UNIVERSITY OF TURKU

Internet of Things security

Case: IoToys

Information and Communication Technology
Faculty of Technology
bachelor's thesis

Author:
Noorulzahraa Al-Sulttan

May 2025
Turku

Bachelor's Thesis
Subject: Information and Communication Technology
Author: Noorulzahraa Al-Sulttan
Title: Internet of Things Security – Case: IoToys
Number of pages: 23 pages
Date: May 2025

The Internet of Things (IoT) is expanding rapidly, with an estimated 30 billion devices by 2025, and with this growth comes security challenges. This thesis examines the security requirements and architectural framework of the IoT, highlighting the need for confidentiality, integrity, authorisation, authentication and availability. It looks at different IoT architectures, including three-, four- and five-layer models, and identifies common security threats such as node capture, sniffing, false data injection and denial of service attacks. It also highlights the vulnerabilities of the Perception and Network layers, and suggests advanced security measures, including AI-driven technologies such as blockchain, to enhance IoT security. A focused analysis of smart toys reveals specific security concerns, such as unprotected network ports, unsecured Bluetooth, and lack of data encryption, which pose risks to children's privacy and safety. The study concludes with recommendations for improving IoT security, particularly for IoToys, through increased parental awareness, secure communication channels and strong security protocols.

Key words: Internet of Things (IoT), Security requirements, IoT architectures, Security threats, AI-driven security, Smart toys security Smart toys.

Contents

1 Introduction

Computer security expert, Eugene Spafford once said, “The only truly secure system is one that is powered off, cast in a block of concrete, and sealed in a lead-lined room with armed guards—and even then, I have my doubts.” [1]. There is a sobering truth in his statement: Absolute security is an illusion. In the technology industry, every layer of protection contains potential vulnerabilities.

Security can be defined as a system remaining in a correct state, despite the efforts of the malicious adversary, perhaps in conspiracy with an uncooperative universe. [2]

Internet use is growing. More and more devices are being connected to the Internet. It is estimated that there will be 30 billion Internet of Things IoT devices by 2030 [3].However, according to the Statista website, we will reach 30 billion devices five years earlier, in 2025, as shown in Figure 1 [4].

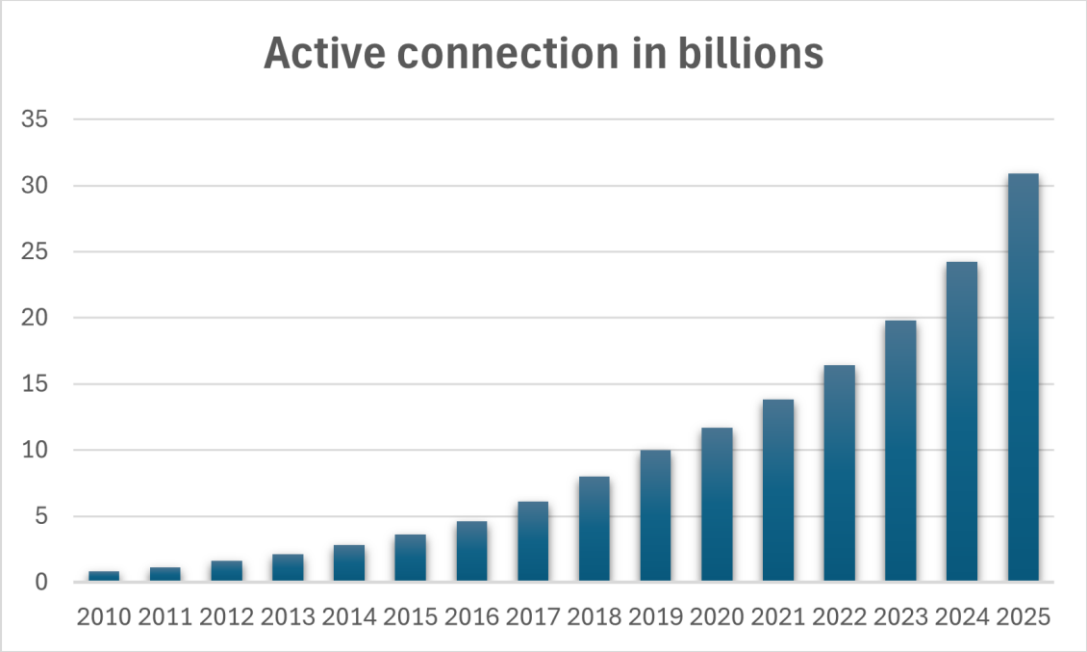

Figure 1 IoT active device connections worldwide from 2010 to 2025 [4].

The Internet of Things has become an extremely interesting area of research. The growth of IoT devices is associated with an increase in various security risks. Many researchers have raised concerns about security issues in the IoT [3][4][5][6]. In October 2016, Twitter and Netflix were hit by a DoS attack because users were unable to access these platforms [7]. This is evidence that even large platforms, which have a reputation for efficient security, are not immune to cyber-attacks. Furthermore, finding solutions to the security problems that arise may not be synchronized with the rapid development in this area.

Another case that raised security concerns was the Verkada hack (2021), Verkada is a security camera company that had security vulnerabilities that allowed a hacker to access security cameras connected to the internet and view patients in mental health and women's health clinics. [8]

IoT devices collect data from their environment through sensors. When the collected data is analyzed, user actions can be highly predictive. It is therefore scary to consider what can be done with the collected data when malicious activity occurs.

Inspired by Spafford's statement, the focus of this thesis is on the security issues in the IoT specifically the case of smart toys. Smart toys are IoT devices. They have a particularly vulnerable target group. Children are particularly vulnerable users, because they may not fully understand the implications of sharing personal information, connecting devices to networks, or interacting with smart technologies. This lack of awareness, combined with their natural curiosity, makes them an easy target for exploitation and a critical demographic to consider when addressing IoT security concerns.

Since no system is secure, security awareness is the second-best solution. To achieve such awareness of security issues and threats, this thesis presents different IoT architecture models and related security issues for each model, address answers to the following questions:

RQ1: What are the main security threats and issues for IoT?

RQ2: How IoT architecture layers are affected by the identified threats and issues?

RQ3: How do the security issues in IoT impact smart toys security?

For the literature review, the keywords are “IoT security”, “IoT architecture”, “security requirements”, “privacy and security AND IoT”, “IoT protocols”, “wireless protocols AND IoT”, “IoT security threat”, “smart puppet”, “smart toy”, “smart toy and AI”, “IoT AND AI”, “AI AND security”, “AI and IoT security”. The databases of articles used in the thesis were the following: IEEE, ACM, Research Gate, Web of Science. The sources were selected based on the most relevant ones. However, the distribution of relevant sources was not equivalent. Research indicates that there are more resources available for instances on “IoT” than “IoT AND AI”. Furthermore, there is a shortage of relevant resources on IoToys. Furthermore, while there were numerous relevant resources on the subject of “AI AND security”, there was a lack of material specifically addressing “AI and IoT security”. Therefore, some topic was researched individually, and the dots were then connected to create a comprehensive overview of the topic.

The structure of the thesis is as follows: in chapter two, the IoT security and architecture are examined through three main topics which are security requirements for IoT systems, IoT architecture and security issues. In addition, the security issues in the system are mapped. The third chapter discusses the case of smart toys, focusing on the possible risks in the interaction between children and smart toys, security risks and possible recommendations for safe use. Finally, chapter four represents the conclusions and answers to the research questions.

2 IoT security and architecture

The term Internet of Things was coined in 1999 by technologist Kevin Ashton, he states that the IoT has great potential to affect everything [4]. This statement holds true as we witness the growth of the IoT. IoT refers to the network of devices that can communicate and exchange data with each other, integrating heterogeneous systems and devices [5]. IoT devices are known as smart objects, e.g. smart homes, smart cities, smart toys, etc. IoT devices not only exchange data autonomously but also perform various tasks autonomously.

2.1 IoT security requirements

IoT systems face many security challenges, especially because IoT relies on many technologies that are still in the early stages of development. For example, sensors, wireless communication and cloud computing [6]. There are many questions that need to be answered when designing a secure system, such as What makes a system secure? Is a simple system more secure than a complex one? What is a good cost to design a secure system? Well, in [6] it is shown that simplicity can be a reason for a system with many vulnerabilities when it comes to confidentiality. As for the cost, it depends on many factors, but the cost must not exceed the value of what it's protecting [1].

Furthermore, before diving deeper into the security issues, it is important to introduce the security requirements that an IoT system should fulfill, regardless of the architecture used. Failure to meet these requirements is called a security problem. Over time, the requirements have changed depending on the security needs, in 1980 the requirements were confidentiality, integrity, and availability [7]. Later the requirements were authorization, confidentiality, integrity, availability, and authentication [6][1][8]. Requirements are illustrated in Figure 2.

Authentication and authorization are the keystones of security in an IoT environment, ensuring the identity of users accessing devices [8]. Authentication is the process of verifying that a claim of identity is correct. It is important to remember that authentication is different from verification. Verification is the process of checking that something is true. Authorization is what gives an authenticated identity the role of what exactly it can do. [1]

Authentication and authorization are good approaches to malicious actions. Brute force is a type of attack that uses this approach. Attackers try to gain access to the system by guessing possible credentials to the system [6].

Confidentiality is the protection of data from unauthorized access [1]. Even though IoT devices work collaboratively, devices do not share data with neighboring devices. Confidentiality can be achieved through data encryption and two-step verification [9][6]. The challenges with these methods are high computational and energy requirements, as IoT device sensors have limited processing capabilities and are designed to operate with minimal energy consumption [9]. However, lightweight cryptographic algorithms can be a solution that suits IoT [9][1].

Integrity is the process of preventing unauthorised access to make changes to the data [1]. It also ensures that data is not altered during transmission, either intentionally or unintentionally [9]. Integrity can be divided into code integrity and data integrity. One of the best ways to achieve integrity is through symmetric cryptographic algorithms, such as HMAC HASH-based authentication methods and digital signatures [5]. HMAC is a technique that uses hash-function and a secret key for authentication. However, asymmetric algorithms are more efficient, but also more resource consuming compared to symmetric algorithms [6].

Availability means that data is accessible when it is needed [1]. IoT devices and their services need to be constantly available and connected, so availability is a must in IoT. However, it is also a major target for attackers, because it means the device is always available for malicious actors [7]. DoS is an example of an attack that can lead to service unavailability.

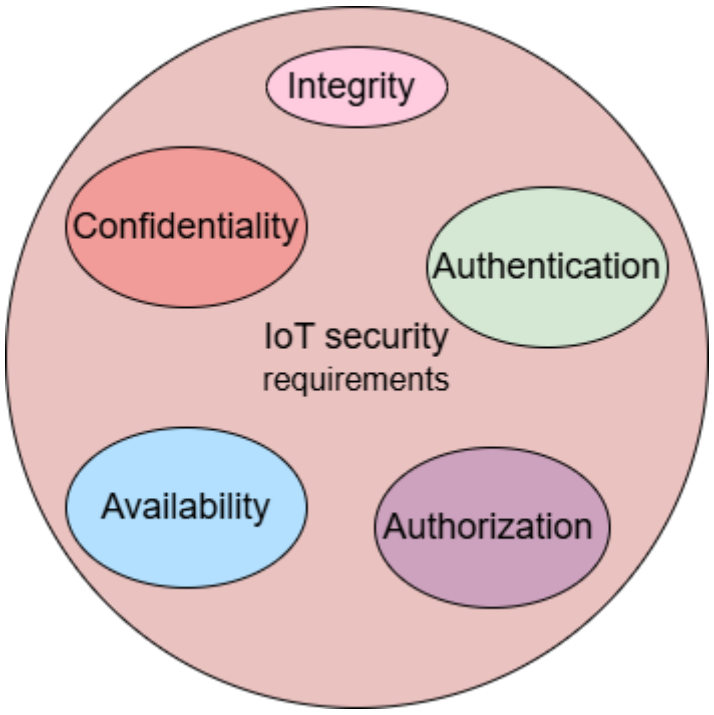

Figure 2 Security requirements in IoT

2.2 Architectures

The term IoT architecture refers to the framework that defines how different elements of the IoT interact within the IoT environment. The basic and most commonly used IoT architecture is a three-layer model, which divides the IoT system into three different main layers [7]. Furthermore, in this chapter, we will introduce the three-layer architecture, four-layer architecture, and five-layer architecture and demonstrate the core functionalities in different models. Figure 3 represents the different models and included layers. However, regardless of the different models, all IoT models have similar functionalities.

The ***three-layer architecture*** includes a recognition layer, a network layer, and an application layer [10], layers are also called application layer, network layer, and perception layer [11].

In the ***four-layer architecture***, the layers are divided into the application layer, middleware layer, network layer, and perception layer. [9]

The ***five-layer architecture***, in [12], five-layer model includes a perception layer, network layer, middleware layer, application layer, and business layer. [13] introduces the five-layer architecture with the same names as mentioned above. [10] introduced five layers perception layer, transport layer, processing layer, application layer, and business layer. Regardless of the differences in the names of the layers, they all have the same functionalities.

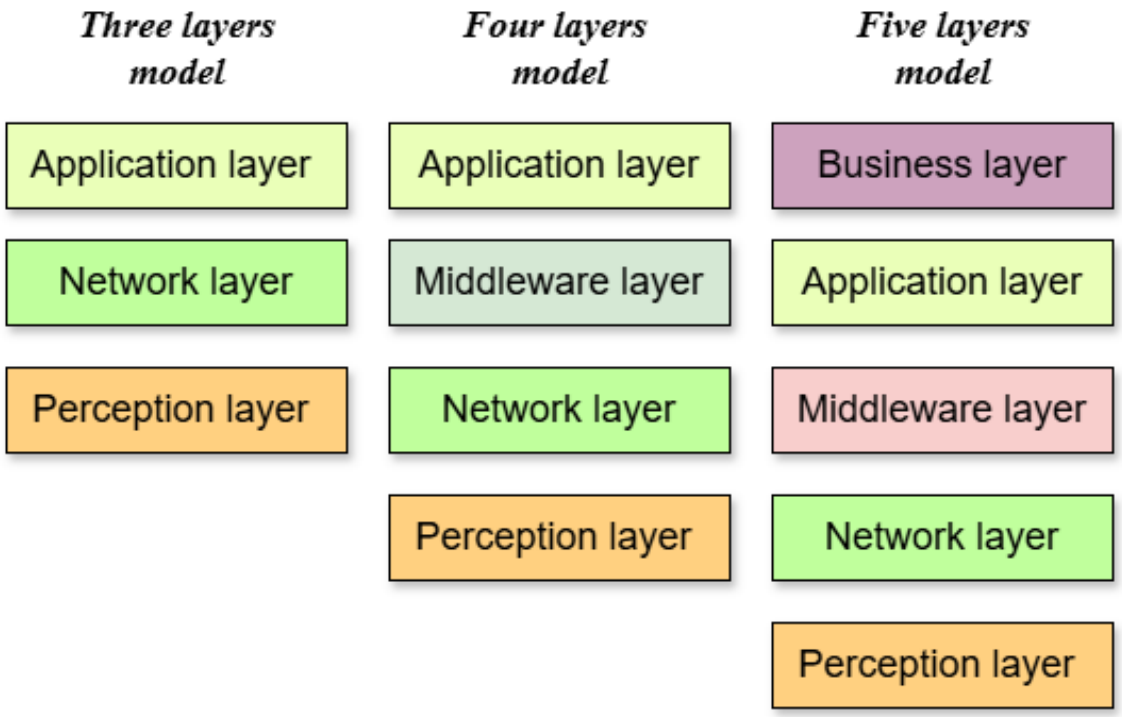

Figure 3 IoT architecture models

The description of the functionality of different layers using the five layers architecture:

Perception layer, which is also known as the sensor layer, it is the physical layer of IoT. It collects data from the environment of IoT objects and identifies objects. Additionally, it executes commands [7]. The perception layer has two components which are perception nodes and perception networks [8]. The perception node is responsible for collecting data, on the other hand, the network is responsible for communication between the perception layer and network layer for sending data and receiving commands [9].

In many cases, it includes sensors and actuators embedded in the environment [7]. The perception layer uses different protocols divided into communication and transmission protocols. Communication protocols include Wi-Fi, Bluetooth, and Zigbee, wireless communication protocols; in which Zigbee and Bluetooth are considered to have lower power consumption than Wi-Fi [9]. Transmission protocols are Hypertext Transfer Protocol HTTP, Constrained Application Protocol CoAP, and Message Queuing Telemetry Transport MQTT.

Network layer is responsible for transmitting the data collected by the sensor layer to the middleware or application layer via wired or wireless technologies, depending on the model used [9][14]. Additionally, it connects different devices. It plays the same role as the physical layer in a four-layer architecture [15]. The network layer also performs the initial classification and processing of data [9].

The network layer is critical to enable devices to work collaboratively. Therefore, network deployment, management, and scheduling are essential in network layer [6]. And because of the network layer's critical role, it is very important to be highly secured.

Middleware layer it is the service management layer. It integrates services and applications operations [10]. It has functionalities such as data storage, computation, processing, and analysis. It processes the received data enable IoT object to makes decisions [11].

Application layer works as an interface layer that connects network and IoT devices [9]. It processes the data it receives from the previous layers, and based on this data, it provides different services [7][8]. In addition, it has the authority to provide different services based on the data from the sensor layer. There are no general standards for the application in IoT, which makes it difficult to design security patterns [8].

Business layer manages the entire IoT system. It monitors and manages the underlying four layers. It has functionalities to structure flowcharts, and graphs, and analyse results because this business layer can improve IoT system performance. [8]

2.3 Threat in IoT Environments

IoT systems are vulnerable to a variety of attacks [16][17]. These attacks are presented at different layers. IoT layers rely on each other's data, therefore any damage in any layer can cause the device to perform wrong actions, and since IoT is the connection of different devices and different systems, any attack can be highly damaging.

Node capture while IoT consists of multiple low-energy nodes. These nodes can be targeted in many ways. Attackers replace the network node with a capture node. This node is observable by the system and controlled by the attackers. [12][13]

Sniffing attacks appear when attackers put malicious sensors or devices in the actual physical device to collect data [13]. In 2017 Mariott International was targeted to a data breach. Attackers were able to get to over 500 million guest records that contained personal information [14]. According to the Medium website, Mariott was the target of the same attack in 2018 and 2020, where almost 5.2 million guest records were impacted [15].

Manipulation an attack that involves altering, injecting, or tampering with data, configurations, or hardware components to exploit a system’s vulnerabilities. Manipulation attacks can be represented in different forms which are malicious code attacks, manipulation of unstable configurations, and injection of fake information. [13]

Malice code injection is an attack in which the attacker will lead the IoT node to execute unintentional functions by inserting a code for them [12]. Malicious code attacks are, for instance, botnet Mirai, ransomware, and manipulation [13]. In a botnet Mirai attacker can listen to the network activity. In ransomware, the attacker sends packets for the purposes of attacking of communicating. Traditionally the ransomware attacker suspends the user from getting into their device or documents, till the ransom is paid [16]. Manipulation attack which represents hardware or sensors [13].

Manipulation of unstable configuration attack where attackers exploit misconfigured remote servers, operating systems, or cloud storage settings in an IoT environment which leads to unauthorized access, data leaks, or security breaches at the application layer. [13]

False data attack occurs when the attackers insert wrong data into the IoT network and because IoT makes real-time decisions this can lead to the device executing the wrong command [12][17]. This also makes the IoT network more vulnerable to various types of attacks [13]. If the attacker can inject false data to the sensor layer in IoT, that collects data. This data will be transmitted to the rest of the system through the network layer and based on the false data the IoT device will take action. For instance, smoke alarm devices that are found in every apartment, if these devices were injected with false data, will either make false emergency calls or not make any emergency calls even when it is needed.

Jamming attack is where the attacker disrupts communication in the IoT network, by blowing up the radio link, and sends corrupting or lost messages to temporarily suspend or block connection to the nodes. Eventually, it will stop the service of IoT and exhaust resource [18][12][13]. GPS jamming devices are an example of a jamming technique.

Phishing, experts call it also identity theft. It occurs when a malicious actor makes an identical website to the original or pretends to be a legitimate one to manipulate users to provide sensitive data such as username and password leading to making an entire IoT device vulnerable to cyber-attack [13][12]. For instance, spam emails are categorized as phishing attacks. This type of attack requires a minimal effort to achieve. Phishing damages the confidentiality of the system [13].

Authorization attack in which during it an unauthorized person gains access to the IoT network. The attacker is not seeking to disrupt the IoT network but rather to collect sensitive information, or gain control without being detected, because the attacker is not identified on the network [12]. Unlike the phishing attack, this attack requires technical skills to achieve.

Denial-of-Service DoS attack is an malicious action where the attacker overwhelms the network by sending too many requests that eventually will drown the user's machine and network [12]. DoS attack and DDoS attack differences are that in a DDoS attack, multiple sources flood the network with traffic to overwhelm the targeted network. A recent DDOS attack was in 2021 when Azure experienced the largest attack at the time. The attack sources were almost 10 000 that are located in 10 different countries [19].

Routing attack is an malicious action that aims to restructure the path and draw nodes [12]. Routing attacks include selective forward attack, Sybil attack, hello flood attack, and reply attack [20][21].

Hello flood attack where the attacker captures a node and sends a Hello message with a high power, so the nodes of the network will consider it to be a parent node. Therefore, all messages and communications will be routed through the captured node which can cause significant damage to the system [12][13]. In a Hello flood attack, the targeted network will congest [21]. Therefore, it is harder to detect the attack when the network is congested.

Replay attack in which legitimate node messages are recorded by a malicious node and can be used later in the network to reorder data packets. [22][20]

Sybil attack achieved by using a malicious single node to operate several identities to track other nodes [12]. This can damage many network agreements. When the Sybil attack succeeds the attack becomes capable of destroying the distributed storage mechanism, the routing mechanism, and the sensor network data marge mechanism [23]. A Sybil attack is divided into three categories SA1, SA2, and SA3 [20]. In SA1, the malicious node forms a bond within one specific area. Unlike SA1, in SA2 the malicious nodes are scattered among legitimate nodes. SA3 is similar to SA2 but SA3 nodes can be mobile.

Selective forward attack/ Gray hole attack is a variant of black hole attacks in which the attacker selectively drops packets, resulting in partial or total data loss for every packet routed through this malicious node [23]. It selectively forwards packets while dropping everything else [19][20].

Man-in-the-middle MITM is when a third party breaks into the connection of two parties. This will allow the third party to collect desired data. Because IoT devices share real-time data, MITM attacks can target multiple devices simultaneously [11][24][13][25]. Common MITM attacks are Wi-Fi eavesdropping and Domain Name System Spoofing DNS [11]. One of the most famous MITM attacks is the Equifax attack. Equifax is a multinational consumer credit reporting agency, which reported in 2017 that malicious actors gained access to the sensitive information of 143 million American consumers [25].

Extra interfaces attack in which the attacker finds an extra port of the IoT gateway for backdoor authentication which results in the disclosure of users' information. [11]

Side-channel attack SCA where is the attacker takes advantage of information leakage in the physical device to form an attack [13]. The leakage may be related to timing, power, electromagnetic signals, sound, and light. SCA is a non-intrusive and passive attack that is performed without removing the chip to gain direct access to the physical device [11]. It is used usually against encrypted devices.

Spoofing is an attack in which a malicious actor pretends to be illegitimate equipment to obtain illicit entry or interfere with normal operations. [26]

Table 1 IoT attacks in located in different layers

Perception layer	Network layer	Middleware layer	Application layer	Other (gateway)
Node capture	DDoS	Hello flood attack	DoS	False data attack
False data attack	Hello flood	MITM attack	Sniffing code	End-to-End encryption
Jamming	Replay attack	-	Authorization access attack	Extra interfaces
Sniffing attack	Sybil attack	-	False data attack	-
Malicious code injection	Gray hole attack	-	-	-
Malicious node	MITM	-	-	-
Side-channel attack	Phishing attack	-	-	-
Battery drainage attack	Malicious node	-	-	-

The mapping of different attacks is shown in Table 1 above. We can observe that the most vulnerable layers in IoT systems are the perception layer and the network layer.

Security threats can be divided into physical and digital access threats, as shown in Table 2. Physical access threats often need direct contact with the devices, unlike digital access threats. IoT security has been researched very well, therefore, finding data was not an obstacle.

Table 2 Physical access attacks VS digital access attacks

Physical access threats	Digital access threats
Node capture	DDoS
Jamming	Hello flood attacks
Extra interfaces	DOS
Side-Channel-Attack	False data attack
Battery Drainage attack	MITM
-	Sniffing attack
-	Replay attack
-	Authorization access attack
-	Sybil attack
-	Malicious code injection
-	Gray hole attack
-	Malicious node attack
-	Phishing attack

The objectives of these attacks vary: some target data access for purposes such as manipulation, theft, or injecting false information, while others focus on disrupting system operations or causing failures. Table 3 categorizes these attacks into two groups: those that exploit data and those that hinder system functionality. However, when a security system is designed, it should mitigate any kind of attack regardless of its place in the category.

Table 3 Classification of IoT Attacks Based on Data Exploitation and System Disruption

Attacks that use data	Attacks that hinder the system
Node Capture	Jamming
Sniffing Attacks	DoS & DDoS
Routing Attacks (Replay Attack, Sybil Attacks)	Routing Attacks (Hello Flood, Selective Forward Attack/Gray Hole Attack)
Malice Code Injection	Manipulation
Phishing	-
Authorization Attacks	-
False Data Attacks	-
MITM	-
Extra Interfaces Attacks	-
SCA	-
Spoofing	-

2.4 Security recommendation

By evaluating the attacks mentioned above, this chapter will present various mitigation methods. In conclusion, most attacks occur for specific reasons, such as a lack of encryption, mutual authentication methods, and secure data storage.

Meanwhile, many attacks are autonomous, which makes them more effective than classic attack methods. As a result, it is more difficult to mitigate attacks using traditional methods. Therefore, we believe that we should take advantage of the development of artificial intelligence (AI) to prevent and mitigate IoT attacks.

Blockchain

Many researchers suggest using blockchain to enhance the security of IoT [27][28][29][30]. The secure blockchain method is a high-impact process for IoT security using distributed and decentralized security for real-time data [31]. Blockchain benefits are demonstrated in securing data, enhancing authentication and integrity [30].

IoT communication in public areas can be secured by blockchain using public blockchain platforms. Public blockchain is a permissionless blockchain, where all parties are visible in the network. However, parties' privacy is secured by an anonymous identity policy [32]. Public blockchain platforms store encryption keys. When a device wants to send data it uses the receiver's public key from the blockchain to encrypt the messages, which the receiver decrypts with their private key [30]. Blockchain can additionally act as a public key infrastructure, which ensures consistent key management and secure communication between IoT devices.

Another research recommended using the DPA-PBFT (Dynamic Priority Agreement-Practical Byzantine Fault Tolerance) algorithm to secure data in terms of consensus problems between non-peer node. [33]

Artificial Intelligence -enhanced methods

AI-Driven Communication and Authentication enhances the security of communication and authentication in IoT environments by leveraging AI-powered technologies. These technologies help ensure secure interactions between IoT devices and protect sensitive data from cyber threats.

AI-Driven Cryptographic Techniques for Data Transmission utilizes artificial intelligence to improve cryptographic protocols and key management, ensuring secure and robust IoT device communication. AI algorithms optimize encryption processes, enhance key exchange mechanisms, and strengthen overall communication security in IoT systems. [34]

AI-Driven Data Management can be used for data classification, minimizing and access authorization. The employment of AI-powered data classification techniques facilitates organisations in evaluating the sensitivity and criticality of collected data. This, in turn, can be used to reduce unnecessary storage while ensuring the availability of high-quality, relevant data for IoT decision-making. Furthermore, fine-grained access control mechanisms, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), ensure that only authorized entities can access IoT data [36].

Real-Time Monitoring with AI enables real-time monitoring in IoT systems by analyzing network flows and system logs. Techniques such as attention-based models and Random Forest (RF) classifiers help detect abnormalities, while SHAP improves model interpretability [37].

AI-enhanced camera security can be used to secure IoT-connected cameras, implementing various AI-driven techniques such as face blurring algorithms to anonymize sensitive visual data, and end-to-end encryption to protect camera feeds from unauthorised access.

Machine Learning techniques can help detect and prevent various cyberattacks, including Denial-of-Service (DoS), eavesdropping, spoofing, and privacy leakage. [38]

Table 4 shows the security problems and the proposed technology. It also shows the key technology used for the purpose.

Table 4 Summary of security solutions

Problem	Proposed technology	Key technology
Consensus in non-peer IoT nodes	DPA-PBFT Algorithm	Dynamic Priority Agreement, Byzantine Fault Tolerance
Authentication	AI-powered biometrics authentication	AI cryptography
Lack of encryption, mutual authentication, and secure data storage.	Leverage AI for advanced prevention and mitigation of IoT attacks.	Artificial Intelligence (AI)
The increasing complexity of autonomous attacks	Use AI-driven communication, cryptographic, and authentication technologies to enhance security	AI-powered authentication, AI-driven cryptography
Low regulation of IoT devices for children	Enforce governance policies to mandate comprehensive testing before releasing IoT devices	Governance policies
IoT communication security in public areas	Use blockchain for secure communication, encryption key	Blockchain, Public Key Infrastructure (PKI)
Consensus issues in distributed IoT systems	Employ the DPA-PBFT algorithm for secure data consensus	DPA-PBFT algorithm
Data sensitivity and access control	Implement AI-based data classification and fine-grained access techniques	AI, RBAC, ABAC
Real-time anomaly detection and monitoring	Use AI models to monitor IoT systems and identify abnormalities	AI (Random Forest, SHAP)
Privacy concerns with IoT cameras	Apply Face Blurring algorithms and End-to-End Encryption to secure camera feeds	Face Blurring, Encryption
Various IoT attacks (e.g., DoS, spoofing)	Detect and mitigate attacks using ML-based techniques	Machine Learning (ML)

3 Smart Toy

Today's children are growing up surrounded by IoT. At the early age of 3-10, children interact directly with the Internet of Toys IoToys. These are devices connected to the internet which have high networking capability, processing, and reasoning. IoToys are similar to the rest of IoT devices and they are able to make real-time decisions [35].

The general properties of IoToys are pervasive, social-aspect, interactive, and connected [35]. Pervasive means that the toy follows the child wherever. The social aspect means that the IoToys should be able to form different ways of socializing, one-on-one conversation, one-many, and many-many. Interactive means that toys have sensors and respond to input. Connected IoToys are able to connect and communicate with other toys, services, and online platforms through Wi-Fi and/or Bluetooth.

There are many security concerns when it comes to children interacting with IoToys. Concerns are related to social aspect and technical aspects. Children at early ages do not have the ability to have a critical mind on things. Therefore, they will learn what they are told and will behave according to the instructions they are given. [36] found that children between the ages of 4-10 consider IoToys to be trustworthy. Therefore, when children were asked moral-related questions, their answers changed influenced by the smart toys. For instance, an experiment was done that showed how IoToys could influence children's morals, they were asked to ask the smart toy "my friend Cayla" the following:

- "Is it ok to tease another child",
- Cayla said "I think it's ok"
- "Not ok" In the beginning, the child replayed to Cayla

And asked Cayla again the same question

- "I think it's ok," Cayla said

Eventually, the child chose "OK" to tease another child. This demonstrates kids' attachment and trust to smart toys.

While children learn that friends can be trustworthy, it is hard to explain that "My friend Cayla" is occasionally not trustworthy. Children get attached to smart toys they are hanging out with most of the time. This relationship between a child and smart toys develops over time, and children consider

these toys the be their secret keepers, their inner thought listeners, and the model they are learning from. When a child gets attached to an IoToy, it is harder to be taken away from later. In 2017 Federal Internet Agency (Bundesnetzagentur) in Germany warned the parents of the privacy risk of the smart doll, Cayla. The warning led to the parents destroying Cayla [37]. Eventually, the German government banned My friend Cayla due the privacy concerns [38]. This type of panning can affect children's mental health due to their attachment to their smart friends.

IoToys works using voice recognition technology to recognize users' voices and start a conversation with the user. They contain sensors just like the rest of IoT devices that collect data from their environment and focus and speech recognition. This data is being recorded and analyzed in real-time, like many IoToys, For example, my friend Cayla is using the internet to find data that she can use as an answer to a question. Recorded data is being sent to the company to improve its services [39]. These data are being stored based on the data storage law in the country it is being used in.

3.1 Security concerns in smart toys

As was previously mentioned security concerns increase when the devices' users are children. Children are more prone to cyber-attacks. They can become victims of abuse and harassment due the bad security. Figure 4 below shows what kind of messages children can receive and obey from IoToys. Smart toys contain various components that if attacked sensitive data might be revealed. IoToys consist often of embedded cameras, microphone accelerometers, and pressure-detecting plate [40]. These components are meant to capture children’s environment without their awareness or consent, even parents don’t know about some of these components. For instance, FP’s smart Bear does not notify the parent about the cameras embedded in the toys nor does it notify to when it is on or off like other devices such as laptops. Next security concerns going to be presented based on true events.

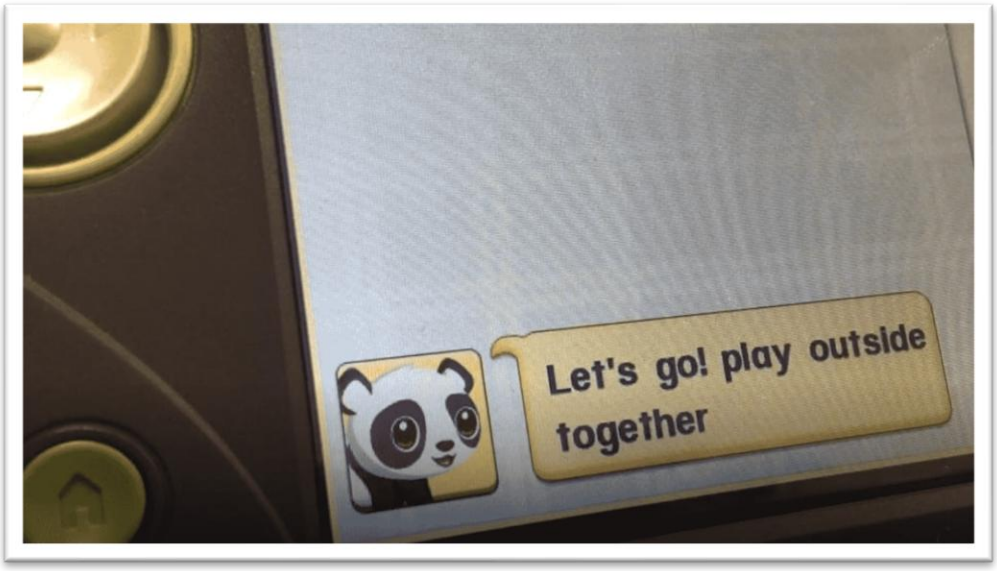

Figure 4 preset phrase on Pet Chat [41].

Security concerns

Unprotected network connection ports: In 2018, UI researchers found a method that enabled controlling the toy remotely by installing software if given a few minutes of access to the physical devices. [40]

Unsecured Bluetooth: In 2018, Amazon and eBay took off the CloudPets due to their vulnerabilities. However, these vulnerabilities were found in 2017, when millions of children's voice recordings were exposed online unprotected [42]. Additionally, researchers confirmed that CloudPets can be accessed by unauthorized users, which led to significant malicious activities [43].

Unsecured data: Vtech, a children's electronic learning product company, reported that 11.6 million accounts were compromised in a cyberattack, including 6.3 million children's accounts. Due to this event photos of children and parents, chat logs, and the children's names, genders, and birthdays were accessed by unauthorized parties. [39]

Lack of encryption: in 2016 researchers from a cybersecurity company named Rapid7 reported that data sent to the cloud was not encrypted, allowing malicious actors to access it [40]. Another case that proves the lack of encryption in many IoToys was in 2019, LeadFrog Leadpad. Researchers in Checkmarx had notified that these pads are supposed to be safe, they used basic HTTP protocol which stores data encrypted ""The first thing we found is that some of LeapFrog's communications aren't encrypted. It uses a very simple HTTP protocol, storing information in clear text and allowing an attacker to become a man-in-the-middle." [41][44].

Authentication & Authorization: Researchers found that My friend Cayla has an embedded microphone device that lacks any form of authentication. [40]

All previously mentioned cases demonstrate the failure to fulfill the security requirements.

3.2 Security recommendation for IoToys

We are going to go through different security recommendations specifically for IoToys.

Parental awareness and control

When it comes to educating parents, many questions can be raised. What parents need to know. Privacy is one of the most important concepts that parents should be fully aware of. Understanding privacy policies has been a problem for a long time, because of the vogue terms that are used to explain companies' privacy, research has shown that more than half of its participants in reading the privacy contract, they could not understand its contents [48]. It is therefore crucial to educate parents about the different terms and what they refer to. On the other hand, companies should be required to use terms that can be understood by users, not only experts. Terms such as "we may collect...", "personal information", "trusted third parties", "to improve our services", etc. do not give a clear picture of what exactly is being collected and what it means to improve our services, is the service the user is using or is the data being used to feed an AI model, for example.

Parents should also be aware of the embedded components in children's smart toys, which require in-depth research, as not all companies market all hidden components in IoToys, as mentioned earlier in this chapter. However, the problem should be addressed, and companies should market all embedded components and their performance, e.g. "This toy contains a camera that is ALWAYS ON".

Parents should also have full access to and control over smart toys. In the previous chapter, it was mentioned that UI researchers download software by accessing the physical devices for a few minutes. This can be prevented if parents can control the downloads and updates in the smart toys. In addition, smart toy components need to have on/off switches that allow parents to control the toy; if the toy is not being used, it can be turned off, or only the camera can be turned off.

Finally, parental awareness is a collaborative effort between producers and parents that enhances the quality of the IoToys experience.

Secure communication channel

It is recommended to take advantage of the revolutionary development in AI to secure communication channels. Such as AI leveraging encryption algorithms, real-time detection, and AI-powered mutual authentication.

Security certificate and Manufacturing plan

Another recommendation is that companies should obtain a special certificate before putting toys on the market. The controversy surrounding this certification lies in determining the minimum safety standards that each company must meet. The standards must be higher than for products intended for adults.

In addition, a clear manufacturing plan. Define specific goals for IoT toy production, whether the toys are intended for: Entertainment purposes, educational enhancement and skill-building for children, or supporting the development of children with special needs.

Data encryption and minimizing

It is recommended that companies encrypt all data, not only the firmware but also the massive amount of data generated by IoToys. The encryption standards must be robust enough to prevent unauthorized access and data breaches.

In addition, companies should implement data minimization practices. Define specific objectives for data collection and ensure that only the data necessary for the toy to function is collected. This approach not only enhances safety but also respects the privacy of children and their families.

4 Conclusion

This thesis provides a comprehensive exploration of the Internet of Things, beginning with an examination of its fundamental principles, including security requirements and architectural frameworks. Building on this foundation, it delves into the challenges of securing IoT environments and explores viable solutions to these problems. A focused analysis of IoToys provides practical insights into the complexities of implementing security measures in real-world scenarios. The thesis concludes by revisiting the central research questions and weaving the findings into a cohesive narrative that underscores the significance of the study.

The research literature is richer in some areas such as IoT security, but on the other hand, not much literature was found on IoToys.

RQ1: In Chapter 2 of this thesis, security requirements were analyzed to clarify the critical requirements for a system to be called "secure", security requirements are authorisation, confidentiality, integrity, availability, authentication. Security threats are represented by the failure to meet these requirements. When reviewing the threats in chapter two, it was observed that the network is the biggest target layer in the IoT. Attacks on the network layer are usually aimed at disrupting the system rather than exploiting the data. This means failing to meet availability requirements.

Key attack vectors include node capture, sniffing, false data injection, malicious code injection, jamming, phishing and various forms of denial-of-service attacks. Each of these attacks exploits specific weaknesses in the IoT architecture, whether through physical access or digital means. For example, node capture and side-channel attacks require physical access, while phishing and DDoS attacks are executed digitally.

By understanding the different attack vectors and their implications, stakeholders can better prepare and implement security measures to protect IoT systems, ensuring their reliability and integrity in an increasingly connected world.

RQ2: How are IoT architecture layers affected by the identified threats and issues?

The attacks were categorized into different layers as shown in Table 1, Section 2.3. According to the data collected, the most targeted layer is the network layer. However, any attack on any layer will result in incorrect performance of the IoT object.

IoT systems are inherently vulnerable to a wide range of attacks due to their interconnected and layered architecture. These vulnerabilities span multiple layers, including the sensor, network, middleware, and application layers. The interconnected nature of the IoT means that an attack on any one layer can have cascading effects, potentially causing significant damage.

(RQ3) IoT security vulnerabilities directly impact the safety of smart toys by exposing children to privacy risks, cyber threats, and psychological manipulation. Lack of or weak encryption and insecure connections could allow unauthorized access to sensitive data. It could also lead to inappropriate and manipulative interactions with children. Legislation, parental awareness, and improved security protocols are needed to mitigate these threats.

Future work

Forthcoming research should pinpoint its focus on the standardized security frameworks regarding IoToys, also considering the challenges arising from the topic that requires further analysis. Threat detection, decentralized security, blockchain, and AI capabilities are all areas that could have a significant impact and potential research starting points. Shifting from the more technological aspects, measures and considerations such as child-centric privacy, legal and ethical matters, security certification processes, and usability studies on parental controls represent significant areas for study. Improving investigations in these endeavours could enhance the security of smart toys and potentially have a significant impact on the broader IoT risk mitigation efforts, with a focus on vulnerability aspects by which children are affected.

5 Reference

[1] J. Andress. "Foundations of Information Security: A straightforward introduction". No Starch Press, 2019.

[2] S. Smith. "The Internet of Risky Things: Trusting the Devices That Surround Us". O'Reilly Media Inc., 2017.

[3] T. Rajmohan, P.H. Nguyen & N. Ferry. "A decade of research on patterns and architectures for IoT security." Cybersecurity 5, 2 (2022). https://doi.org/10.1186/s42400-021-00104-7 (accessed April 30, 2025).

[4] Statista. Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025. [Online]. Available: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/ (accessed March 1, 2025).

[5] M. Adam, M. Hammoudeh, R. Alrawashdeh, and B. Alsulaimy, “A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems,” IEEE Access, vol. 12, pp. 57128–57149, 2024, doi: 10.1109/ACCESS.2024.3382709.

[6] S. Li, Securing the Internet of Things. Saint Louis: Elsevier Science, 2017.

[7] Z. Wang et al., “A Survey on IoT-Enabled Home Automation Systems: Attacks and Defenses,” IEEE Commun. Surv. Tutor., vol. 24, no. 4, pp. 2292–2328, 2022, doi: 10.1109/COMST.2022.3201557.

[8] K. Abdul Sattar and A. Al-Omary, “A survey: security issues in IoT environment and IoT architecture,” in 3rd Smart Cities Symposium (SCS 2020), Online Conference: Institution of Engineering and Technology, 2021, pp. 96–102. doi: 10.1049/icp.2021.0894.

[9] S. J. Danbatta and A. Varol, “Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation,” in 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal: IEEE, Jun. 2019, pp. 1–5. doi: 10.1109/ISDFS.2019.8757472.

[10] M. Ahmid and O. Kazar, “A Comprehensive Review of the Internet of Things Security,” J. Appl. Secur. Res., vol. 18, no. 3, pp. 289–305, Jul. 2023, doi: 10.1080/19361610.2021.1962677.

[11] W. Fei, H. Ohno, and S. Sampalli, “A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions,” ACM Comput. Surv., vol. 56, no. 5, pp. 1–40, May 2024, doi: 10.1145/3625094.

[12] M. S. Rajan, J. R. Arunkumar, A. Ramasamy, and B. Sisay, “A comprehensive study of the Design and Security of the IoT layer Attacks,” in 2021 6th International Conference on

Communication and Electronics Systems (ICCES), Coimbatre, India: IEEE, Jul. 2021, pp. 538–543. doi: 10.1109/ICCES51350.2021.9489235.

[13] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, “Smart home security: challenges, issues and solutions at different IoT layers,” J. Supercomput., vol. 77, no. 12, pp. 14053–14089, Dec. 2021, doi: 10.1007/s11227-021-03825-1.

[14] R.A. Spinello. "Corporate Data Breaches: A Moral and Legal Analysis". Journal of Information Ethics, vol. 30, no. 1, pp. 12-32, 2021.

[15] LoginRadius, Marriott Data Breach 2020: 5.2 Millions Guest Identity Compromised. [Online]. Available: https://medium.com/@loginradius/marriott-data-breach-2020-5-2-millions-guest-identity-compromised-6247106dcc9b (accessed April 30, 2025).

[16] K. Khaliq, N. Z. Ab Rahim, K. Hamid, M. Ibrar, U. Ahmad, and M. U. Ullah, “Ransomware Attacks: Tools and Techniques for Detection,” in 2024 2nd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates: IEEE, Feb. 2024, pp. 1–5. doi: 10.1109/ICCR61006.2024.10532926.

[17] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, “Security and Privacy in Smart Farming: Challenges and Opportunities,” IEEE Access, vol. 8, pp. 34564–34584, 2020, doi: 10.1109/ACCESS.2020.2975142.

[18] M. Ahmid and O. Kazar, “A Comprehensive Review of the Internet of Things Security,” Journal of Applied Security Research, vol. 18, no. 3, pp. 289–305, Jul. 2023, doi: 10.1080/19361610.2021.1962677.

[19] Cloudflare, “Famous DDoS attacks: The largest DDoS attacks of all time.” [Online]. Available: https://www.cloudflare.com/en-gb/learning/ddos/famous-ddos-attacks/ (access April 30, 2025).

[20] A. Agiollo, M. Conti, P. Kaliyar, T.-N. Lin, and L. Pajola, “DETONAR: Detection of Routing Attacks in RPL-Based IoT,” IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1178–1190, Jun. 2021, doi: 10.1109/TNSM.2021.3075496

[21] M. Karthigha, L. Latha, and K. Sripriyan, “A Comprehensive Survey of Routing Attacks in Wireless Mobile Ad hoc Networks,” in 2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India: IEEE, Feb. 2020, pp. 396–402. doi: 10.1109/ICICT48043.2020.9112588.

[22] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, “A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis,” Sensors, vol. 20, no. 13, p. 3625, Jun. 2020, doi: 10.3390/s20133625.

[23] Z. T. K, M. E. M, and A. A.A, “Sybil Attack Detection In Wireless Sensor Networks,” in 2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT), Tashkent, Uzbekistan: IEEE, Oct. 2020, pp. 1–6. doi: 10.1109/AICT50176.2020.9368790.

[24] M. Adam, M. Hammoudeh, R. Alrawashdeh, and B. Alsulaimy, “A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems,” IEEE Access, vol. 12, pp. 57128–57149, 2024, doi: 10.1109/ACCESS.2024.3382709.

[25] S. Bansal and V. K. Tomar, “Challenges & Security Threats in IoT with Solution Architectures,” in 2022 2nd International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), Mathura, India: IEEE, Jan. 2022, pp. 1–5. doi: 10.1109/PARC52418.2022.9726660.

[26] A. Sharma and H. Babbar, "Preventing Spoofing Threats in IoT: Machine Learning Approaches for Intrusion Detection," 2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC), Gwalior, India, 2024, pp. 1267-1271, doi: 10.1109/AIC61668.2024.10730888.

[27] R. Salama et al., “Blockchain Technology and Artificial Intelligence’s Future Applications in Cyber Security,” in 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE), GHAZIABAD, India: IEEE, Nov. 2023, pp. 412–418. doi: 10.1109/AECE59614.2023.10428598.

[28] A. Dharani and S. M. Khaliq-ur-Rehman Raazi, “Integrating Blockchain with IoT for Mitigating Cyber Threat In Corporate Environment,” in 2022 Mohammad Ali Jinnah University International Conference on Computing (MAJICC), Karachi, Pakistan: IEEE, Oct. 2022, pp. 1–6. doi: 10.1109/MAJICC56935.2022.9994206.

[29] X. Wei, Y. Yan, S. Guo, X. Qiu, and F. Qi, “Secure Data Sharing: Blockchain-Enabled Data Access Control Framework for IoT,” IEEE Internet Things J., vol. 9, no. 11, pp. 8143–8153, Jun. 2022, doi: 10.1109/JIOT.2021.3111012.

[30] S. Vikas Reddy, “IoT Security Enhancement Using Blockchain,” in 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballari, India: IEEE, Apr. 2022, pp. 1–5. doi: 10.1109/ICDCECE53908.2022.9792693.

[31] N. A. Khan, A. Awang, and S. A. A. Karim, “Security in Internet of Things: A Review,” IEEE Access, vol. 10, pp. 104649–104670, 2022, doi: 10.1109/ACCESS.2022.3209355.

[32] A. A. Sadawi, M. S. Hassan, and M. Ndiaye, “A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges,” IEEE Access, vol. 9, pp. 54478–54497, 2021, doi: 10.1109/ACCESS.2021.3070555.

[33] D. Liao, H. Li, W. Wang, X. Wang, M. Zhang, and X. Chen, “Achieving IoT data security based blockchain,” Peer-to-peer networking and applications, vol. 14, no. 5, pp. 2694–2707, Sep. 2021, doi: 10.1007/s12083-020-01042-w.

[34] M. Humayun, N. Tariq, M. Alfayad, M. Zakwan, G. Alwakid, and M. Assiri, “Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey,” IEEE Access, vol. 12, pp. 25469–25490, 2024, doi: 10.1109/ACCESS.2024.3365634.

[35] A. Catala, C. Sylla, A. G. Ozgur, P. Ihamäki, and K. Heljakka, “Smart toys, smart tangibles, robots and other smart things for children,” in Proceedings of the 2020 ACM Interaction Design and Children Conference: Extended Abstracts, London United Kingdom: ACM, Jun. 2020, pp. 38–45. doi: 10.1145/3397617.3398061.

[36] R. Williams, C. V. Machado, S. Druga, C. Breazeal, and P. Maes, “‘My doll says it’s ok’: a study of children’s conformity to a talking doll,” in Proceedings of the 17th ACM Conference on Interaction Design and Children, Trondheim Norway: ACM, Jun. 2018, pp. 625–631. doi: 10.1145/3202185.3210788.

[37] BBC news, “German parents told to destroy Cayla dolls over hacking fears.” [Online]. Available: https://www.bbc.com/news/world-europe-39002142 (accessed April 30, 2025).

[38] S. S. Nelson, “Germany Bans ‘My Friend Cayla’ Doll Over Spying Concerns,” npr, 2017. [Online]. Available: https://www.npr.org/2017/02/20/516292295/germany-bans-my-friend-cayla-doll-over-spying-concerns (accessed April 30, 2025).

[39] E. Taylor and K. Michael, “Smart Toys that are the Stuff of Nightmares [Editorial],” IEEE Technology and Society Magazine, vol. 35, no. 1, pp. 8–10, Mar. 2016, doi: 10.1109/MTS.2016.2527078.

[40] J. Streiff, N. Noah, and S. Das, “A Call for a New Privacy & Security Regime for IoT Smart Toys,” in 2022 IEEE Conference on Dependable and Secure Computing (DSC), Edinburgh, United Kingdom: IEEE, Jun. 2022, pp. 1–8. doi: 10.1109/DSC54232.2022.9888910.

[41] D. Sopas, “LeapFrog LeapPad Ultimate Security Vulnerabilities.”, Checkmarx, 2019. [Online]. Available: https://checkmarx.com/blog/leappad-security-vulnerabilities/ (accessed April 30, 2025).

[42] BBC News. “Children’s messages in CloudPets data breach,” BBC, 2017. [Online]. Available: https://www.bbc.com/news/technology-39115001 (accessed April 30, 2025).

[43] BBC News. “Amazon and eBay pull CloudPets smart toys from sale,” BBC, 2018. [Online]. Available: https://www.bbc.com/news/technology-44382135 (accessed April 30, 2025).

[44] Responsive Technology Partners. “LeapPad Kids Tablet Found To Have Security Issues,” 2019. [Online]. Available: https://www.responsivetechnologypartners.com/2019/08/21/leappad-kids-tablet-found-to-hav (accessed April 30, 2025).