IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 11 April 2025, accepted 13 May 2025, date of publication 22 May 2025, date of current version 25 June 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3572626

SURVEY

AI-Enhanced Threat Intelligence in Remote Patient Monitoring Systems: A Survey on Recent Advances, Challenges and Future Research Directions

JOLLY TRIVEDI, MOHAMMAD TAHIR, (Senior Member, IEEE), AND JOUNI ISOAHO
Department of Computing, University of Turku, 20540 Turku, Finland
Corresponding author: Mohammad Tahir (tahir.mohammad@utu.fi)

ABSTRACT Modern healthcare is increasingly relying on Remote Patient Monitoring (RPM) systems, which continuously collect health data and provide the ability to monitor patients in real-time. RPM systems are extremely susceptible to cyber threats due to their growing reliance on interconnected devices and hence need comprehensive security. AI has emerged as a crucial technology for addressing security issues in RPM systems. The objective of this survey is to understand the impact on the security of RPM systems by integrating Artificial Intelligence (AI) with threat intelligence. This survey analyzed 86 research articles from leading databases related to AI models, security of RPM systems, anomaly detection, and architectural solutions, in addition to 24 articles related to existing RPMs. This survey article emphasizes that RPM systems become much more resilient when automated attack mitigation, real-time anomaly detection, and predictive analytics are provided by AI-powered models. To secure the sensitive data in RPM, this survey discusses how AI can be applied to various architectural solutions, including edge computing, cloud integration, blockchain technology, and Federated Learning (FL). Furthermore, the benefits and challenges of deploying AI-driven threat intelligence, cross-platform compatibility, and the need for explainable AI to improve trust in automatically made decisions are presented. Moreover, this review highlights research gaps, including the necessity of comprehensive end-to-end architectures for maintaining security and privacy in RPM systems. It is revealed through this survey that AI-powered threat intelligence enhances RPM security considerably due to its ability of continuous monitoring, adaptive defense mechanisms, and early detection of threats. However, challenges such as the explainability of AI models persist and necessitate continued innovation. The survey paper suggests integrating AI-enhanced threat Detection as a Service (TDaas) that implements FL to transform the existing RPM security system, and ultimately contributes to a secure and reliable threat detection system in healthcare. This review provides a roadmap for future research in the area of AI-driven threat intelligence security for RPM systems and offers insights for developing resilient healthcare infrastructure.

INDEX TERMS Remote patient monitoring (RPM), telemedicine, human digital twin (HDT), pseudonymization, security, privacy, cloud, artificial intelligence, cyber threat intelligence (CTI), HIPAA, GDPR, machine learning, federated learning, anomaly detection, threat detection, healthcare security, personalized healthcare.

I. INTRODUCTION

With the growing adoption of Remote Patient Monitoring (RPM) systems, it is possible for healthcare providers to continuously monitor patients in real-time, offering timely

The associate editor coordinating the review of this manuscript and approving it for publication was Shadi Alawneh.

involvements and reducing hospital re-admissions. RPM provides medical professionals with up-to-date patient vital sign data, medication compliance, and lifestyle decisions using a range of technological tools, such as wearables and mobile applications. Owing to the ability to receive personalized care and timely interventions, patients with chronic illnesses stand to benefit the most from this change in healthcare management, from reactive to proactive.

Healthcare businesses are desirable targets for cybercriminals to exploit infrastructure flaws because they employ cutting-edge technologies which may not be properly secured. Health data is highly sensitive and hence it is necessary to implement robust security measures. A breach of health data can result in identity theft, compromising patient safety and even leading to financial loss. The privacy of patient data is a priority in the healthcare sector. Unauthorized access to data and data breaches can result in potentially dangerous outcomes, such as privacy violations and threats to patient safety [1]. Consequently, it has become imperative to conduct research and development in the area of RPM system security.

Data encryption, secure transmission, and compliance with HIPAA and GDPR are some of the few challenges encountered by the present conventional methods used for threat detection. However, they are not adequate to address the evolving threat landscape encountered by EPM systems. Hence, there is a need to develop a secure, scalable, and interoperable architecture that addresses these challenges in addition to enhancing personalized healthcare delivery. Artificial Intelligence (AI) can revolutionize cybersecurity by enhancing threat intelligence. Threat intelligence driven by AI increases the accuracy and precision of RPM systems in detecting anomalies and assessing potential risks. It also aids in responding swiftly and efficiently to attacks. Machine learning (ML) algorithms enable AI models to analyze a large amount of patient data, device interactions, and network traffic, in addition to detecting anomalies that may cause a security breach.

A. MOTIVATION

Conventional cybersecurity measures have shortcomings in terms of securing RPM systems. As dependence on these systems increases, it is necessary to identify and mitigate the challenges of existing cybersecurity measures. Hence, robust security solutions are required that can predict, identify, and eliminate the potential security threats before they can cause harm. Recently, AI has been considered to be a robust solution to these concerns, and this revolutionizing threat intelligence in RPM Systems. In order to detect anomalies, predict potential new threats, and respond to security breaches, ML algorithms and Neural networks can play a vital role. This is a very important implementation in the healthcare industry, as it can detect anomalies and provide all necessary details about malicious activity in e-health telemonitoring systems [2]. These systems can improve their capabilities for threat detection, prevention, and response using anomaly detection techniques, ML algorithms, and natural language processing [3].

However, despite significant advancements in RPM systems, several critical gaps remain in the literature. Most of the literature on AI-driven threat intelligence focuses on general cybersecurity applications rather than specific healthcare contexts like RPM systems [4]. Strict laws such as the HIPAA and GDPR must be followed when integrating AI with threat intelligence in healthcare settings. However, existing literature often overlooks the nuances of these regulations in the context of AI-driven threat intelligence.

B. COMPARISON WITH EXISTING LITERATURE

In cybersecurity, AI is being applied to threat modeling, although there is a lack of generalization across domains and it has been discussed in various research work that there is a need for more research on automating threat modeling processes. AI and ML are also revolutionizing social media use in telehealth and RPM, improving data management and stakeholder relationships [5]. However, challenges remain, including privacy concerns, standardization of RPM systems, and addressing ethical issues in AI adoption [5], [6]. The current literature primarily focuses on organizational security rather than patient-centric approaches. Existing AI models often lack context-awareness specific to patient data and operational environments, leading to challenges in accurately differentiating between benign anomalies and genuine security threats.

Several articles have discussed the integration of AI into threat intelligence [7], but they often overlook the complexities involved in integrating AI solutions with existing RPM infrastructure [4], [8]. There is a need for research that specifically addresses the technical and operational challenges healthcare organizations face when implementing AI-driven threat intelligence solutions within their RPM systems. Real-time monitoring and response capabilities are necessary to mitigate the dynamic nature of cyber threats. AI has proven to be a crucial component of cybersecurity, offering real-time threat detection and prevention capabilities [9]. The existing literature lacks concrete examples specific to RPM systems despite the mention of the potential of AI in real-time analysis. The adoption of AI in RPM systems also requires addressing complexities of human-AI interaction, scalability, and accessibility obstacles [10]. Organizations should focus on developing robust cybersecurity strategies by establishing clear ethical guidelines and legal frameworks and promoting interdisciplinary collaboration to overcome these challenges [6], [11].

For effective threat intelligence, it is essential for human analysts and AI systems to collaborate. AI can elevate cyber threat intelligence (CTI) processing by automating tasks and providing real-time insights, although human expertise remains essential for high-fidelity intelligence [12]. However, most of the existing literature ignores the chal-

lenges associated with collaboration between humans and AI in complex healthcare environments. Threat intelligence solutions must be scalable and adaptable because healthcare environments evolve rapidly owing to advancements in technology. Existing literature rarely addresses these aspects comprehensively within the context of RPM systems. While traditional blockchain solutions offer improved security and privacy, they struggle with limited scalability [13]. In addition, the lack of proper interaction between patients and healthcare providers within RPM systems is a notable shortcoming [14].

The integration of AI in threat intelligence necessitates specialized skills and knowledge among cybersecurity professionals working in healthcare environments. To address the shortage of AI-trained cybersecurity professionals, some institutions have developed lab-intensive modules covering topics such as cyber threat intelligence, malware analysis, and classification [15]. AI-based cyber threat intelligence is particularly relevant in the banking sector, where it is being implemented to build resilient cyber-defense systems, although its adoption varies globally [16]. However, existing literature rarely discusses training programs tailored for professionals working within RPM contexts.

By addressing these gaps, this article aims to provide a comprehensive understanding of how AI can be leveraged to enhance threat intelligence, specifically within RPM systems, while ensuring compliance with healthcare regulations and prioritizing patient-centric approaches. This detailed analysis highlights both the existing literature on AI-driven threat intelligence and the gaps that need to be addressed in order to provide a comprehensive review focused on RPM systems. There is a lack of standardized metrics to evaluate the effectiveness of AI-enhanced threat intelligence in RPM systems across different use cases and threat landscapes.

C. RESEARCH QUESTIONS

The primary objective of this survey article is to investigate RPM systems that not only safeguard patient data but also enhance the personalization and effectiveness of remote healthcare services. To achieve this overarching goal, the following Research Questions (RQ) are outlined:

1) **RQ1:** What is the current status of research related to AI-driven RPM systems to enhance patient care?
2) **RQ2:**What are the various ways in which AI-automated threat intelligence can be implemented to improve security measures in RPM systems?
3) **RQ3:** What are current Applications of AI for Cybersecurity in RPM?
4) **RQ4:** What are the various methods of integration of AI with Threat Intelligence in RPM?

D. CONTRIBUTION

This survey contributes to the field of cybersecurity by demonstrating how AI can be harnessed to enhance threat intelligence practices, specifically within the context of RPM. In particular, the main contributions are as follows:

1) The paper provides a comprehensive overview of how AI is currently being utilized in RPM to enhance patient care and security. It highlights various applications such as automated threat detection, predictive analytics, and real-time monitoring, illustrating the transformative impact of AI on healthcare security.
2) Discussion on strategies for ensuring data privacy and mitigating biases in AI algorithms, contributing to responsible AI usage in sensitive environments like RPM.
3) The paper proposed the approach to integrate AI-based TDaas that implement FL for AI models for Anomaly Detection.
4) This review highlight the strengths and limitations of existing AI applications in RPM security, focusing on AI-driven threat intelligence.
5) The compliance requirements and challenges associated with implementing AI in RPM systems.
6) Challenges and future research directions associated with implementing a Secure AI-based RPM system.

E. ORGANIZATION OF PAPER

The rest of the survey article is organized as follows. Section II provides the background provides an overview of RPM systems, emphasizing their growing role in healthcare for real-time patient monitoring. Section III describes the systematic approach used to gather and analyze relevant literature. It includes details of the search strategy, selection criteria, data extraction, and analysis process. Section IV explores the current status of research based on the research question presented. In Section V, various AI techniques employed in threat intelligence are discussed, and how AI can be integrated with threat intelligence processes, including automated data collection, enhanced threat detection, intelligence sharing, and predictive analytics. Section II-D presents the findings on the integration of AI with threat intelligence in RPM. Section VI analyses the literature on AI-driven anomaly detection techniques in RPM. In Section II-D discussion on AI-enhanced threat intelligence for RPM systems is presented. Section VII outlines challenges and limitations, including advancements in AI algorithms, integration with new technologies, and addressing ethical considerations. The future research directions are outlined in Section VIII. Finally, Section IX presents the conclusions.

II. BACKGROUND

The rapid advancement of technology in healthcare has made it possible to use innovative solutions to enhance patient care and enable more efficient monitoring of health conditions. RPM has become a pivotal component of modern healthcare systems, especially for chronic disease management, elderly care, and post-operative follow-ups [17]. RPM leverages various technologies, including wearable devices, mobile

applications, and cloud computing to facilitate continuous health monitoring outside traditional clinical settings.

A. EVOLUTION OF RPM SYSTEMS

The concept of RPM has changed over the course of many years with the development of technology and increasing demand for effective healthcare delivery models. Initially, RPM systems were very simple and depended on telecommunications equipment to send vital health data of blood pressure and heart rate to medical professionals. Some of the major issues with these traditional RPM systems include, low quality of data, low scalability, and lack of ability for real-time monitoring.

With the introduction of wearable technology and IoT applications, the adoption of RPM systems has increased. Various wearable devices such as smartwatches, fitness trackers, and specialized medical equipment can be used to collect health data such as sleeping patterns, physical activity, and vital signs. The sensors in these gadgets continuously track the physiological parameters of the user and then send them to the central system for analysis. There is a rise in chronic diseases, such as cardiovascular diseases, diabetes, and respiratory disorders, which increases the need to change the approaches in healthcare from reactive to proactive. RPM helps in building this approach through timely interventions and individualized care plans by providing medical professionals with access to real-time data on the health metrics of patients. This data include glucose levels, heart rate, blood pressure, and physical activity. This change is especially necessary because of the increase in the aging population, and the preservation of their health and independence is of utmost importance. After the COVID-19 pandemic, there has been an increase in the adoption of RPM technology, as healthcare systems have looked for solutions to reduce in-person visits as well as maintain continuous patient care [18]. The integration of RPM into healthcare systems has aided in lowering healthcare costs and improving patient engagement and satisfaction by reducing hospital readmissions and emergency room (ER) visits.

RPM systems can handle large amounts of data generated by multiple devices and are more scalable because of the integration of cloud computing. Cloud platforms offer the infrastructure required for real-time data processing, storage, and analysis, empowering healthcare providers to make informed decisions based on current and accurate data. Thus, the evolution of RPM systems has been defined by a move from straightforward localized monitoring to intricate distributed systems that can offer patients complete round-the-clock care.

B. ROLE OF WEARABLE DEVICES IN RPM SYSTEMS

In RPM systems, wearable devices are the main source of data collection [19]. A wide range of physiological parameters, such as heart rate, blood pressure, glucose levels, and oxygen saturation, can be measured by the sensors in these devices. As sensor technology has advanced and battery technology has significantly improved, the reliability and usability of these devices have increased, contributing to their widespread adoption. Wearable technology has become indispensable to RPM because it gives patients the ability to actively participate in their care management and provides continuous monitoring capabilities. These devices collect massive amounts of data that can be analyzed to identify trends and inform medical decisions. Studies have shown that RPM aids in enhancing the standard of patient care, reducing expenses, and expediting diagnosis [17]. The ability of various systems and devices to successfully communicate and exchange data is known as interoperability, and is becoming increasingly important as wearable technologies proliferate.

C. UNIQUE CHALLENGES OF TRADITIONAL RPM SYSTEMS

RPM faces several unique challenges that hinder its full potential in healthcare. These include issues with data quality and management such as inaccuracies in wearable devices and difficulties in data interpretation [20]. Technical challenges include the lack of standardization, automation, and quality of service in RPM systems [21]. Some of the significant drawbacks reported by healthcare practitioners include patient anxiety, increased workload, and privacy concerns [22]. Moreover, there are concerns related to the integration of health data generated by patients with electronic medical records [20]. Other challenges include mobility issues, heterogeneous networks, and financial constraints [21], [22].

1) DATA ACCURACY AND RELIABILITY

RPM systems face several data accuracy and reliability challenges. These include issues with patient-generated health data (PGHD) quality, as patients collect data without supervision using non-certified devices [20]. The lack of PGHD integration with electronic medical records further complicates data management [20]. Patients may incorrectly use devices, leading to inaccurate readings. For example, improperly positioned sensors can result in faulty data. There can be periods of missing data due to patients not consistently using devices or technical issues such as poor Internet connectivity.

2) TECHNOLOGY AND INFRASTRUCTURE LIMITATIONS

RPM faces several technological and infrastructural challenges. These include issues with data collection, transmission, storage, analysis, and presentation [23]. Poor digital literacy among elderly patients and lack of technology interoperability with existing health systems are significant barriers [24]. Some patients, especially the elderly or those with limited technology literacy, may find it difficult to navigate RPM technology, leading to frustration or misuse. Since RPM relies on connectivity, the absence of broadband access in rural or underserved areas presents significant challenges in adoption. Since RPM heavily relies on stable

connectivity, sensitive health data transmitted online must be protected, making it essential to have strong encryption, which is not always guaranteed.

3) SECURITY AND PRIVACY CONCERNS

Security and privacy concerns are serious problems in data protection for healthcare industry, and the adoption of RPM systems introduces new challenges [25]. Health data breaches can have serious repercussions for patients and healthcare organizations because of their sensitive nature, making them prime targets for cyberattacks. Studies have shown that there has been a sharp rise in healthcare data breaches, resulting in monetary losses and a decline in patient confidence. It is crucial to incorporate security and privacy features into remote monitoring systems from the beginning of their design [26]. There are multiple security concerns regarding the implementation of proper cybersecurity measures for medical devices [27]. Due to inadequate security implementation and lack of familiarity, patient data is easily vulnerable to attackers. In addition, with current models, the number of users that can share a single RPM device is very limited [27]. Few other critical challenges include high workload for healthcare providers, insufficient funding, and lack of ethical considerations regarding patient autonomy and data privacy [24], [25]. These challenges need to be addressed in order to fully utilize RPM to enhance patient services and healthcare delivery. Patients worrying about the security and privacy of their health information may prevent them from interacting with the RPM to the fullest extent.

There is always a risk of interception if the transfer of RPM data between different systems is not sufficiently secure. While integrating RPM solutions with various platforms, such as health apps, EHR systems, and cloud services, it is challenging to ensure secure data exchange between these platforms and maintain patient privacy.

4) REGULATORY COMPLIANCE

RPM systems are required to comply with the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and the General Data Protection Regulation (GDPR) in Europe. Therefore, strict measures are required to safeguard personal health information as the penalties for non-compliance with these regulations can be severe. Additionally, it can be challenging to enforce these laws on all digital platforms. There are also certain geogrophical restrictions amidst which health data need to be stored locally in certain countries and cannot be exchanged with servers located outside the geogrophical boundaries. In healthcare setups, where providers use cloud services to store and exchange data in RPM systems, data handling is very difficult.

Adherence to these regulations is imperative to protect patient data and to maintain legal and ethical obligations. However, healthcare organizations, specifically Small and Medium Enterprises (SMEs), may find it difficult to comply with these regulations because of their budget and complexity. In order to maintain patient confidence in RPM systems, it is necessary to balance clinical utility with privacy concerns and mitigate ethical and legal risks to healthcare providers [28].

D. INTEGRATION OF AI WITH THREAT INTELLIGENCE IN RPM

With the integration of AI with threat intelligence, there is drastic change in the manner in which organizations implement cybersecurity. Natural language processing and advanced ML algorithms, AI has helped to automate and elevate various aspects of the threat intelligence lifecycle. This section discusses the areas where AI is being integrated with threat intelligence to enhance the accuracy and efficiency of cybersecurity measures deployed.

1) AUTOMATED DATA COLLECTION AND ANALYSIS

One of the key benefits of integrating threat intelligence with AI is the automation of data-collection and analysis processes. AI systems can scan vast amounts of data from many sources, including social media, threat alerts, and dark web forums, to locate relevant information about potential threats. AI systems can read textual inputs and extract pertinent information that may identify new attack vectors or threats due to natural language processing (NLP). Because this automated data collection and enrichment process keeps information accessible, security personnel may remain informed about the evolving threat landscape without becoming overwhelmed.

2) ENHANCED THREAT DETECTION AND RESPONSE

RPM systems produce large amounts of data consisting of real-time patient health information that needs to be processed, transmitted, and securely stored. As cyber threats constantly evolve, it can be difficult for traditional security measures like firewalls and intrusion detection systems to prevent them. AI-driven threat detection systems can analyze large datasets using machine learning and deep learning to identify patterns and anomalies that may indicate a security breach [29], [30]. Historical data can be used to train an AI model, which can help recognize typical system behavior and identify deviations that can predict or identify an attack. An AI system has the potential to identify anomalous surges in data traffic as well as distributed denial-of-service (DDoS) attacks. AI-driven threat detection continuously learns from data and adapts to new and unexpected threats, making it more successful in recognizing and mitigating security issues in RPM settings than traditional RPM systems.

The ability of AI systems to recognize patterns is used to improve threat detection and response systems in RPM. There are significant benefits of AI-driven approaches such as supervised, unsupervised, and reinforcement learning, in threat mitigation across various domains [31].

By analysing system logs, network traffic, user behaviour, and anomalies that may indicate the presence of a threat, AI algorithms can establish baselines of normal activity. AI-powered behavioral analytics is particularly effective at spotting advanced persistent threats (APTs) and insider threats that traditional security measures can overlook. AI systems can provide early warnings of potential threats by continuously comparing real-time activity with predefined baselines. This makes mitigation and proactive response strategies feasible. AI-based early warning systems improve situational awareness by analyzing data in real-time, aiding in the prompt detection of security events [32].

However, issues such as scarcity of qualified professionals, excessive implementation costs, and concerns regarding data security persist [29]. In addition, ethical considerations and the need for large labelled datasets pose further obstacles [30], [33]. Despite these challenges, it is crucial for organizations to integrate AI into cybersecurity to combat evolving threats effectively. Moreover, cross-disciplinary collaboration and ongoing research are necessary to unlock the full potential of AI in securing digital infrastructure [33], [34].

3) PREDICTIVE ANALYTICS AND THREAT HUNTING ASSISTANCE

AI facilitates a structured approach to threat hunting, allowing for the systematic detection of tactics, techniques, and procedures (TTP) used by attackers [35]. The analytical capabilities of AI go beyond detection and response to include predictive analytics and assistance with threat hunting. By analyzing historical threat data and new trends, AI can build predictive models that anticipate potential threats, attack routes, or weaknesses in the future. By leveraging past data to predict possible risks, AI algorithms, particularly ML and Distributed Learning, allow for analysis that goes beyond conventional detection techniques [36]. By adopting a proactive approach, organizations can mitigate the potential impact of cyberattacks and implement preventive measures to counter threats. AI can also assist human analysts in threat hunting by automating the initial stages of data analysis and quickly spotting potential compromise indicators and areas of concern.

Data from cyberattacks can be analyzed with the help of AI to identify trends and patterns that lead to potential new threats. Healthcare organizations can prepare for such incidents well in advance with the assistance of the predictive capability of AI. AI technologies can enhance present cybersecurity because of their ability to examine several aspects of emails and websites and detect phishing attempts [37]. AI is capable of analyzing data from a variety of sources, including user behavior, network traffic, and external threat feed, in the context of RPM systems in order to predict the potential location and mode of an attack. An AI system can notify administrators to improve email security procedures if it detects an increase in phishing attempts directed towards healthcare practitioners. By generating baseline profiles for user behaviors, AI can identify odd trends in network behavior that might point to phishing attempts [38]. This proactive approach to cybersecurity offers a substantial benefit in securing sensitive patient data in contrast to traditional systems that frequently react to threats after they have already caused damage. Even though AI greatly improves threat hunting and predictive analytics, there are still issues mostly related to the requirement for trained humans to understand AI results and the possibility that AI systems would fall behind quickly changing cyber threats.

4) AUTOMATED INCIDENT RESPONSE

In addition to detection and prediction, AI plays a vital role in automating the incident response in RPM systems. The speed at which cyber-attacks can compromise systems necessitates rapid and effective responses that are often difficult to achieve through manual intervention alone. AI enables automation of various aspects of the incident response process, ensuring prompt and well-coordinated actions to mitigate the effects of security breaches. Based on the detected threats, AI algorithms can suggest efficient responses, such as separating affected computers, installing security updates, or adding more monitoring. The efficiency is improved and the mean time to resolution (MTTR) is reduced by bypassing conventional procedures and automating the incident ticket assignment as well as the resolution [39].

With the smooth integration of AI algorithms into threat intelligence procedures, autonomous threat hunting has been considered as the critical methodology [40]. This technique offers proactive threat detection and prevention, not limiting only to reactive measures [41]. AI-driven models offer various solutions for identifying anomalies and suspicious activities, including the range from neural network-based threat identification to natural language processing [41]. An AI-driven system can automatically isolate affected devices, block suspicious IP addresses, or initiate data recovery processes, on detecting a potential threat. AI enables enhanced and efficient resource allocation by prioritizing incident response based on the seriousness of the threat. AI considerably minimizes the window of risk by reducing the time between the detection of a threat and response. As a result, it protects patient data and maintains the integrity of RPM systems.

5) CONTINUOUS LEARNING AND ADAPTATION

AI systems adapt their detection and response strategies over time because they constantly learn from new data and emerging threats. Because systems can incorporate new threat intelligence and modify their algorithms accordingly, this feature guarantees that AI-driven threat intelligence remains effective against evolving cyber threats.

6) SCALABILITY

Solutions with AI capabilities can readily expand to accommodate growing data and alert volumes. For RPM

systems, which could see variations in data flow as a result of changing patient populations and monitoring activities, this scalability is very helpful. AI can effectively handle these modifications without sacrificing functionality, thereby guaranteeing continuous security.

7) ENHANCED USER BEHAVIOR MONITORING

AI monitors and analyzes the user activity within RPM systems in order to identify anomalies from the normal behavior patterns. This capability is highly beneficial for identifying compromised accounts or insider threats. To improve the security of sensitive patient data, anomalous access or attempts to access unlawful data can trigger alerts for additional inquiries.

8) COST-EFFECTIVENESS

AI can lower the overall expenses related to cybersecurity events by automating routine security processes and enhancing threat detection capabilities. Healthcare companies can reduce the financial impact of breaches using AI-driven threat intelligence because of their early identification and automated responses.

9) COMPLIANCE WITH REGULATORY STANDARDS

Threat intelligence driven by AI can help healthcare firms stay in compliance with laws like GDPR and HIPAA. AI solutions make it easier to monitor and document activities necessary for regulatory compliance by offering comprehensive logs and reports on threat identification and response. This feature helps companies avoid potential fines for non-compliance legal duties.

10) ENHANCING USER AUTHENTICATION AND ACCESS CONTROL

Since sensitive data is involved in the RPM systems, user authentication, and access control are essential components. Phishing and brute-force attacks are more prevalent against vulnerable traditional authentication methods like passwords. AI can enhance these methods by implementing more sophisticated authentication techniques, including behavioral biometrics and continuous authentication [42]. AI solutions automate identity proofing and authorization tasks that traditionally require significant human intervention. This flexibility in access control reduces friction in the authentication process, making it easier for users to access the resources they need while maintaining high security. Organizations can handle large numbers of requests efficiently with the help of AI automation as this automation reduces the risk of errors and also increases the speed of verification of the identity [42].

Security of access control systems can be enhanced and the threats of unauthorized access and data breaches can also be lowered with AI and ML [43]. In order to continuously verify the identity of a user, AI algorithms can analyze patterns in user behavior like typing speed, device usage, and location data. AI-driven access management systems can handle large volumes of access requests efficiently, and hence beneficial to organizations of all sizes, especially those experiencing rapid growth [43]. Automation of access management processes helps minimize human errors that can lead to security vulnerabilities, ensuring a more reliable access control system.

AI systems can trigger additional security measures for authentication, such as multi-factor authentication or locking the account until the required verification is completed if the behavior that deviates significantly from the user's established pattern is detected [44]. This dynamic and adaptive approach to access control ensures that only authorized individuals can access sensitive patient data, thereby improving the overall security of the RPM systems.

E. THREAT MODEL OF RPM SYSTEMS

The threat model for existing RPM systems involves the identification of potential risks and vulnerabilities, the attack vectors that could compromise security, privacy, and data integrity as well as the mitigation strategies. This section discusses the threat model for traditional RPM systems. Figure 1 shows the possible security threats in traditional RPM systems and the corresponding AI-based solutions.

Multiple strategies must be employed in RPM systems to mitigate security threats. The implementation of multi-factor authentication (MFA) ensures device identity verification, which addresses spoofing. Tampering can be addressed by signing secure firmware and regular updates to prevent unauthorized changes. For preventing Man-in-the-Middle (MitM) attacks and information disclosure, encryption of data both at rest and in transit is very important. Healthcare providers should implement load balancing and intrusion detection systems (IDS) to protect against DoS attacks. Robust role-based access control (RBAC) and continuous security monitoring can help minimize the risk of privilege escalation and insider threats. The overall security posture of RPM systems can be improved through security awareness, regular security patches, vulnerability assessments, and by educating users about phishing and social engineering.

F. CURRENT CYBERSECURITY POSTURE OF RPM SYSTEMS

There have been notable cybersecurity incidents in the RPM system in the past. In 2020, a security breach in medical devices resulted in unapproved access to patient information. This incident compromised the privacy of patients and raised concerns about the vulnerabilities in the RPM systems and how they can be exposed [45]. Moreover, unauthorized access to data loss is a major security concern introduced by the incorporation of IoT technology in the healthcare sector [46]. Studies show that if a new technology is deployed without the required security standards, then there can be a high rise in vulnerabilities causing data leakages [47]. These hazards are highlighted by incidents such as the 2017 FDA recall of 465,000 pacemakers because of security issues [48].

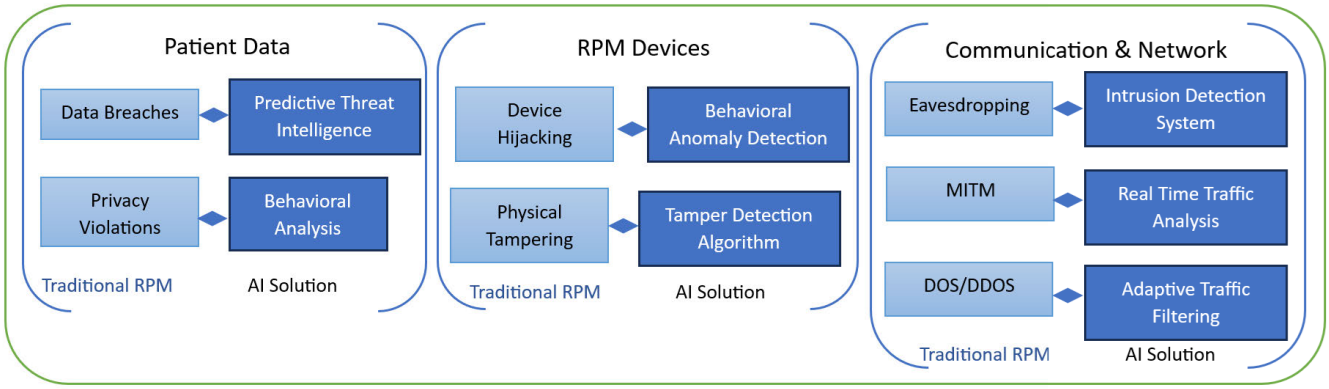

FIGURE 1. Security threats in traditional RPM systems and its AI-based solutions.

Significant financial and reputational harm has been caused by attacks such as WannaCry and ransomware attacks on a Los Angeles hospital in 2016 [49]. Security issues arise during data collection, transmission, and storage for Internet-of-Medical-Things (IoMT) systems, which allow remote patient monitoring [50].

During the COVID-19 pandemic, it was critical and urgent to address security problems in the deployment of RPM systems. According to a review, RPM technologies have made patient monitoring easier throughout the pandemic, but they have also raised new concerns regarding data security and privacy [51]. The necessity of implementing secure authentication techniques has been underscored owing to the susceptibility of current systems to multiple forms of attacks, such as impersonation and man-in-the-middle attacks [52]. In order to improve data integrity and security, this circumstance calls for the creation of more secure frameworks for RPM systems, such as those that use cutting-edge technologies like AI and BlockChain [53]. This article contributes to the analysis of the role of AI in enhancing threat detection for RPM systems.

G. THE ROLE OF AI IN ENHANCING THREAT INTELLIGENCE

AI is an invaluable tool for improving security protocols in several industries including healthcare. Cyber threat intelligence (CTI) is being revolutionized by AI, which is also improving cybersecurity defenses. AI-driven approaches perform noticeably better in terms of accuracy, identification of real-time threats, and adaptive response capabilities than conventional approaches [4]. AI-driven technology may evaluate enormous volumes of data, spot trends, and spot anomalies that could be signs of impending security issues in the context of RPM. Healthcare companies may better respond to cyber threats in real-time by proactively monitoring suspicious activity of their systems by integrating AI with threat intelligence. Applications such as intrusion detection systems (IDS), behavioral analysis, and predictive analytics are all included in the category of artificial intelligence-enhanced threat intelligence. Healthcare practitioners may anticipate and reduce the impact of evolving threats in addition to detecting known threats, using these technologies. From data intake to resilience verification, an AI-enhanced threat intelligence processing pipeline can help automate processes and work in tandem with human expertise to generate high-fidelity intelligence in a timely manner [7]. The demand for enhanced threat intelligence solutions in RPM systems is more than ever as cyber threats become more complex. Nonetheless, issues still exist, such as potential biases, ethical concerns, and the requirement for transparency in decisions made using AI [7].

III. METHODOLOGY FOR LITERATURE REVIEW

The purpose of this literature review is to synthesize existing research and knowledge regarding the integration of AI with threat intelligence in RPM systems. This section also outlines the methodology used to conduct the literature review, including the search strategy, selection criteria, data extraction, and analysis process. The detailed steps of the survey conducted in this study are illustrated in Figure 2.

A. SEARCH STRATEGY

To ensure a comprehensive review, a systematic search was conducted across multiple academic databases and repositories presented in Table 1.

The keywords and phrases that were used to formulate search queries include "AI-enhanced threat intelligence," "Remote Patient Monitoring," "Anomaly detection in healthcare," "Cybersecurity in healthcare," "Machine learning in RPM," "AI algorithms for threat detection." These keywords were combined using Boolean operators (AND, OR) to refine the search results and ensure relevance to the research topic.

B. SELECTION CRITERIA

Specific inclusion and exclusion criteria guided the selection of literature to ensure the relevance and quality of the studies included in the review:

TABLE 1. List of databases considered.

Database	Usage
PubMed	Research on AI utilization in RPM for enhancing patient care and security.
IEEE Xplore	Access to papers discussing AI techniques and cybersecurity measures relevant to RPM systems.
Google Scholar	Broad search for academic literature on AI-driven threat intelligence and its applications in healthcare.
ScienceDirect	Access to peer-reviewed journals covering AI, cybersecurity, and healthcare technologies.
ACM Digital Library	Research on AI methodologies and their implications for cybersecurity practices.
Web of Science	Comprehensive literature reviews on AI applications in RPM and related fields of study.

1) INCLUSION CRITERIA

- Relevance: Articles must focus on AI applications in threat intelligence, cybersecurity, or RPM systems.
- Publication Date: Studies published within the last ten years (January 2014 to August 2024) were prioritized to capture the most recent advancements in the field.
- Peer-Reviewed: Only peer-reviewed journal articles, conference papers, and reputable industry reports were included to ensure the credibility of the information.
- Language: Articles published in English were considered for inclusion.

2) EXCLUSION CRITERIA

- Non-Peer-Reviewed Sources: Articles that were not subjected to peer review, like blogs, were excluded.
- Irrelevant Topics: Studies that did not directly address AI, threat intelligence, or RPM systems were not considered for the review.
- Duplicate Studies: To avoid redundancy, any duplicate articles identified during the search were omitted.

To ensure a comprehensive understanding of the current landscape of AI-driven security threat intelligence, a rigorous literature review was conducted. A total of **175** articles were systematically evaluated, covering a range of sources, including peer-reviewed journals, conference proceedings, workshop reports, and other papers. The article selection procedure uses the PRISMA flow diagram shown in Figure 3, which outlines the search, inclusion, and exclusion criteria. The distribution of the articles is shown in Figure 4.

C. DATA EXTRACTION

Once the relevant literature was identified, key information was extracted from each selected study. The following data points were collected:

- Citation Information: Author(s), title, journal, publication year, and DOI.
- Study Objectives: The primary aims and research questions addressed in the study.
- Methodology: The research methods employed, including AI techniques used, data sources, and analysis approaches.
- Key Findings: Main results and conclusions relevant to AI-enhanced threat intelligence and RPM systems.
- Limitations: Any limitations noted by the authors that could impact the applicability of the findings.

D. THEMATIC ANALYSIS

The findings were synthesized into major themes:

- AI Techniques in RPM Security: This theme consolidates the various AI models and algorithms used in cybersecurity applications specific to RPM.
- Challenges in AI-based Threat Intelligence: Challenges like data privacy issues, AI model transparency (the ''closed box'' problem), and regulatory compliance were categorized.
- Benefits of AI: This theme addressed how AI improves threat detection, reduces manual labour, and enhances real-time responses.
- Future Research Directions: Identified gaps in the current literature were highlighted to propose potential areas for further study.

IV. STATUS OF THE RESEARCH

This section reviews the current state of the research presented in the literature related to the RQs presented in the paper.

A. RQ1

There is an increased demand for the implementation of artificial intelligence in RPM systems to improve patient care and system security. AI technologies have been extremely important for RPM systems due to their ability to monitor vital signs for chronic diseases, detect irregularities, and enable forecasting the medical issues. This has helped healthcare experts react swiftly to patient health issues, thus enhancing patient treatment. AI-driven RPM systems play a critical role in transforming healthcare by enhancing patient care and operational efficiency [6], [54]. These systems utilize wearable devices, sensors, and advanced technologies such as cloud computing and blockchains to monitor patients remotely and reduce hospital visits and associated costs [6]. Large amounts of patient data is analyzed to identify patterns and anomalies, detect early health deterioration, and personalize monitoring [6]. AI in RPM offers benefits such as reduced costs through optimized hospitalization and complication prevention [55]. It also enables elderly individuals to live independently by simplifying medical diagnosis and monitoring [56]. Table 2 displays the most relevant research related to RQ1.

The literature gap concerning the current status of research related to AI-driven RPM systems, particularly in enhancing

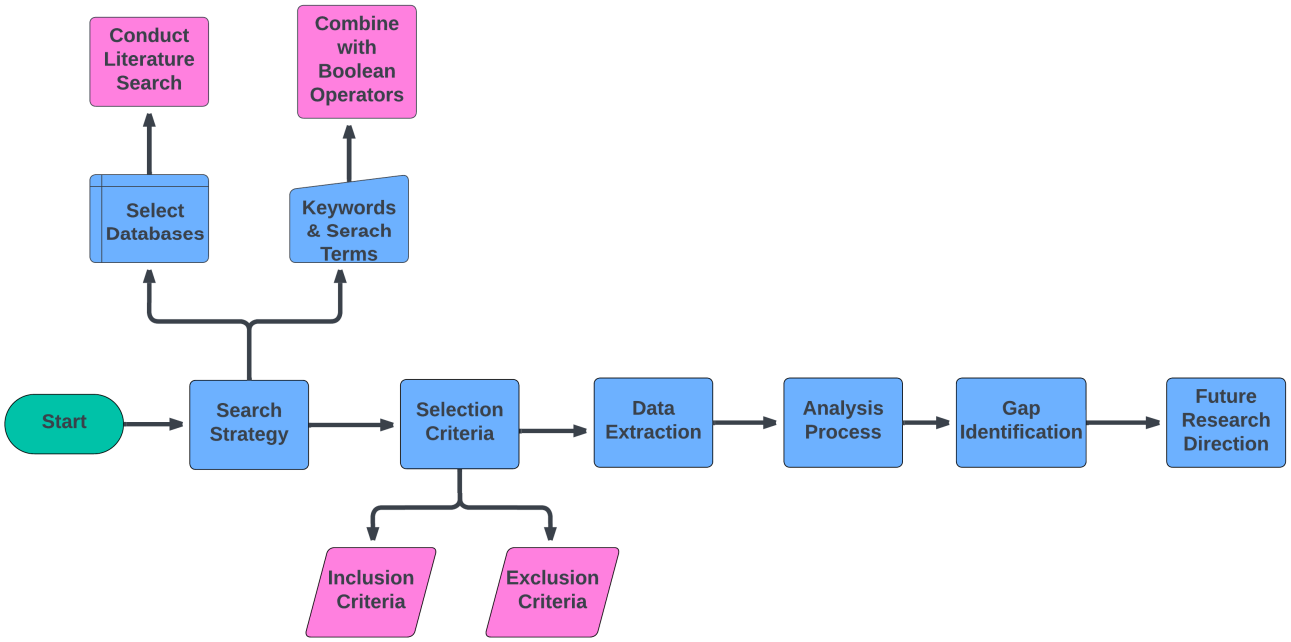

FIGURE 2. Search process.

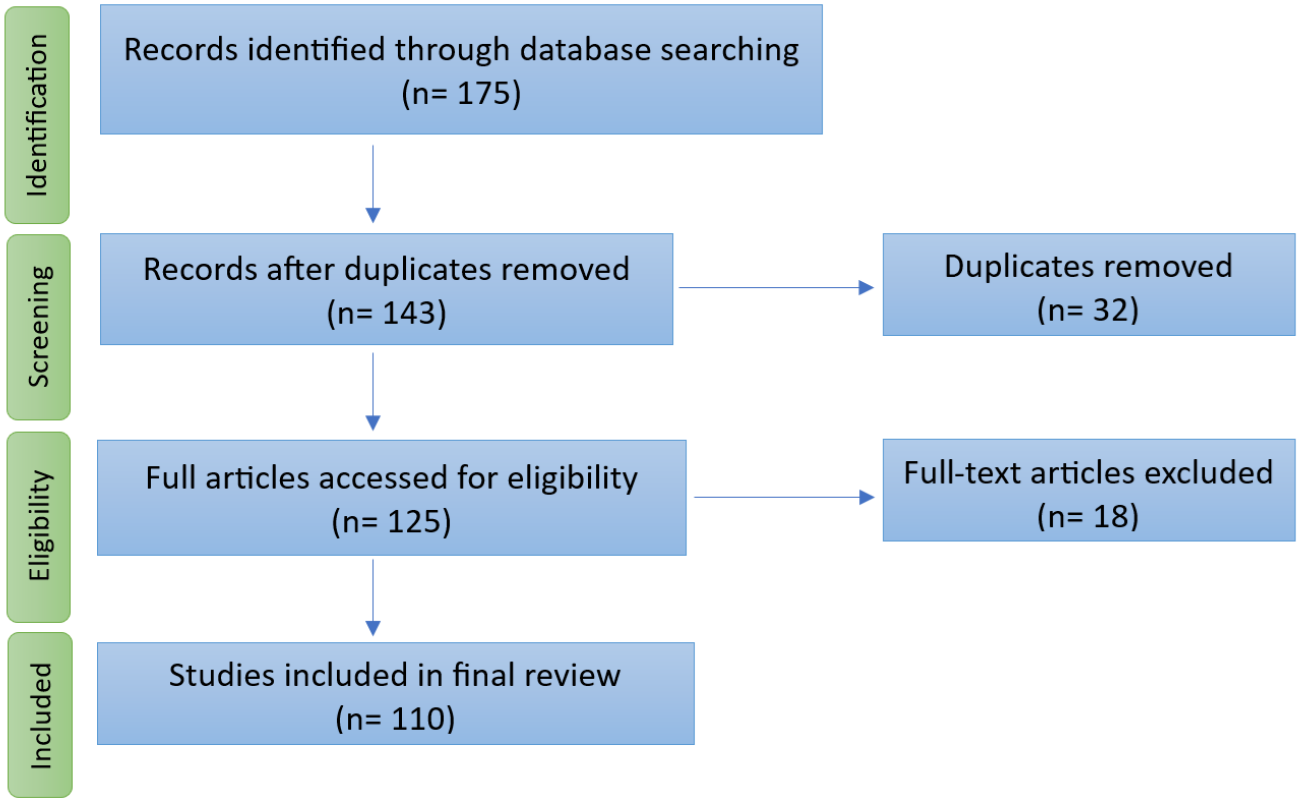

FIGURE 3. PRISMA flow diagram.

patient care, lies in several key areas that remain underexplored or insufficiently developed. This study shows that there are still many gaps in the practical integration of AI in RPM systems. AI has proven its potential for specific medical

TABLE 2. Key literature discussing the current status of research related to AI in threat intelligence.

Articles	Summary
Pulimamidi et al. [54]	This paper examines the transformative effects of AI on Remote Patient Monitoring Systems (RPMS) and highlights how AI enhances patient care, early intervention capabilities, and operational efficiency. It emphasizes the potential of AI-driven technologies to revolutionize healthcare delivery, particularly in the context of increasing reliance on remote monitoring.
Shaik et al. [6]	The article discusses how RPM using AI improves healthcare by enabling activity recognition and continuous vital signs monitoring early detection of health deterioration. It discusses the integration of AI with IoT devices to provide real-time insights and support clinical decision-making for improved patient care
Dubey et al. [55]	They discuss the US healthcare market, where AI-based RPM devices primarily focus on cardiovascular monitoring and arrhythmia detection
Malaviya et al. [56]	Mentions about how AI in telemedicine is improving medical diagnosis, simplifying remote monitoring, and revolutionizing senior care by enabling independent living
Ravikumar et al. [57]	An overview of the state-of-the-art in RPM with IoT is provided in this article. It also highlights its potential to save time, lower healthcare costs, and upgrade service quality and patient quality of life.

TABLE 3. Literature gaps in research related to AI in threat intelligence.

Literature Gap	Description
Limited Focus on Specific Patient Populations	Lack of targeted research on specific groups (e.g., chronic illness, elderly).
Integration Challenges with Existing Healthcare Systems	Insufficient exploration of interoperability issues with current workflows.
Data Privacy and Security Concerns	Inadequate frameworks for ensuring data security in AI-driven RPM systems.
Real-World Implementation and Case Studies	Scarcity of empirical evidence from practical applications of AI in RPM.
Longitudinal Impact Studies	Lack of studies assessing long-term effects of AI-driven RPM on patient outcomes.
User Engagement and Behavioral Insights	Limited research on how patient behavior affects the effectiveness of AI interventions.
Ethical Considerations and Bias in AI Algorithms	Insufficient exploration of algorithmic bias and ethical implications in healthcare settings.
Scalability and Cost-Effectiveness	Need for studies evaluating the scalability and economic viability of AI-driven RPM solutions.
Emerging Technologies and Future Directions	Current research may not capture emerging trends in AI and IoT integration with RPM systems.
Ethical and Regulatory Considerations	Research exploring the ethical, legal, and regulatory challenges of integrating AI into RPM systems is still nascent.

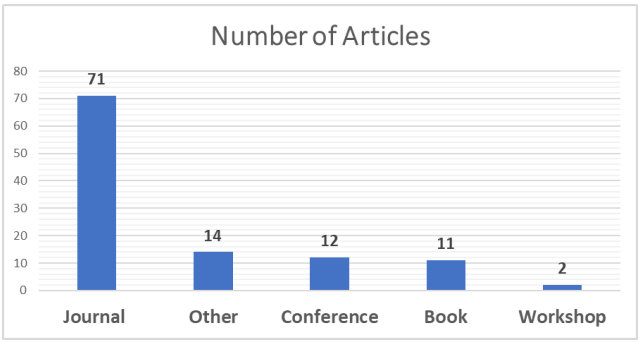

FIGURE 4. Number of articles studied.

issues such as cardiovascular disease and diabetes. However, there is a lack of comprehensive AI-driven RPM solutions for more complicated scenarios in healthcare, as presented in Table 3.

Although there is promising research on AI-driven RPM systems, there is a lack of large-scale real-world implementations, holistic integration across diverse health data, longitudinal studies on patient outcomes, ethical and regulatory explorations, and solutions tailored to diverse patient populations. Addressing these gaps is essential to fully realize the potential of AI to enhance patient care through RPM systems.

B. RQ2

AI-driven threat intelligence offers promising solutions for enhancing cybersecurity in various domains, including RPM systems. AI can detect anomalies and pattern through constant monitoring. To detect patterns and anomalies indicative of cyberattacks, AI-enabled systems can analyze large amounts of data and, as a result, provide automated and continuous improvement in threat detection and response [8]. In RPM, AI transforms healthcare monitoring by enabling early detection of health deterioration and personalized patient monitoring [6]. AI-driven security solutions can strengthen defenses by incorporating behavioral analysis, automated response mechanisms, and dynamic threat detection [58]. Small and medium-sized enterprises (SMEs) are particularly susceptible to advanced security attacks; hence,

TABLE 4. Literature related to AI integration for security.

Articles	Summary
Sankaram et al. [4]	The research highlights the tremendous superiority of AI-driven methodologies over conventional methods regarding the accuracy, real-time threat identification, and capabilities of adaptive response
Rangaraju et al. [58]	It draws attention to the observable benefits of using AI-centric security measures, such as increased resilience to new cyber threats, faster reaction times, and better threat detection accuracy.
Saddi et al. [60]	Generative AI can give enterprises an extra line of defense against more complex threats by combining vital and intriguing data items that might have otherwise gone unnoticed.
Dutta et al. [61]	This paper has addressed the use of threat intelligence for enhancing cyber security.
Sills et al. [62]	The authors describe a system that gathers Cyber Threat Intelligence (CTI) from manufacturers and ICS-CERT vulnerability reports about a variety of medical equipment and their known vulnerabilities.
Gupta et al. [63]	This study offers a convincing justification for important AI methods that identify cyberattacks and how data analysis can be used to provide guidance to various businesses and Internet-connected equipment.

TABLE 5. Literature Gaps related to AI integration for security.

Literature Gap	Description
Limited Implementation of Advanced Threat Detection	AI research mainly focuses on anomaly detection; lacks advanced predictive analytics and proactive threat detection in RPM.
Integration with Existing Security Frameworks	Research lacks studies on how AI can work alongside traditional security measures like MFA, encryption, and blockchain in RPM.
FL for Privacy-Preserving Security	Studies on FL for secure, decentralized AI model training across RPM systems are underdeveloped.
AI Adaptability to Dynamic Threat Landscapes	Insufficient research on AI's ability to dynamically update or retrain to combat evolving cyber threats in RPM.
Explainability and Trust in AI Security Decisions	Lack of focus on explainable AI to ensure healthcare providers trust automated threat intelligence decisions.
Scalability in Large-Scale RPM Deployments	Current research does not address the scalability of AI models for large RPM ecosystems involving numerous devices.
Resource Constraints and AI Efficiency	Insufficient research on optimizing AI models to function effectively on resource-constrained RPM devices with limited power.
Long-term effectiveness and Adaptability	Insufficient research on the long-term adaptability of AI-driven threat intelligence to evolving cyber threats within RPM systems.

they must adopt AI-based Cyber Threat Intelligence (CTI). It is critical to address challenges like knowledge gaps and lack of expertise to improve the cybersecurity posture [59]. AI can also be utilized for performing behavioral analytics that monitor the interaction between the RPM systems and patients in real time and detect the unusual behavior of patients, software, and medical devices.

Although AI-driven threat intelligence has enormous potential, there are still research gaps. For example, FL has not been explored to its full potential in RPM systems. FL is a new AI technology that processes across several devices without exchanging raw data and thus helps elevate RPM security. Overall, AI-powered security solutions provide more accurate threat detection, lowering the time to respond and improving the ability to respond to new cyber threats across industries. Table 4 lists the key literature related to RQ2.

The research gap related to the various ways to implement AI automated threat intelligence for enhancing security measures in RPM systems encompasses several underdeveloped areas, as listed in Table 5.

Addressing these gaps in the literature will provide valuable insights into the current status of research related to implementing AI-automated threat intelligence in RPM systems. By focusing on these areas, future studies can contribute to more effective security measures that enhance patient care, while ensuring data privacy and ethical considerations.

C. RQ3

Recent research have proposed innovative architectures for securing RPM and other IoT systems using AI-based threat intelligence. Uddin et al. [64] present a tier-based architecture with a patient-centric agent managing a blockchain component for privacy preservation. Ammi et al. [65] suggested a cloud-native architecture that enhances cyber-threat intelligence by connecting security-related data from diverse sources. SafaeiSisakht et al. [66] presented an architecture for an SDN-based IoT infrastructure that was automated in two phases and included AI-based threat detection algorithms and feature selection. Moustafa et al. [67] provided a threat intelligence scheme for Industry 4.0, which combines a threat intelligence module employing beta-mixture-hidden Markov models with a smart management module to handle heterogeneous data sources. These architectures address key challenges in securing complex, data-driven systems by leveraging AI, blockchain, cloud technologies, and advanced data processing techniques to enhance threat detection and

privacy protection in interconnected environments. A few of the proposed solutions are further discussed in the subsequent section.

D. PRESENT SOLUTIONS

1) FEDERATED LEARNING (FL) BASED SOLUTION

FL has become an effective technique for protecting privacy in IoT network security and enhancing threat intelligence. FedCTI uses FL to share Cyber Threat Intelligence (CTI) in an IoT environment in a secure and private manner [68]. Intrusion detection systems based on FL offer benefits for maintaining privacy and facilitating cooperation between entities that are unable to directly share datasets [69]. The FL framework encompasses horizontal, vertical, and transfer learning approaches, addressing challenges of data isolation and privacy in AI [70]. Differential privacy and homomorphic encryption are combined in a decentralized approach to threat intelligence with FL to safeguard sensitive data and facilitate cooperative model training. With its emphasis on collaboration, privacy protection, and fortifying collective defense against cyberattacks, this approach presents a bright future for cyber security [71].

2) BLOCKCHAIN BASED SOLUTION

Recent studies have explored blockchain-based architectures to secure RPM systems with AI integration. Zaabar et al. [72] propose a Hyperledger Fabric-based architecture to enhance data security and privacy in RPM. Singh et al. [73] present BlockIoTIntelligence, combining blockchain and AI for efficient IoT data analysis. Hathaliya et al. [74] talk about a controlled blockchain-based architecture for healthcare, along with the security challenges and integration of ML. Ashraf and Reaz [75] provided a comprehensive IoT-blockchain framework for RPM, addressing centralization issues and integrating best practices. These studies demonstrate how blockchain technology can enhance data confidentiality, integrity, and traceability in RPM systems [72], [75]. The integration of AI and blockchain technology into IoT architectures elevates security features and data analysis capabilities [73], [74]. Overall, these architectures propose the creation of more secure, efficient, and privacy-aware RPM systems.

3) CLOUD-BASED ARCHITECTURE IMPLEMENTING HUMAN DIGITAL TWIN (HDT) AND OPC UA

The authors in [76] addressed the challenges in RPM through the integration of OPC UA for secure and standardized communication, pseudonymization for better privacy, and Human Digital Twin (HDT) technology for advanced data processing and predictive modeling. By addressing the significant shortcomings of the present RPM systems, this all-encompassing strategy aims to improve the development of secure, effective, and personalized remote healthcare solutions. This work lays the groundwork for future healthcare technology research and development by addressing the gaps in the literature. There is much room for further research into the integration of the OPC UA and HDTs into RPM systems. This type of RPM system, which addresses important issues of patient privacy and data security, marks a revolutionary breakthrough in individualized healthcare. Integrating FL in healthcare wearable devices as well as at the edge of HDT can greatly help in improving the Threat Detection system.

4) CLOUD-EDGE HYBRID ARCHITECTURE

Recent research has explored cloud-edge hybrid architectures for securing RPM with an AI-based threat intelligence. Edge computing strategies have been proposed to enhance RPM security by processing data in the proximity of the source, thereby offering lower latency and improved privacy [77]. RPM devices use edge computing for data management and cloud computing for AI-assisted decision-making resulting in a unified edge-cloud computing architecture [78]. An osmotic cloud-edge AI microservice architecture enables flexible migration of training tasks between edge and cloud, optimizing resource utilization and prediction accuracy [79]. Additionally, a cloud-native architecture leveraging semantic technologies is suggested to improve data interconnectedness for cyber threat intelligence in cloud environments [65]. These approaches aim to address security challenges in RPM systems while maintaining efficient data processing and analysis, utilizing the strengths of both cloud and edge computing paradigms.

While AI holds immense potential to revolutionize the security landscape for healthcare systems, several areas within architectural design remain underdeveloped or inadequately explored. The existing body of literature often focuses on isolated solutions but lacks comprehensive end-to-end approaches that fully integrate AI into RPM systems for real-time, scalable, and secure operations. Table 6 highlights the key research gaps in architectural solutions for securing RPM with AI-based threat intelligence.

In conclusion, while AI-based threat intelligence offers significant promise for RPM systems, current research lacks focus on fully integrated, scalable, and cross-compatible architectural solutions. Future studies need to explore how AI models, FL, edge computing, and blockchain can be woven together to create a more secure, adaptable, and robust architecture for RPM systems. Addressing these gaps is critical to maintaining the integrity and enhancing the security of sensitive healthcare data in modern RPM environments.

E. RQ4

Cybersecurity can benefit significantly from AI-driven threat intelligence. To detect patterns and anomalies indicative of cyber-attacks, a plethora of data from various resources is automatically analyzed [8]. Although the system continuously learns and improves, security teams can focus on strategic tasks due to this automation [8]. AI-powered solutions aid in identifying and responding to sophisticated threats in real-time, thus improving the effectiveness and the efficiency of

TABLE 6. Literature gaps related to architecture solutions.

Research Gap	Description
Lack of Comprehensive End-to-End Architectures	Few studies propose holistic architectures combining AI-driven threat detection, response mechanisms, and secure communication across RPM systems. Most focus on isolated AI components.
FL for Distributed Security	Limited exploration of FL to create distributed security solutions for RPM systems. Research lacks focus on privacy-preserving decentralized AI model training across patient data.
Edge Computing and AI Integration	Sparse research on how edge computing can be combined with AI to offer real-time, low-latency threat intelligence in RPM systems using IoT and wearable devices.
Blockchain for AI-Based RPM Security	Insufficient exploration of combining blockchain with AI models to ensure data integrity and secure, verifiable data exchanges in RPM systems.
Cloud-Based AI Threat Intelligence	Research gaps exist in understanding how cloud-based architectures can fully integrate AI-driven security models, focusing on scalability, latency, and cost for RPM systems.
AI-Based Architectures for Real-Time Processing	Few studies address how to design architectures supporting real-time AI-based threat detection and response without delaying critical RPM system processes.
Cross-platform interoperability	Limited research on AI architectures that ensure seamless cross-platform integration and interoperability across diverse RPM devices and ecosystems.
Data Privacy and Security Protocols	While some studies touch upon security measures, there is a lack of comprehensive guidelines on data privacy and security protocols specific to AI-enhanced RPM systems
User-centric design Considerations	Limited research focus on the user interface and experience in AI-driven threat intelligence systems for RPM, which affects usability and adoption by healthcare professionals.
Long-Term Effectiveness of AI Architectures	Current literature lacks longitudinal studies that assess the long-term effectiveness and adaptability of AI-driven threat intelligence architectures in evolving cyber threat landscapes.

cyber defense [80]. For small and medium-sized enterprises (SMEs), adopting AI-based cybersecurity can help defend against advanced threats despite limited resources [59]. The ''Secure by Intelligence'' paradigm integrates AI-driven security measures into products, leveraging deep learning, ML, and anomaly detection to proactively predict, detect, and respond to potential threats [58]. This helps in elevating threat detection accuracy, lowering response times, and improving adaptability to emerging cyber threats across various industries [58]. Table 7 summarizes the benefits of implementing AI in Threat Intelligence.

AI-driven threat intelligence presents both opportunities and challenges for cybersecurity. Autonomous threat hunting has emerged as a crucial paradigm that integrates AI algorithms to enhance cyber defense mechanisms [40]. However, ethical concerns arise, including issues of privacy intrusion, explainability, bias, and political security [81]. An AI-enhanced cyber threat intelligence processing pipeline offers potential solutions, automating tasks from data ingestion to resilience verification, while emphasizing the importance of human-AI collaboration [12]. There are many challenges in examining adversary tactics, techniques, and procedures (TTP) and identifying Indicators of Compromise (IOC) [82]. The integration of AI in threat intelligence necessitates addressing ethical dilemmas and potential biases and ensuring transparency in AI-driven decisions [12]. Despite these challenges, AI-driven threat intelligence has significant potential for advancing cybersecurity defenses against evolving threats [40]. Table 8 presents the challenges related to the implementation of AI in Threat Intelligence.

V. CURRENT APPLICATIONS OF AI FOR CYBERSECURITY IN RPM

The use of AI in RPM systems is growing in order to improve cybersecurity. AI-based RPM solutions dominate the US healthcare industry for cardiovascular monitoring (74.2%) and ECG-based arrhythmia detection (59.4%) [55]. Vulnerability assessments, manual security log analysis, and external threat feeds are the key components of traditional RPM threat intelligence methodologies. These methods require considerable time and labour, and healthcare industry usually have a limited capacity to identify sophisticated and changing threats. Automation of data processing, pattern recognition, and attack prediction are some of the ways that AI-enhanced threat intelligence provides a more effective and efficient solution. AI-based solutions help enhance the RPM systems by facilitating early intervention and elevating the standard of care by analyzing large amounts of patient data to identify abnormalities, trends, and possible problems [54]. These systems assist in diagnosing health vitals remotely, as demonstrated by successful applications like Dozee.ai and Qure.ai during the COVID-19 pandemic [94].

1) **Anomaly Detection:** AI algorithms can analyze large volumes of RPM data to identify deviations from normal patterns. This can help detect anomalies that include data breaches, unauthorized access, or malicious activities. AI-based threat intelligence in RPM offers promising applications for anomaly detection. Hidden Markov Models have shown over 98% accuracy in identifying anomalous user behaviour in RPM systems using IoMT and smart home devices [95].

TABLE 7. Literature discussing benefits of AI in threat intelligence.

Articles	Summary
Rangaraju et al. [58]	AI-driven security solutions can increase the resilience and security of products by detecting threats more accurately, responding more quickly, and being able to adapt to new and emerging cyber threats.
Thapaliya et al. [83]	To improve cybersecurity, AI provides cutting-edge capabilities in threat identification, anomaly detection, and reaction automation.
Jawaid et al. [84]	Threat identification, vulnerability management, and compliance can all be improved by AI, which strengthens cyber security defenses.
Rachit et al. [85]	Through the automation of identification, analysis, and reaction, AI-driven cybersecurity solutions can enhance the defense of networks and computer systems against cyberattacks.
Caldren et al. [86]	Though they come with hazards that must be weighed, AI and ML can improve the detection rate of cybersecurity tools.
Olabanji et al. [87]	Traditional techniques of threat identification in cloud security are somewhat more accurate than AI-driven user behavior analysis, but AI-driven methods offer stronger predictive capabilities.

TABLE 8. Literature discussing challenges of AI in threat intelligence.

Articles	Summary
Caldwell et al. [88]	Security measures powered by AI encounter difficulties with accountability, transparency, and dependability as well as moral issues like bias.
Familoni et al. [89]	The difficulties of AI-driven cybersecurity are covered in the study, along with the necessity of an extensive risk management system and sophisticated assaults and algorithmic biases.
Oseni et al. [90]	Threat identification, vulnerability management, and compliance can all be improved by AI, which strengthens cyber security defenses.
Yupeng et al. [91]	Throughout their lifespan, AI-driven systems are susceptible to a various security risks, necessitating the development of solutions.
Susanto et al. [92]	The difficulties of implementing AI-driven security measures to secure government agency data and systems are covered in the study.
Alzboon et al. [93]	The article explains that in order for businesses to use AI responsibly and profitably, they must create cybersecurity solutions that are reliable and ethical in addition to being effective at thwarting threats while maintaining openness and trust.

A novel AI-based remote monitoring system for wireless sensor networks achieved 98.2% prediction accuracy and 97.3% precision in detecting anomalies [96].

2) **Threat Prediction:** Future attacks and vulnerabilities can be predicted by training AI models on historical threat data. This enables proactive security measures to be implemented before incidents occur. Ardito et al. [2] discussed cybersecurity threats by employing AI-based cyberattack-detection systems (CADS) that can detect anomalies, explain malicious activities, and display suspected attack data for healthcare monitoring.
3) **Vulnerability Assessment:** AI can automate vulnerability scanning and assessment processes, identifying weaknesses in RPM systems that attackers could exploit. By leveraging AI for continuous monitoring, healthcare organizations can proactively address vulnerabilities before they escalate into serious security incidents [97]. Secure data sharing among healthcare providers can be enabled using AI in threat intelligence for RPM. Sensitive patient data can be shielded from unauthorized access using AI by creating secure communication channels. This is especially crucial in telemedicine because a large amount of data is frequently transmitted over networks that may be vulnerable to cyberattacks [31].
4) **Incident Response:** Tasks such as identifying the root cause of an attack, containing the damage, and implementing remediation measures can be automated with AI and thus help improve the incident response. As AI can evaluate a plethora of data in real time, the speed and precision of incident detection are greatly increased, which is beneficial in emergency scenarios. [98]. Predictive analytics aided by AI can also be used to forecast patient outcomes using past data and present health parameters. This predictive ability is especially helpful for RPMs as it can help with timely interventions and better chronic illness management by identifying possible dangers [99].
5) **Phishing Detection:** To detect and prevent phishing attacks targeting RPM users, AI can analyze email content, sender behavior, and other factors. The detection of phishing attempts has been significantly enhanced by the use of Natural Language Processing (NLP) techniques within AI frameworks. NLP can analyze email and message textual content to identify malicious intent such as odd demands for sensitive information or suspect language patterns [100], [101]. This feature is especially important for RPM systems because most communications take place over email or messaging apps, which leaves them vulnerable to phishing scams [102].

VI. AI-DRIVEN ANOMALY DETECTION IN REMOTE PATIENT MONITORING SYSTEMS

The integration of AI-based threat intelligence has considerably elevated anomaly detection within RPM systems, thus enhancing RPM cybersecurity. In order to shield sensitive health data collected remotely, from being exposed to cyber threats, these systems require robust security measures. AI anomaly detection capabilities offer an efficient solution for identifying and mitigating security vulnerabilities in RPM systems by leveraging sophisticated algorithms and real-time data analysis. One of the existing works discussed that AI-based event and anomaly detection (EAD) identifies the issues earlier and enables timely interventions as well as minimizes the false alarms, which results in the enhancement of patient outcomes [103]. Advanced techniques, including deep learning and meta-heuristic optimization, enhance the precision of anomaly detection in ECG signals [11].

The first step in developing AI-based threat intelligence is to create a baseline model for the typical RPM system behavior. In order to comprehend normal patterns of patient data flows, device interactions, user behaviors, and network traffic, historical data must be analyzed. To recognize these regular patterns and characterize typical operating behavior, ML algorithms are utilized, such as clustering techniques or statistical methods. Every person, device, and data flow has a unique behavioral profile created by AI systems. The system focuses on aspects such as user interactions with the RPM system, access times, and typical patterns of patient data transmission. Any departures from these standard characteristics are marked as possible anomalies.

In order to create AI models for anomaly detection and health monitoring while safeguarding patient data, RPM systems use FL. AI models are trained in FL, across multiple devices or locations. One of the biggest advantages of using FL in RPM systems is that the data of patients remain on their devices and only model updates are sent to a central server for aggregation. In federated learning, the global model is updated by aggregating the updates from multiple local models trained on decentralized data. This can typically be represented by the following equation referring to the methods discussed by McMohan et al. [104].

$$\mathrm{w}^{t} + 1 = w^{t} - \mathrm{r}\Delta L(w^{t})$$

- w^{t}: Model weights at iteration t.
- r: Learning rate.
- N: Total number of participating devices.
- L(wt): Gradient of the loss function for a device with respect to model weights w^{t}.

This equation shows how the global model is updated by weighted contributions from all devices.

In RPM, anomaly detection frameworks such as Isolation Forests can be mathematically represented as:

$$S(x) = 2^{\frac{-Eh(x)}{c(n)}}$$

where S(x) is the anomaly score for a given data point x, $Eh(x)$ is the average path length from the root to x, and $c(n)$ is a normalization factor based on the number of samples. This approach allows for the identification of unusual patterns that may indicate cybersecurity threats or malfunctions in monitoring devices [105].

A dynamic thresholding approach can be implemented based on historical trends in the patient data. This can be modeled as:

$$T = \mu + k$$

In this equation, T is the dynamic threshold, μ is the mean anomaly score from historical data, k is a constant that adjusts sensitivity (e.g., $k = 2$ for 95% confidence), is the standard deviation of the anomaly scores.

The AI models continuously monitor for deviations from the expected behavior, such as unusual data traffic or unauthorized access attempts. These detections happen locally on each RPM device. The model updates from various RPM devices around the healthcare system are combined by the central server, which is hosted as part of the proposed AI-based TDaaS platform. Without gaining access to the underlying data, it averages and aggregates the changes. The combined model continues to improve as it gets the updated models from different devices. This global model is then re-distributed to the RPM devices for enhanced threat detection. This method assists in distinguishing between acceptable behavioral variances and possible threats. AI-based TDaaS benefits from FL because AI models can improve over time without compromising data security. Figure 5 illustrates how AI can help in anomaly detection and improve threat detection systems.

Transport Layer Security (TLS) or End-to-End Encryption can be implemented for communication between RPM devices and the central server. Model updates should be encrypted before the model sending to the cloud, to ensure security during transmission. AI-based models in a TDaaS framework can help to analyze patient data in real time and promptly detect anomalies or malicious activities. The continuous monitoring of network traffic and device interactions increases the ability of the system to respond proactively to ever-changing threats. The AI-based system triggers automated security responses by isolating compromised devices or alerting administrators and ensuring rapid threat mitigation.

A. MACHINE LEARNING ALGORITHMS

Healthcare organizations are using ML techniques in great numbers for anomaly detection in RPMs. These systems employ various sensors and wearable devices to continuously monitor patients' health status [106], [107]. These AI-driven systems enable early detection of health issues, improving the efficiency of healthcare services, particularly for remote patients, elderly individuals, and those with chronic conditions [106], [108]. The capabilities of RPM systems are elevated by integrating IoT devices and cloud computing with ML algorithms [106], [108]. Supervised learning algorithms, such as support vector machines (SVMs), decision trees, and

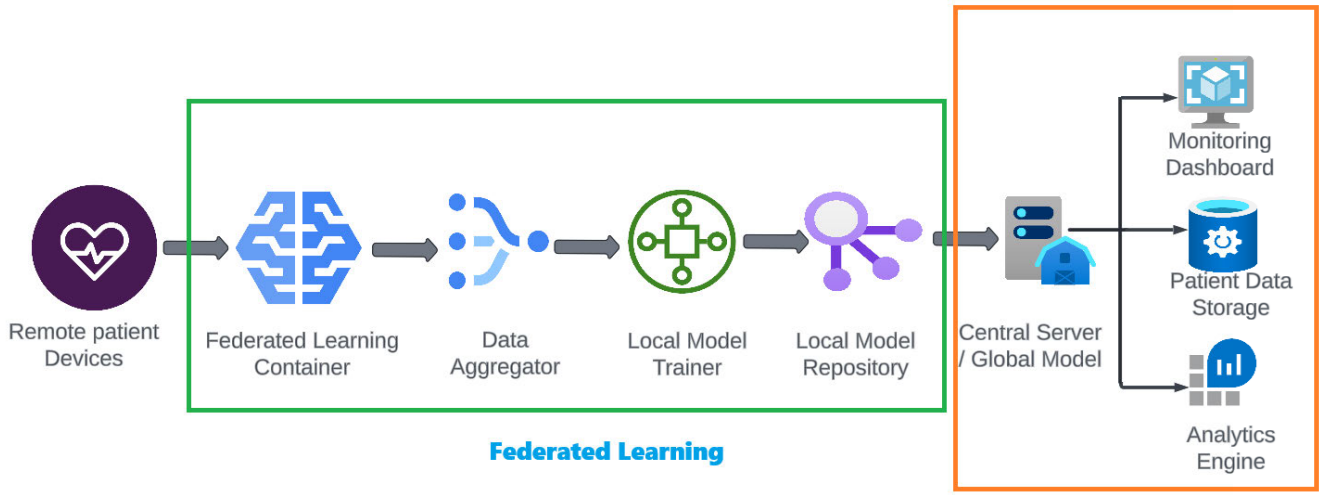

FIGURE 5. AI-Driven Threat Detection As A Service (TDaas) in RPM systems.

neural networks, are used in situations where labeled data are available. Examples of both normal and abnormal behaviour are included in the datasets for training these algorithms. After training, the AI model can classify fresh data points according to the patterns they have learned and identify potential security breaches. Unsupervised learning methods, such as clustering and anomaly detection algorithms, are implemented when the data is not labeled. These methods can help to detect departures from regular patterns without the need for prior labeling. By comparing the observed behavior to the learned behavior, unsupervised methods search for patterns in the data and detect anomalies.

Advanced deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), can be used for complex anomaly detecting applications. These models are very efficient in identifying anomalies and complex patterns in parallel with handling data from patient healthcare devices. They can detect subtle variations that conventional approaches can miss. For identifying anomalies in the cellular network key performance metrics, Recurrent convolutional neural networks (R-CNNs), which combine CNNs and RNNs, have been considered to be successful [109].

Homomorphic Encryption (HE) helps not only in anomaly detection in RPM systems but also aids preserving data privacy. One of the biggest advantage of this technique is that it allows computations to be performed directly on encrypted data without decrypting it. This property enhances privacy preservation in Remote Patient Monitoring (RPM) systems, where sensitive data must be processed while ensuring confidentiality. Patient health data, such as blood pressure, heart rate, and temperature, are encrypted at the source (RPM devices) using an encryption function Enc:

$$c = Enc(x, p_k)$$

Here, x is plaintext data (e.g., patient health readings), p_k is public key used for encryption and c is encrypted data (ciphertext). This ensures that the sensitive patient data is never exposed in plaintext during transmission or processing. Machine learning algorithms can be applied directly to the encrypted data.

B. REDUCING ALERT FATIGUE

The enormous amount of notifications produced by conventional security systems frequently results in alert fatigue for security staff. AI can help prioritize alerts based on severity and potential impact and ensures that serious anomalies receive rapid attention while filtering out less significant warnings. This prioritization helps healthcare organizations focus their resources on dealing with actual problems.

C. REAL-TIME MONITORING AND ANALYSIS

AI systems provide real-time data processing and continuous monitoring of RPM systems. AI systems continuously evaluate data streams to identify abnormalities as they occur, in contrast to traditional methods that rely on sporadic scans or manual checks. By ensuring that any risks are quickly discovered and dealt with, this real-time capacity reduces the window of opportunity for attackers. The system can modify its thresholds to consider changes in typical behavior patterns, for instance, and thereby lower the probability of false positives while retaining sensitivity to novel dangers.

D. AUTOMATED INCIDENT RESPONSE

When AI systems identify anomalies, they can initiate automated response measures to mitigate dangers. For example, the system alerts cybersecurity staff, immediately isolates a compromised device and restricts suspicious network connections. By assuring a prompt response to anomalies, AI lowers the impact of possible intrusions. AI systems

aid in prioritizing the alerts based on their criticality and possible risks associated. AI assists cybersecurity teams in resource allocation optimally based on the seriousness of the threats and potential hazards linked with each anomaly. AI-powered threat intelligence provides advanced functionality for real-time monitoring, spotting deviation from expected behavior, and automated incident response, all of which greatly improve anomaly detection in RPM systems and hence are very crucial. AI systems use continuous learning and contextual analysis to facilitate optimized means for identifying and reducing security risks in RPM environments. Healthcare organizations can strengthen patient data security and guarantee the reliability of remote monitoring systems by utilizing these capabilities.

VII. CHALLENGES AND LIMITATIONS

There are benefits and drawbacks to using AI-driven security measures in RPM systems. Although AI enhances threat detection, automation, and response capabilities [58], it also introduces new vulnerabilities and ethical concerns [88]. The complexity of AI algorithms raises issues of transparency, reliability, and potential biases [88]. A strong defense mechanism is necessary because adversarial attacks against AI models can significantly affect their performance [90]. For the integration of AI in cybersecurity, a multifaceted approach is needed that incorporates threat intelligence, ethical considerations, and adaptive defenses [89]. For effective AI-driven security, privacy-preserving solutions and cross-industry applications are very much essential [58]. For ensuring accountability and compliance, regulatory frameworks and industry standards play a vital role [89]. Ongoing research focuses on developing resilient AI models, comprehending adversarial objectives, and creating adaptive defenses to address these challenges [90]. Interdisciplinary collaboration and cybersecurity education are essential for navigating the evolving threat landscape [89].

To develop effective AI models, a large volume of high-quality data is required, but these may not always be available in healthcare facilities. Moreover, the high requirement for computational resources to run advanced AI algorithms can prevent their use in smaller healthcare institutions. The use of AI in RPM systems can also raise ethical and privacy concerns. Some key essentials for maintaining trust and safeguarding patient privacy are ensuring that AI systems are unbiased, transparent, and compliant with healthcare regulations such as HIPAA. Moreover, there is a need for human supervision in critical situations where there is the possibility of autonomous decision-making by AI systems raises concerns about responsibility.

A. DATA AVAILABILITY AND QUALITY

For AI-based threat intelligence, large datasets are critical for AI models to learn and generate accurate predictions. In RPM systems, there are often high-quality datasets available for training AI models. RPM systems produce enormous volumes of data related to health, but cybersecurity data comprising attempted breach logs, malware signatures, and known attack vectors may not be easily available in sufficient quantities for AI training. Furthermore, due to privacy and competitive concerns, threat intelligence information is not shared among healthcare organizations. In order to identify new risks accurately and generalize well, large and diversified datasets are necessary for AI algorithms. Moreover, biased AI outputs can produce false positives or negatives in threat detection.

B. HIGH COMPUTATIONAL AND RESOURCE DEMANDS

It takes a lot of processing power to train AI models for cybersecurity applications, particularly for real-time threat intelligence. A significant amount of processing power, memory, and storage is required to analyze massive amounts of data, spot abnormalities in real-time, and find patterns using AI systems such as deep learning neural networks or sophisticated ML algorithms. Due to the possibility of resource constraints, healthcare organizations, especially those with smaller staff sizes or less sophisticated IT systems, may find it difficult to deploy and manage AI-based threat intelligence systems.

Cloud-based AI systems can mitigate this problem by contracting out computing tasks, however, cloud environments itself raise issues related to data security and legal needs. For healthcare companies, striking a balance between the infrastructure that is currently in place and the requirement for strong AI-driven cybersecurity can be rather challenging.

C. AI INTERPRETABILITY AND EXPLAINABILITY

AI algorithms, specifically deep learning models, are often known as "closed boxes" because of the difficulty in understanding how they arrive at specific decisions. In the case of AI-based threat intelligence in RPM systems, this lack of transparency can pose serious concerns. Healthcare administrators and cybersecurity professionals need to trust the AI system's decisions, especially in critical scenarios where data breaches or unauthorized access to patient data are detected.

The inability to explain how an AI model identifies threats or prioritizes security risks can lead to distrust in the system. Ensuring that security activities comply with regulations such as HIPAA is critical in the healthcare industry. Hence, interpretability must be considered while designing a complex AI model, not ignoring the need to make it explainable. In reality, it is difficult to make complex models explainable while retaining their accuracy.

D. FALSE POSITIVES AND FALSE NEGATIVES

When the regular activity is identified as a threat, it is termed a false positive, and a false negative is the act of not identifying the real threat. For AI-based threat intelligence in RPM systems, the issue of false positives and false negatives can be challenging. There could be serious consequences for both in the healthcare industry. False positives can disrupt RPM servicesby harming patient care and raising concerns among

medical professionals. On the other hand, false negatives, in which a security threat is overlooked, can result in data breaches, compromising the privacy and safety of patients. Sensitivity and specificity must be balanced, particularly in dynamic scenarios such as RPM. A highly sensitive system may identify every anomaly and overwhelm cybersecurity analyst with alerts. While a less sensitive system might ignore serious threats. Improving AI models to minimize false positives and negatives is an ongoing research in AI-driven cybersecurity.

E. HUMAN SUPERVISION

Human supervision is still necessary despite the capabilities of AI. Although AI can automate repetitive operations and provide insights, human analysts are still required to evaluate findings, interpret AI-generated insights, and make strategic decisions. Reliance on AI in the absence of sufficient human input can result in erroneous interpretations and failure to recognize serious risks.

F. ETHICAL CONCERNS AND PRIVACY RISKS

The application of AI in cybersecurity also raises important moral and privacy issues. Patient data protection is the main objective of RPM systems; nevertheless, there may be situations where using AI for cybersecurity puts patient privacy at risk. Large datasets are necessary for AI systems to function, and in the healthcare industry, this includes personal health information (PHI). Even if AI is being used to protect this data, using AI algorithms themselves may unintentionally reveal sensitive data, particularly when processing, sharing, or aggregating data in external systems like cloud platforms. Concerns exist around the moral application of AI in decision-making as well. For example, an AI model may inadvertently deny genuine users access to vital patient data or services if it automatically denies access to some users based on behavioral patterns that it considers questionable. It is a significant issue to ensure that AI systems provide efficient cybersecurity solutions while upholding ethical norms, minimizing bias, and protecting patient privacy.

G. REGULATORY AND COMPLIANCE ISSUES

AI for cybersecurity in RPM systems must be implemented in accordance with a number of legal and compliance requirements, including HIPAA. Careful and continuous planning is necessary to ensure that AI systems retain effective cybersecurity while complying with compliance requirements. These laws impose strict guidelines for the collection, storage, analysis, and security of patient data.

As AI-based threat intelligence systems frequently handle enormous volumes of sensitive data, they need to ensure that these laws are followed. Integrating AI with cloud services that store or handle patient data across legal boundaries can be specifically challenging. To guarantee that AI systems improve cybersecurity in addition to adherence to regulations, meticulous planning is needed.

H. INTEGRATION WITH EXISTING SYSTEMS

Seamless integration of AI technologies with the current healthcare infrastructure to develop AI-based threat intelligence is challenging. Electronic health records (EHRs), network security, and handling of patient data are all managed by the majority of healthcare institutions. Integrating AI into this mix without impacting system performance or disrupting workflow, in general, is challenging.

It is necessary to upgrade or replace the legacy systems if modern AI solutions might be incompatible with legacy systems. Moreover, AI systems must work in tandem with human cybersecurity specialists. This will enable a smooth flow of information between AI-driven automation and manual intervention resulting in a successful defense mechanism for RPM systems.

I. EVOLVING NATURE OF CYBER THREATS

The rapid growth of cyber threats has made AI-based cybersecurity in RPM more challenging. Cybercriminals constantly breach security with innovative strategies, such as ransomware, phishing schemes, and complex malware that can trick even sophisticated AI models. Hence, to identify and block novel threats, AI systems need to be updated and retrained regularly. It takes ongoing investment in research, development, and threat intelligence to keep AI systems updated to handle new types of threats, which can put pressure on the healthcare resources of the organization.

J. TRAINING AND SKILL DEVELOPMENT

The cybersecurity workforce must continuously acquire specialized skills and expertise owing to the incorporation of AI in threat intelligence. Companies that want to guarantee that their employees can use AI technologies and understand the insights produced by AI must invest in training programs. This problem is exacerbated by the lack of qualified experts in cybersecurity and AI. Several other limitations and challenges are presented in Table 9.

VIII. FUTURE RESEARCH DIRECTIONS

As the integration of AI into RPM systems for cybersecurity evolves, several key areas require further research and development to enhance the effectiveness of AI-powered threat intelligence. This section outlines potential future research directions.

A. IMPORTANCE OF NATURAL LANGUAGE PROCESSING (NLP) AND FL

The majority of threat intelligence obtained using AI depends on anomaly and pattern identification. However, future research should focus on developing context-aware AI models that can recognize the larger picture of anomalies and distinguish between dangerous deviations and benign variations caused by patient-specific causes or environmental factors. These models could combine real-time monitoring with techniques like natural language processing (NLP) and

TABLE 9. And challenges of AI based threat intelligence in RPM systems.

Limitations and Challenges	Description
Data Privacy and Security Risks	Sensitive health data in RPM systems highly vulnerable to breach risks, especially if AI models are compromised by adversarial attacks or insufficient encryption [110].
Adversarial Attacks	AI algorithms can be manipulated by Malicious actors to evade detection, creating false negatives in threat identification.
False Positives and Alert Fatigue	Overloaded healthcare staff may ignore critical alerts due to AI-generated false alarms, undermining trust in the system [110].
Interoperability Challenges	Most of the time AI tools are not compatible or often fail to integrate seamlessly with various RPM devices and legacy healthcare IT infrastructure, limiting its capacity of threat detection coverage.
Bias in Health Data	If the training data is skewed toward specific demographics, there is chance to reduces threat detection accuracy for underrepresented patient groups.
Black-Box Decision-Making	Lack of transparency in AI algorithms complicates audits and explanations of threat detection logic for regulators [111].

use unstructured data (such as patient notes or medical records). FL offers a compelling possibility for enhancing AI in RPM cybersecurity, especially in light of privacy issues in the healthcare industry. Future research should examine possible solutions for using FL to train AI models across decentralized RPM systems, such that it does not require the transfer of sensitive health data from local devices. This approach can enhance collaborative threat detection among hospitals and healthcare providers while maintaining data security and privacy as a priority.

B. NEED OF EXPLAINABLE AI (XAI)

One of the major challenges for AI in cybersecurity is the lack of transparency of AI in the decision-making process, which is commonly known as the ''closed box'' problem. The development of explainable AI (XAI) methods for threat intelligence in RPM systems should be the main focus of future studies. XAI models would help security and healthcare professionals better comprehend AI-driven judgments, which would increase trust, make regulatory compliance easier, and support decision-making during critical cases. The majority of AI models used in RPM cybersecurity are intended for reactive threat detection, in which case a breach is discovered after it has already happened. Future studies should focus on creating proactive AI models that continuously analyze patient data, device behavior, and external danger landscapes to anticipate such threats before they materialize. These predictive models can significantly reduce the risk of cyberattacks, allowing RPM systems to mitigate risks before they escalate into serious problems. Explainable AI (XAI) is increasingly important in RPM systems, which use AI to monitor patients with chronic or acute illnesses at remote locations [6]. XAI techniques are crucial for unveiling the reasoning behind AI systems' predictions and decisions, especially when dealing with sensitive health data [112]. The XAI framework, utilizing Shapley values and attention mechanisms, has been proposed to provide both post-hoc and intrinsic explainability for regression and classification tasks in RPM [6]. XAI in RPM can help detect early deterioration in patients' health, personalized monitoring, and learn human behavior patterns [6]. However, challenges remain in clinical validation, consistency assessment, and standardized quality evaluation of XAI methods [112].

C. CONCEPT OF "SECURE BY DESIGN"

The ''Secure by Design'' paradigm is becoming increasingly important in guaranteeing the security and safety of patient data as AI-driven threat intelligence is integrated into RPM systems. This approach emphasizes the importance of implementing security controls at every stage of the system development lifecycle, from the initial design to implementation and ongoing maintenance. RPM systems can detect and mitigate vulnerabilities efficiently before exploitation by including security elements from the beginning. In the healthcare industry, where data breaches can have serious repercussions for patient safety and privacy, taking a proactive approach is crucial. By integrating the most recent security practices and technology continuously, a ''Secure by Design'' approach makes it possible for AI-driven threat intelligence systems to adjust to new threats. Future research could examine the precise effects of applying the ''Secure by Design'' principles on the efficacy of threat intelligence generated by AI in the context of RPM. Research may concentrate on creating best practices, weighing the costs and benefits, and determining how these security measures actually affect patient outcomes and system integrity in the real world.

AI models need to adapt to the ongoing evolution of cyber threats. Subsequent investigations have to concentrate on creating adaptable AI systems capable of promptly assimilating emerging forms of cyberattacks, encompassing adversarial attacks on AI models. The integrity of RPM systems depends on the ability of AI-based threat intelligence to adapt constantly to shifting security environments. AI provides promising solutions in anomaly detection, but its application to automated incident response is still relatively new. Future studies should focus on developing AI-driven, real-time incident response frameworks that can mitigate possible harm without the need for human interaction by detecting and responding to cyber threats on their own. The combination of

AI and quantum computing can enhance the cybersecurity of RPM systems in the future. AI models could profit from more processing power, while quantum computing could be used to improve encryption methods. Subsequent research should investigate how quantum computing might improve the capacity of AI to identify complex dangers in RPM systems. Utilizing the ''Secure By Design'' concept, current research has addressed cyber security in the Remote Monitoring and Teleoperation (RMTO) of Autonomous Vehicles (AV). It examines the issue of possible attack routes, attack vectors, and threat surfaces that could be used to launch a malicious assault against an AV and an RMTO and demonstrates how this strategy could aid in enhancing security [113]. These studies can help lay the foundation of research work for implementation in Healthcare.

The future of AI-enhanced threat intelligence in RPM systems is promising, with opportunities for advancements in context-aware threat detection, FL, XAI, and proactive cybersecurity. Addressing these areas will not only strengthen the security of patient data but also improve the overall trust, compliance, and effectiveness of AI-powered RPM systems.

IX. CONCLUSION

This paper presents a comprehensive survey of AI-enhanced Threat Intelligence in Remote Patient Monitoring (RPM) systems, including recent developments, challenges, and future research directions. This review examined **113** research papers covering most aspects of AI-driven cybersecurity and its relevance to healthcare. The focus of this study was specifically on integrating AI models to secure data, mitigate threats, and detect anomalies. The intention was to gauge the current landscape of AI-driven cybersecurity, pinpoint significant trends, and emphasize areas that require further research. The analysis focused on four primary research questions regarding threat intelligence implementation, architectural solutions, integration of AI with RPMs, and related benefits and challenges.

The research papers considered were categorized into relevant thematic areas, such as AI-based anomaly detection, architecture for securing RPMs, and FL. The results revealed that the adoption of AI for securing RPMs is becoming more popular, specifically in anomaly detection. However, sufficient research has not been conducted on issues such as scalable architecture, data privacy, cross-platform interoperability, and data privacy. There is an apparent need for innovation in AI-based architectures for securing RPMs, as studies have shown the limitations of integrating blockchain to enhance data integrity.

According to the present state of research, AI is primarily used in RPM systems for automated threat mitigation, anomaly detection, and real-time monitoring. However, the integration of AI into RPM security is still in its early stages. Currently, ML models are used for anomaly detection and in predictive analytics. Edge AI and FL also have limited applications in terms of the security and privacy of healthcare data. This paper showed the gaps in existing systems and proposed how AI-based threat intelligence can be integrated. Most existing solutions lack the capabilities of distributed operations with real-time processing and cross-platform interoperability.

One of the key issues discussed in this paper is the requirement of AI systems to manage the ever-evolving cyber threats in RPM systems. A crucial need for future research on explainable AI (XAI), as well as the ethical issues regarding the implementation of AI in RPM systems, was highlighted in the paper. FL and Blockchain integration with AI for security and privacy in RPM also require further research. Subsequent investigations should focus on developing a scalable architecture that can address both privacy and security concerns in RPM systems. Advancing Federated Learning, Cloud-Edge architecture will make RPM security more resilient and robust to handle emerging threats.

In conclusion, this paper provides an extensive review of threat intelligence enhanced by AI in RPM systems, discussing important research questions in addition to revealing the potential benefits and challenges ahead. This review provides a foundation for future research on enhancing the cybersecurity framework of RPM systems by integrating AI technologies.

REFERENCES

[1] M. Elkhodr, S. Shahrestani, and H. Cheung, ''An approach to enhance the security of remote health monitoring systems,'' in *Proc. 4th Int. Conf. Secur. Inf. Netw.*, Nov. 2011, pp. 205–208.

[2] C. Ardito, T. D. Noia, E. D. Sciascio, D. Lofu, A. Pazienza, and F. Vitulano, ''An artificial intelligence cyberattack detection system to improve threat reaction in e-Health,'' in *Proc. ITASEC*, Apr. 2021, pp. 270–283.

[3] R. Mamadaliev, ''Artificial intelligence in cybersecurity: Enhancing threat detection and mitigation,'' *Sci. Collection InterConf.*, vol. 2023, no. 157, pp. 360–366, 2023.

[4] M. Sankaram, M. Roopesh, S. Rasetti, and N. Nishat, ''A comprehensive review of artificial intelligence applications in enhancing cybersecurity threat detection and response mechanisms,'' *Global Mainstream J.*, vol. 3, no. 5, pp. 1–14, Jul. 2024.

[5] R. Leung, ''Using AI–ML to augment the capabilities of social media for telehealth and remote patient monitoring,'' *Healthcare*, vol. 11, no. 12, p. 1704, Jun. 2023.

[6] T. Shaik, X. Tao, N. Higgins, L. Li, R. Gururajan, X. Zhou, and U. R. Acharya, ''Remote patient monitoring using artificial intelligence: Current state, applications, and challenges,'' *WIREs Data Mining Knowl. Discovery*, vol. 13, no. 2, p. e1485, Mar. 2023.

[7] L. Alevizos and M. Dekker, ''Towards an AI-enhanced cyber threat intelligence processing pipeline,'' *Electronics*, vol. 13, no. 11, p. 2021, May 2024.

[8] A. Singh, Kanishka, and S. K. Dubey, ''Analytical approach towards cybersecurity through AI-enabled threat intelligence,'' in *Proc. 11th Int. Conf. Rel., INFOCOM Technol. Optim. (Trends Future Directions) (ICRITO)*, Mar. 2024, pp. 1–6.

[9] M. Rizvi, ''Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention,'' *Int. J. Adv. Eng. Res. Sci.*, vol. 10, no. 5, pp. 55–60, 2023.

[10] F. C. Udegbe, O. R. Ebulue, C. C. Ebulue, and C. S. Ekesiobi, ''The role of artificial intelligence in healthcare: A systematic review of applications and challenges,'' *Int. Med. Sci. Res. J.*, vol. 4, no. 4, pp. 500–508, Apr. 2024.

[11] A. Petrovic, L. Jovanovic, K. Venkatachalam, M. Zivkovic, N. Bacanin, and N. Budimirovic, ''Anomaly detection in electrocardiogram signals using metaheuristic optimized time-series classification with attention incorporated models,'' *Int. J. Hybrid Intell. Syst.*, vol. 20, no. 2, pp. 159–183, Jun. 2024.

[12] L. Alevizos and M. Dekker, "Towards an AI-enhanced cyber threat intelligence processing pipeline," 2024, *arXiv:2403.03265*.
[13] G. Srivastava, A. Dhar Dwivedi, and R. Singh, "Automated remote patient monitoring: Data sharing and privacy using blockchain," 2018, *arXiv:1811.03417*.
[14] M. Jayson Baucas and P. Spachos, "Fog and IoT-based remote patient monitoring architecture using speech recognition," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2020, pp. 1–6.
[15] M. Gupta, S. Mittal, and M. Abdelsalam, "AI assisted malware analysis: A course for next generation cybersecurity workforce," 2020, *arXiv:2009.11101*.
[16] E. R. Ndukwe and B. Baridam, "A graphical and qualitative review of literature on AI-based cyber-threat intelligence (CTI) in banking sector," *Eur. J. Eng. Technol. Res.*, vol. 8, no. 5, pp. 59–69, Oct. 2023.
[17] N. El-Rashidy, S. El-Sappagh, S. Islam, H. M. El-Bakry, and S. Abdelrazek, "Mobile health in remote patient monitoring for chronic diseases: Principles, trends, and challenges," *Diagnostics*, vol. 11, no. 4, p. 607, Mar. 2021.
[18] O. Nait Hamoud, T. Kenaza, Y. Challal, L. Ben-Abdelatif, and M. Ouaked, "Implementing a secure remote patient monitoring system," *Inf. Secur. J., A Global Perspective*, vol. 32, no. 1, pp. 21–38, Jan. 2023.
[19] S. K. Polu, "Design of remote patient monitoring system for chronic diseases," *IJARCCE*, vol. 11, no. 3, p. 34, Mar. 2022.
[20] R. Abdolkhani, K. Gray, A. Borda, and R. DeSouza, "Patient-generated health data management and quality challenges in remote patient monitoring," *JAMIA Open*, vol. 2, no. 4, pp. 471–478, Dec. 2019.
[21] K. Boikanyo, A. M. Zungeru, B. Sigweni, A. Yahya, and C. Lebekwe, "Remote patient monitoring systems: Applications, architecture, and challenges," *Sci. Afr.*, vol. 20, Jul. 2023, Art. no. e01638.
[22] L. P. Serrano, K. C. Maita, F. R. Avila, R. A. Torres-Guzman, J. P. Garcia, A. S. Eldaly, C. R. Haider, C. L. Felton, M. R. Paulson, M. J. Maniaci, and A. J. Forte, "Benefits and challenges of remote patient monitoring as perceived by health care practitioners: A systematic review," *Permanente J.*, vol. 27, no. 4, pp. 100–111, Dec. 2023.
[23] J. Claggett, S. Petter, A. Joshi, T. Ponzio, and E. Kirkendall, "An infrastructure framework for remote patient monitoring interventions and research," *J. Med. Internet Res.*, vol. 26, May 2024, Art. no. e51234.
[24] B. R. N. Uka and P. O. Okunji, "Could remote patient monitoring (RPM) be effectively used with elderly COPD patients without limitations?" *J. Community Med. Public Health*, vol. 7, no. 3, pp. 3–4, Jul. 2023.
[25] A. Sagahyroon, "Remote patients monitoring: Challenges," in *Proc. IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2017, pp. 1–4.
[26] M. Ianculescu, D. Coardos, O. Bica, and V. Vevera, "Security and privacy risks for remote healthcare monitoring systems," in *Proc. Int. Conf. e-Health Bioeng. (EHB)*, Oct. 2020, pp. 1–4.
[27] B. Ondiege, M. Clarke, and G. Mapp, "Exploring a new security framework for remote patient monitoring devices," *Computers*, vol. 6, no. 1, p. 11, Feb. 2017.
[28] P. Choi and R. Walker, "Remote patient management: Balancing patient privacy, data security, and clinical needs," in *Remote Patient monitoring in Peritoneal Dialysis*, vol. 197, S. Karger, Ed., Karger, Apr. 2019.
[29] V. A. Onih, Y. S. Sevidzem, and S. Adeniji, "The role of AI in enhancing threat detection and response in cybersecurity infrastructures," *Int. J. Scientific Manage. Res.*, vol. 7, no. 4, pp. 64–96, 2024.
[30] N. Kumar, A. Sen, V. Hordiichuk, M. Jaramillo, B. Molodetskyi, and A. Kasture, "AI in cybersecurity: Threat detection and response with machine learning," *Tuijin Jishu/J. Propuls. Technol.*, vol. 44, no. 3, pp. 38–46, Sep. 2023.
[31] R. Sharma, "Artificial intelligence in healthcare: A review," *Turkish J. Comput. Math. Educ.*, vol. 11, no. 1, pp. 1663–1667, 2020.
[32] C. Chaowen, "Research on computer network security situation awareness warning mechanism based on artificial intelligence," in *Proc. IEEE 4th Int. Conf. Electron. Technol., Commun. Inf. (ICETCI)*, May 2024, pp. 748–753.
[33] N. Katiyar, M. S. Tripathi, M. P. Kumar, M. S. Verma, A. K. Sahu, and S. Saxena, "AI and cyber-security: Enhancing threat detection and response with machine learning," *Educ. Admin., Theory Practices*, vol. 30, no. 4, pp. 6273–6282, 2024.
[34] S. K. Sharma, "AI-enhanced cyber threat detection and response systems," *Shodh Sagar J. Artif. Intell. Mach. Learn.*, vol. 1, no. 2, pp. 43–48, 2024.
[35] V. S. Sree, C. S. Koganti, S. K. Kalyana, and P. Anudeep, "Artificial intelligence based predictive threat hunting in the field of cyber security," in *Proc. 2nd Global Conf. Advancement Technol. (GCAT)*, Oct. 2021, pp. 1–6.
[36] S. R. Pulyala, "From detection to prediction: AI-powered SIEM for proactive threat hunting and risk mitigation," *Turkish J. Comput. Math. Educ.*, vol. 15, no. 1, pp. 34–43, Jan. 2024.
[37] C. Chakraborty, S. M. Nagarajan, G. G. Devarajan, M. V. Ramana, and R. Mohanty, "Intelligent AI-based healthcare cyber security system using multi-source transfer learning method," *ACM Trans. Sensor Netw.*, pp. 2–4, May 2023.
[38] M. Diviya, R. Bhuvaneswari, M. Prabu, M. Subramanian, and A. K. Natarajan, "Securing healthcare systems integrating AI for cybersecurity solutions and privacy preservation," in *Cybersecurity and Data Management Innovations for Revolutionizing Healthcare* (Advances in Healthcare Information Systems and Administration Book Series). IGI Global Scientific Publishing, 2024.
[39] S. Ahmed, M. Singh, B. Doherty, E. Ramlan, K. Harkin, M. Bucholc, and D. Coyle, "Knowledge-based intelligent system for IT incident DevOps," in *Proc. IEEE/ACM Int. Workshop Cloud Intell. AIOps (AIOps)*, May 2023, pp. 1–7.
[40] S. Raja Sindiramutty, "Autonomous threat hunting: A future paradigm for AI-driven threat intelligence," 2023, *arXiv:2401.00286*.
[41] Shivam, Y. Yadav, and V. Malhotra, "Cyber AI research trends," *Int. J. Adv. Res. Sci., Commun. Technol.*, vol. 2024, pp. 324–325, Apr. 2024.
[42] S. K. Mandru, "How AI can improve identity verification and access control processes," *J. Artif. Intell. Cloud Comput.*, vol. 2022, pp. 1–5, Dec. 2022.
[43] S. Ramakrishnan, "Revolutionizing role-based access control: The impact of AI and machine learning in identity and access management," *J. Artif. Intell. Cloud Comput.*, vol. 2023, pp. 1–7, Sep. 2023.
[44] P. Neelakrishnan, "AI-driven proactive cloud application data access security," *Int. J. Innov. Sci. Res. Technol.*, vol. 2024, pp. 510–521, Apr. 2024.
[45] M. Ibrahim, A. Alsheikh, and A. Matar, "Attack graph modeling for implantable pacemaker," *Biosensors*, vol. 10, no. 2, p. 14, Feb. 2020.
[46] J. Kongsen, D. Chantaradsuwan, P. Koad, M. Thu, and C. Jandaeng, "A secure blockchain-enabled remote healthcare monitoring system for home isolation," *J. Sensor Actuator Netw.*, vol. 13, no. 1, p. 13, Feb. 2024.
[47] T. Flynn, G. Grispos, W. Glisson, and W. Mahoney, "Knock! Knock! Who is there? Investigating data leakage from a medical Internet of Things hijacking attack," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, 2020, pp. 1–10.
[48] V. Heydari, "A new security framework for remote patient monitoring devices," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Oct. 2020, pp. 1–4.
[49] J. Tully, J. Selzer, J. P. Phillips, P. O'Connor, and C. Dameff, "Healthcare challenges in the era of cybersecurity," *Health Secur.*, vol. 18, no. 3, pp. 228–231, Jun. 2020.
[50] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the Internet-of-Medical-Things (IoMT) systems security," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8707–8718, Jun. 2021.
[51] S. Abdulmalek, A. Nasir, W. A. Jabbar, M. A. M. Almuhaya, A. K. Bairagi, M. A.-M. Khan, and S.-H. Kee, "IoT-based healthcare-monitoring system towards improving quality of life: A review," *Healthcare*, vol. 10, no. 10, p. 1993, Oct. 2022.
[52] Z. Ali, S. Mahmood, K. M. U. Hassan, A. Daud, R. Alharbey, and A. Bukhari, "A lightweight and secure authentication scheme for remote monitoring of patients in IoMT," *IEEE Access*, vol. 12, pp. 73004–73020, 2024.
[53] N. Hamza, "A proposed remote monitoring system (RMS) for COVID-19 pandemic based on IoT medical devices and blockchain network," *J. Med. Internet Res. JMIR*, pp. 3–6, Nov. 2020.
[54] R. Pulimamidi and P. Ravichandran, "Enhancing healthcare delivery: AI applications in remote patient monitoring," *Tuijin Jishu/J. Propuls. Technol.*, vol. 44, no. 3, pp. 3948–3954, Nov. 2023.
[55] A. Dubey and A. Tiwari, "Artificial intelligence and remote patient monitoring in U.S. healthcare market: A literature review," *J. Market Access Health Policy*, vol. 11, no. 1, Dec. 2023, Art. no. 2205618.

[56] R. Malviya and P. Goyal, *Remote Patient Monitoring: A Computational Perspective in Healthcare*. River Publishers, Nov. 2023.

[57] R. Ch, P. Sudheer, and P. D. Kumar, "An overview of remote patient monitoring for improved patient care and cost reduction: The IoT revolutionizing health care," *Int. J. Educ. Manage. Eng.*, vol. 13, no. 6, pp. 33–40, Dec. 2023.

[58] S. Rangaraju, "Secure by intelligence: Enhancing products with AI-driven security measures," *EPH-Int. J. Sci. Eng.*, vol. 9, no. 3, pp. 36–41, Dec. 2023.

[59] A. J. Varma, N. M. Taleb, R. A. Said, T. M. Ghazal, M. Ahmad, H. M. Alzoubi, and M. T. Alshurideh, "A roadmap for SMEs to adopt an AI based cyber threat intelligence," in *The Effect of Information Technology on Bus. and Marketing Intelligence Systems*. Cham, Switzerland: Springer, Feb. 2023.

[60] V. R. Saddi, S. K. Gopal, A. S. Mohammed, S. Dhanasekaran, and M. S. Naruka, "Examine the role of generative AI in enhancing threat intelligence and cyber security measures," in *Proc. 2nd Int. Conf. Disruptive Technol. (ICDT)*, Mar. 2024, pp. 537–542.

[61] A. Dutta and S. Kant, "An overview of cyber threat intelligence platform and role of artificial intelligence and machine learning," in *Proc. Int. Conf. Inf. Sci. Syst.*, Jan. 2020, pp. 81–86.

[62] M. Sills, P. Ranade, and S. Mittal, "Cybersecurity threat intelligence augmentation and embedding improvement—A healthcare usecase," in *Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI)*, Nov. 2020, pp. 1–6.

[63] S. Gupta, A. S. Sabitha, and R. Punhani, "Cyber security threat intelligence using data mining techniques and artificial intelligence," *Int. J. Recent Technol. Eng.*, vol. 8, no. 3, pp. 6133–6140, Sep. 2019.

[64] Md. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous patient monitoring with a patient centric agent: A block architecture," *IEEE Access*, vol. 6, pp. 32700–32726, 2018.

[65] M. Ammi, O. Adedugbe, F. M. Alharby, and E. Benkhelifa, "Leveraging a cloud-native architecture to enable semantic interconnectedness of data for cyber threat intelligence," *Cluster Comput.*, vol. 25, no. 5, pp. 3629–3640, Oct. 2022.

[66] M. SafaeiSisakht, C.-H. Hsu, P.-Y. Hsu, and M.-Y. Chen, "An intelligent two-phase automated architecture for securing SDN-based IoT infrastructure," in *Proc. IEEE 3rd Int. Conf. Electron. Commun., Internet Things Big Data (ICEIB)*, Apr. 2023, pp. 12–16.

[67] N. Moustafa, E. Adi, B. Turnbull, and J. Hu, "A new threat intelligence scheme for safeguarding Industry 4.0 systems," *IEEE Access*, vol. 6, pp. 32910–32924, 2018.

[68] S. El Jaouhari and Y. Etiabi, "FedCTI: Federated learning and cyber threat intelligence on the edge for secure IoT networks," in *Proc. Int. Conf. Internet Things*, Nov. 2023, pp. 98–104.

[69] E. Fedorchenko, E. Novikova, and A. Shulepov, "Comparative review of the intrusion detection systems based on federated learning: Advantages and open challenges," *Algorithms*, vol. 15, no. 7, p. 247, Jul. 2022.

[70] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, Jan. 2019.

[71] E. A. Nitin and N. Sakhare, "A decentralized approach to threat intelligence using federated learning in privacy-preserving cyber security," *J. Electr. Syst.*, vol. 19, no. 3, pp. 106–125, Jan. 2024.

[72] B. Zaabar, O. Cheikhrouhou, M. Ammi, A. I. Awad, and M. Abid, "Secure and privacy-aware blockchain-based remote patient monitoring system for Internet of Healthcare Things," in *Proc. 17th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2021, pp. 200–205.

[73] S. K. Singh, S. Rathore, and J. H. Park, "BlockIoTIntelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence," *Future Gener. Comput. Syst.*, vol. 110, pp. 721–743, Sep. 2020.

[74] J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta, "Blockchain-based remote patient monitoring in Healthcare 4.0," in *Proc. IEEE 9th Int. Conf. Adv. Comput. (IACC)*, Dec. 2019, pp. 87–91.

[75] F. B. Ashraf and R. Reaz, "IoT-blockchain in remote patient monitoring," in *Proc. 5th Int. Conf. Future Netw. Distrib. Syst.*, Dec. 2021, pp. 186–194.

[76] J. Trivedi, J. Isoaho, and T. Mohammad, "A cloud-based secure architecture for remote patient monitoring integrating OPC UA and human digital twin," *Proc. Comput. Sci.*, vol. 251, pp. 248–255, Jul. 2024.

[77] M. Kumar, "Optimizing security for remote patient monitoring with edge computing strategies," *Int. Res. J. Adv. Eng. Manage.*, vol. 2, no. 5, pp. 1530–1535, May 2024.

[78] H. Su, L. Yao, D. Hou, M. Sun, J. Hou, J. Ying, H.-Y. Feng, P.-Y. Chen, and R. Hou, "Cloud computing management architecture for digital health remote patient monitoring," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Aug. 2021, pp. 209–214.

[79] G. Loseto, F. Scioscia, M. Ruta, F. Gramegna, S. Ieva, C. Fasciano, I. Bilenchi, and D. Loconte, "Osmotic cloud-edge intelligence for IoT-based cyber-physical systems," *Sensors*, vol. 22, no. 6, p. 2166, Mar. 2022.

[80] G. B. Prasad, G. Kiran, and H. Dinesha, "AI-driven cyber security: Security intelligence modelling," *Int. J. Multidisciplinary Res. Growth Eval.*, vol. 4, no. 6, pp. 961–965, 2023.

[81] A. Blanchard and M. Taddeo, "The ethics of artificial intelligence for intelligence analysis: A review of the key challenges with recommendations," *Digit. Soc.*, vol. 2, no. 1, p. 12, Apr. 2023.

[82] M. A. Althamir, J. Z. Boodai, and M. M. Hafizur Rahman, "A mini literature review on challenges and opportunity in threat intelligence," in *Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, Feb. 2023, pp. 558–563.

[83] S. Thapaliya and A. Bokani, "Leveraging artificial intelligence for enhanced cybersecurity: Insights and innovations," *SADGAMAYA*, vol. 1, no. 1, pp. 46–52, Jun. 2024.

[84] S. A. Jawaid, "Artificial intelligence with respect to cyber security," *J. Adv. Artif. Intell.*, vol. 1, no. 2, pp. 96–102, 2023.

[85] R. Garg and D. Jayanthila, "Empowering cybersecurity: A deep dive into AI-driven security intelligence modelling," *i-Manager's J. Inf. Technol.*, vol. 12, no. 4, pp. 1–6, Jan. 2023.

[86] R. C. Calderón, "The benefits of artificial intelligence in cybersecurity," Sematic Scholar, Ls Sslle Univ., Tech. Rep., 2019.

[87] S. O. Olabanji, Y. A. Marquis, C. S. Adigwe, S. A. Ajayi, T. O. Oladoyinbo, and O. O. Olaniyi, "AI-driven cloud security: Examining the impact of user behavior analysis on threat detection," *Asian J. Res. Comput. Sci.*, vol. 17, no. 3, pp. 57–74, Jan. 2024.

[88] A. Caldwell, "Novel cybersecurity challenges within artificial intelligence," *J. Internet Technol. Secured Trans.*, vol. 11, no. 1, pp. 796–801, Dec. 2023.

[89] B. T. Familoni, "Cybersecurity challenges in the age of AI: Theoretical approaches and practical solutions," *Comput. Sci. IT Res. J.*, vol. 5, no. 3, pp. 703–724, Mar. 2024.

[90] A. Oseni, N. Moustafa, H. Janicke, P. Liu, Z. Tari, and A. Vasilakos, "Security and privacy for artificial intelligence: Opportunities and challenges," 2021, *arXiv:2102.04661*.

[91] Y. Hu, W. Kuang, Z. Qin, K. Li, J. Zhang, Y. Gao, W. Li, and K. Li, "Artificial intelligence security: Threats and countermeasures," *ACM Comput. Surveys*, vol. 55, no. 1, pp. 1–36, Jan. 2023.

[92] H. Susanto, F. Leu, D. Rosiyadi, A. I. Basuki, and D. Setiana, "Data security for connected governments and organisations: Managing automation and artificial intelligence," in *Web 2.0 and Cloud Technologies for Implementing Connected Government*. IGI Global Scientific Publisher, 2022, pp. 229–251.

[93] M. S. Alzboon, A. F. Bader, A. Abuashour, M. K. Alqaraleh, B. Zaqaibeh, and M. Al-Batah, "The two sides of AI in cybersecurity: Opportunities and challenges," in *Proc. Int. Conf. Intell. Comput. Next Gener. Netw. (ICNGN)*, Nov. 2023, pp. 1–9.

[94] R. V. Krishnaveni, N. Pandey, and S. Modh, "Indigenous and disruptive remote patient monitoring devices—A case study on AI in healthcare," *SDMIMD J. Manage.*, vol. 14, no. 2, pp. 27–34, Oct. 2023.

[95] D. Gupta, M. Gupta, S. Bhatt, and A. S. Tosun, "Detecting anomalous user behavior in remote patient monitoring," in *Proc. IEEE 22nd Int. Conf. Inf. Reuse Integr. Data Sci. (IRI)*, Aug. 2021, pp. 33–40.

[96] P. Nalamani Govardhan, S. Surendranath, and M. Sundararajan, "Artificial intelligence-basedremote monitoring system for automated anomaly detection in wireless sensor networks," *Concurrency Comput., Pract. Exp.*, vol. 35, no. 2, p. 7462, Jan. 2023.

[97] S. Rani, D. Jining, D. Shah, S. Xaba, and P. R. Singh, "The potential application of artificial intelligence in healthcare and hospitals," in *Proc. ITM Web Conf.*, vol. 53, 2023, p. 1005.

[98] A. Albahar, "How AI improves telemedicine through improving data management in healthcare," *J. Knowl. Learn. Sci. Technol.*, vol. 2, no. 3, pp. 242–250, Dec. 2023.

[99] O. P. Adigwe, G. Onavbavba, and S. E. Sanyaolu, "Exploring the matrix: Knowledge, perceptions and prospects of artificial intelligence and machine learning in Nigerian healthcare," *Frontiers Artif. Intell.*, vol. 6, Jan. 2024, Art. no. 1293297.

[100] D. W. S. Ismail, "Threat detection and response using AI and NLP in cybersecurity," *J. Internet Services Inf. Secur.*, vol. 14, no. 1, pp. 195–205, Mar. 2024.
[101] H. N. Fakhouri, S. Alawadi, F. M. Awaysheh, F. Hamad, S. Alzubi, and M. N. AlAdwan, "An overview of using of artificial intelligence in enhancing security and privacy in mobile social networks," in *Proc. 8th Int. Conf. Fog Mobile Edge Comput. (FMEC)*, Sep. 2023, pp. 42–51.
[102] C. S. Eze and L. Shamir, "Analysis and prevention of AI-based phishing email attacks," *Electronics*, vol. 13, no. 10, p. 1839, May 2024.
[103] M. Abououf, S. Singh, R. Mizouni, and H. Otrok, "Explainable AI for event and anomaly detection and classification in healthcare monitoring systems," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 3446–3457, Feb. 2024.
[104] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. Artif. Intell. Statist.*, Jan. 2016, pp. 1273–1282.
[105] J. Lesouple, C. Baudoin, M. Spigai, and J.-Y. Tourneret, "Generalized isolation forest for anomaly detection," *Pattern Recognit. Lett.*, vol. 149, pp. 109–119, Sep. 2021.
[106] M. Dhinakaran, K. Phasinam, J. Alanya-Beltran, K. Srivastava, D. V. Babu, and S. K. Singh, "A system of remote patients' monitoring and alerting using the machine learning technique," *J. Food Quality*, vol. 2022, no. 1, 2022, Art. no. 6274092.
[107] M. Kavitha, P. V. V. S. Srinivas, P. S. L. Kalyampudi, S. F. Choragudi, and S. Srinivasulu, "Machine learning techniques for anomaly detection in smart healthcare," in *Proc. 3rd Int. Conf. Inventive Res. Comput. Appl. (ICIRCA)*, Sep. 2021, pp. 1350–1356.
[108] M. M. R. Woods, "Digital epidemiological surveillance, smart telemedicine diagnosis systems, and machine learning-based real-time data sensing and processing in COVID-19 remote patient monitoring," *Amer. J. Med. Res.*, vol. 8, no. 2, pp. 65–77, 2021.
[109] M. R. Tanhatalab, H. Yousefi, H. M. Hosseini, M. M. Bonab, V. Fakharian, and H. Abarghouei, "Deep RAN: A scalable data-driven platform to detect anomalies in live cellular network using recurrent convolutional neural network," in *Proc. IEEE 18th World Symp. Appl. Mach. Intell. Informat. (SAMI)*, Jan. 2020, pp. 269–274.
[110] F. Tsvetanov, "Integrating AI technologies into remote monitoring patient systems," *Eng. Proc.*, vol. 70, no. 1, p. 54, 2024.
[111] S. Sharma, R. Rawal, and D. Shah, "Addressing the challenges of AI-based telemedicine: Best practices and lessons learned," *J. Educ. Health Promotion*, vol. 12, no. 1, p. 338, Sep. 2023.
[112] F. Di Martino and F. Delmastro, "Explainable AI for clinical and remote health applications: A survey on tabular and time series data," *Artif. Intell. Rev.*, vol. 56, no. 6, pp. 5261–5315, Jun. 2023.
[113] V. Iyieke, J. Bryans, T. Robinson, O. Kosmas, A. Shipman, and H. Jadidbonab, "An adaptable security by design approach for ensuring a secured remote monitoring teleoperation (RMTO) of an autonomous vehicle," in *Proc. SAE Tech. Paper Ser.*, Apr. 2023, pp. 1–19.

JOLLY TRIVEDI received the bachelor's degree in electrical engineering and the master's degree in computer applications from IGNOU, Mumbai, India, in 2004 and 2014, respectively, and the M.Sc. degree in computer science with a major in cybersecurity from the University of Turku, Finland, in 2024, where she is currently pursuing the Ph.D. degree. She has eight years of experience as a Software Developer and six years of experience in leadership and management in software projects under various domains. She has been a Cybersecurity Consultant for the last five years. Her current research focus is the implementation of artificial intelligence in enhancing security and privacy in healthcare, and experimenting with the impact of the human digital twin in healthcare.

MOHAMMAD TAHIR (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in electrical and computer engineering from the Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur, Malaysia, in 2011 and 2016, respectively. He is currently a Lecturer with the Cybersecurity Laboratory, University of Turku, Finland. Prior to joining academics, he worked with the research and development division of industry for seven years on several projects related to the Internet of Things and cognitive radio. His research interests include 5G and beyond, cybersecurity, the Internet of Things, applied ML for wireless networks, network security, and autonomic computing.

JOUNI ISOAHO received the M.Sc. (Tech.) degree in electrical engineering and the Lic.Tech. and Dr.Tech. degrees in information technology from Tampere University of Technology, Finland, in 1989, 1992, and 1995, respectively. Since 1999, he has been a Professor with the University of Turku, Finland. The core of his research is communication and cyber security technologies. His current research interests include security of autonomous systems and AI, human and societal cybersecurity, and smart technology and digitalization.