene Assembly and Reaction Systems
206. **Petter Sandvik**, Formal Modelling for Digital Media Distribution

207. **Jongyun Moon**, Hydrogen Sensor Application of Anodic Titanium Oxide Nanostructures
208. **Simon Holmbacka**, Energy Aware Software for Many-Core Systems
209. **Charalampos Zinoviadis**, Hierarchy and Expansiveness in Two-Dimensional Subshifts of Finite Type
210. **Mika Murtojärvi**, Efficient Algorithms for Coastal Geographic Problems
211. **Sami Mäkelä**, Cohesion Metrics for Improving Software Quality
212. **Eyal Eshet**, Examining Human-Centered Design Practice in the Mobile Apps Era
213. **Jetro Vesti**, Rich Words and Balanced Words
214. **Jarkko Peltomäki**, Privileged Words and Sturmian Words
215. **Fahimeh Farahnakian**, Energy and Performance Management of Virtual Machines: Provisioning, Placement and Consolidation
216. **Diana-Elena Gratie**, Refinement of Biomodels Using Petri Nets
217. **Harri Merisaari**, Algorithmic Analysis Techniques for Molecular Imaging
218. **Stefan Grönroos**, Efficient and Low-Cost Software Defined Radio on Commodity Hardware
219. **Noora Nieminen**, Garbling Schemes and Applications
220. **Ville Taajamaa**, O-CDIO: Engineering Education Framework with Embedded Design Thinking Methods
221. **Johannes Holvitie**, Technical Debt in Software Development – Examining Premises and Overcoming Implementation for Efficient Management
222. **Tewodros Deneke**, Proactive Management of Video Transcoding Services
223. **Kashif Javed**, Model-Driven Development and Verification of Fault Tolerant Systems
224. **Pekka Naula**, Sparse Predictive Modeling – A Cost-Effective Perspective
225. **Antti Hakkala**, On Security and Privacy for Networked Information Society – Observations and Solutions for Security Engineering and Trust Building in Advanced Societal Processes
226. **Anne-Maarit Majanoja**, Selective Outsourcing in Global IT Services – Operational Level Challenges and Opportunities
227. **Samuel Rönnqvist**, Knowledge-Lean Text Mining
228. **Mohammad-Hashem Hahgbayan**, Energy-Efficient and Reliable Computing in Dark Silicon Era
229. **Charmi Panchal**, Qualitative Methods for Modeling Biochemical Systems and Datasets: The Logicome and the Reaction Systems Approaches
230. **Erkki Kaila**, Utilizing Educational Technology in Computer Science and Programming Courses: Theory and Practice
231. **Fredrik Robertsén**, The Lattice Boltzmann Method, a Petaflop and Beyond
232. **Jonne Pohjankukka**, Machine Learning Approaches for Natural Resource Data
233. **Paavo Nevalainen**, Geometric Data Understanding: Deriving Case-Specific Features
234. **Michal Szabados**, An Algebraic Approach to Nivat's Conjecture
235. **Tuan Nguyen Gia**, Design for Energy-Efficient and Reliable Fog-Assisted Healthcare IoT Systems
236. **Anil Kanduri**, Adaptive Knobs for Resource Efficient Computing
237. **Veronika Suni**, Computational Methods and Tools for Protein Phosphorylation Analysis
238. **Behailu Negash**, Interoperating Networked Embedded Systems to Compose the Web of Things
239. **Kalle Rindell**, Development of Secure Software: Rationale, Standards and Practices
240. **Jurka Rahikkala**, On Top Management Support for Software Cost Estimation
241. **Markus A. Whiteland**, On the k-Abelian Equivalence Relation of Finite Words
242. **Mojgan Kamali**, Formal Analysis of Network Routing Protocols
243. **Jesús Carabaño Bravo**, A Compiler Approach to Map Algebra for Raster Spatial Modeling
244. **Amin Majd**, Distributed and Lightweight Meta-heuristic Optimization Method for Complex Problems
245. **Ali Farooq**, In Quest of Information Security in Higher Education Institutions: Security Awareness, Concerns, and Behaviour of Students
246. **Juho Heimonen**, Knowledge Representation and Text Mining in Biomedical, Healthcare, and Political Domains

247. **Sanaz Rahimi Moosavi**, Towards End-to-End Security in Internet of Things based Healthcare

Turku Centre *for* Computer Science

http://www. tucs.fi
tucs@abo.fi

University of Turku
Faculty of Science and Engineering
- Department of Future Technologies
- Department of Mathematics and Statistics

Turku School of Economics
- Institute of Information Systems Science

Åbo Akademi University
Faculty of Science and Engineering
- Computer Engineering
- Computer Science

Faculty of Social Sciences, Business and Economics
- Information Systems

ISBN 978-952-12-3883-3
ISSN 1239-1883

Sanaz Rahimi Moosavi Towards End-to-End Security in Internet of Things based Healthcare

Sanaz Rahimi Moosavi Towards End-to-End Security in Internet of Things based Healthcare

Sanaz Rahimi Moosavi Towards End-to-End Security in Internet of Things based Healthcare