American Journal of Multidisciplinary Research and Innovation (AJMRI)

ISSN: 2158-8155 (ONLINE), 2832-4854 (PRINT)

VOLUME 4 ISSUE 4 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Multidisciplinary Research and Innovation (AJMRI)

Volume 4 Issue 4, Year 2025
ISSN: 2158-8155 (Online), 2832-4854 (Print)
DOI: https://doi.org/10.54536/ajmri.v4i4.3017
https://journals.e-palli.com/home/index.php/ajmri

Securing AI-Enabled IoT Healthcare Devices: Practical Solutions for Protecting Patient Data

Baha Eldin Hamouda Hassan Hamouda[1*]

Article Information

Received: May 08, 2024

Accepted: June 06, 2024

Published: June 26, 2025

Keywords

Advanced Encryption Standard (AES), Artificial Intelligence, Data Breach Prevention, Data Loss Prevention, End-to-End Encryption, Internet of Things (IoT), Use of Healthcare Devices

ABSTRACT

AI provides a biometrics authentication system to enhance a patient's security, which requires unique physiological and behavioral characteristics to access it easily, and AI facilitates patient data through homomorphic encryption, differential privacy, and federation learning, allowing data to be analyzed and shared without exposing sensitive information. AI analyses user behavior patterns to detect potential insider threats or unauthorized access to patient data. The study highlight the centers on the security issues in IoT-based healthcare systems and presents a comprehensive framework designed to safeguard patient data. The study depicts the use of a method of a systematic literature review (SLR) to extract results and analyze unique security risks and their association with AI that enables IoT devices in healthcare. Furthermore, the results showed that implementation of continuous monitoring and audit mechanism is to respond and detected to its security incident implementation of continuous monitoring and audit mechanism is to respond and detected to security incident implementation of continuous monitoring and audit mechanisms is to respond and detect security incidents promptly. In conclusion, the given article addressed IoT solutions in healthcare, such as interoperability challenges and resource constraints. In an intrusion detection system, log monitoring irregularity detection is helpful for identification of unauthorised identification of unauthorized access for suspicious activities. Overall, the adoption of AI enables healthcare to rely on collecting and storing large patient data volumes. As a result, the data can be vulnerable to breaches, unauthorized access, and misuse.

INTRODUCTION

To ensure the integrity and confidentiality of sensitive medical information, securing AI in IoT healthcare devices is crucial. A practical solution involves a multi-faceted approach that addresses both technical and organizational aspects of cybersecurity. One essential element is a robust encryption protocol for secure data transmission between IoT devices in the healthcare system (Akkaoui, 2021). Strong encryption algorithms, such as an Advanced Encryption Standard (AES), guarantee that patient data remains confidential and cannot be intercepted by unauthorized individuals. Additionally, access control mechanisms are vital to restricted to an unauthorized access to IoT devices on healthcare networks. To have stronger authentication methods for example multi-authentication and a biometrics authentication to ensure only authorized personnel that have a direct access to a patient data.

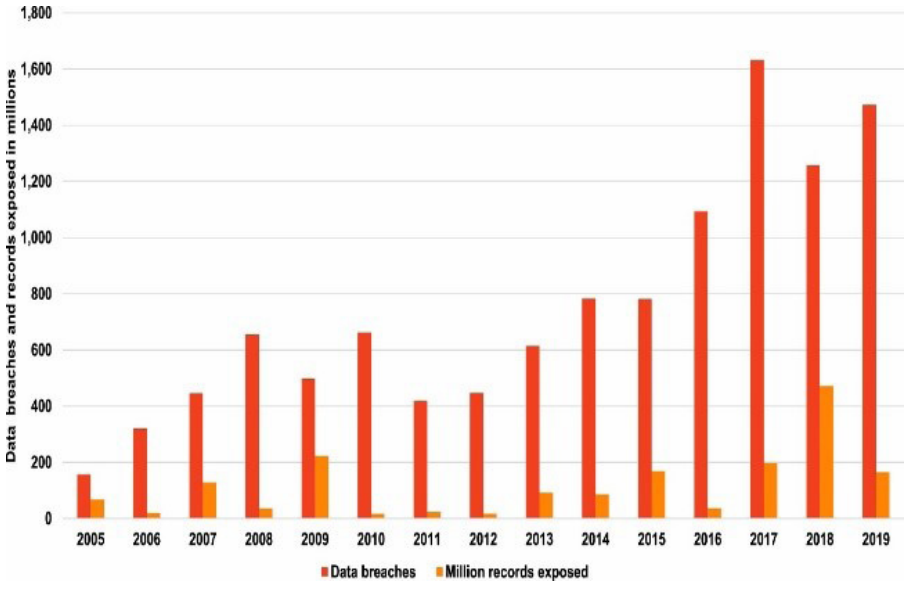

Figure 1: Yearly data violation from 2005 till 2019

[1] Department of Information Technology, Gulf Colleges, Hafar Al-Batin, Saudi Arabia
[*] Corresponding author's e-mail: baha56Hamouda@outlook.com

Despite the immense potential of AI and IoT in smart healthcare, it is crucial to address the security and privacy concerns associated with these innovative devices (Alshamrani, 2022). Figure 1 shows the yearly statistics about data breaches and millions of records exposed. For the last five years, a continuous upward trend has been witnessed in this domain, with more than 1000 data breaches since 2016. As researchers and practitioners explore AI and IoT applications for healthcare services, the protection of patient data must not be overlooked. While the seamless integration of AI-driven IoT into healthcare systems brings unprecedented opportunities, it is intrinsically tied to the challenge of ensuring robust security measures and privacy safeguards (Wang *et al.*, 2020).

Therefore, regular software updates and patch management are essential to mitigate vulnerabilities in IoT devices and software applications. This prompts the application of a security patch and updates, specifically for a healthcare organisation that aims to prevent an exploitation of known vulnerabilities and create a strong defence system against cyber threats. An implementation of intrusion detection prevented systems (IDPS) that enables real monitoring of network traffic and detection of anomalous behavior (Dissanayake *et al.*, 2022). IDPS solution can automatically identify blocked suspicious activity, such as unauthorised access to an attempt or data unfiltered to deteriorate possible security breaches. In addition, a healthcare organisation prioritises an employee in training and awareness programs to educate staff about its cybersecurity best practices to raise awareness, improve password hygiene, and implement device security protocols to empower an employee for recognition and to respond effectively to security incidents.

Lastly, an adherence to regulatory standards and compliance framework, an example of HIPAA (Health Insurance Probability and Accountability Act) in the US, scrutinised that healthcare organisation maintaining rigorous data protection to measure and uphold patient privacy rights (Stuurman & Kamara, 2016). The data encryption is to implement a robust encryption technique for protecting patient data both in rest and in transit, and the purpose is to ensure encryption if unauthorised while access is occurring and that data remains unreadable and this is unstable in the absence of appropriate decryption keys. Establishing rigorous access means controlling and limiting data access from authorised personnel, and role-based access control is a multi-factorial biometric authentication that is helpful to ensure individuals with proper authorisation access to patient data (Cakir, 2013).

For utilising techniques such as anonymisation and pseudonymisation, patient data was identified as unnecessary when fulfilling specific tasks. This act helps reduce data breaches while sitting, allowing AI algorithms to derive valuable insight. This adheres to the principle of data minimisation to collect and store a minimum amount of patient data required for an AI task, and this limits exposure to reduce a potential impact of a data that breaches and enhance overall security protocols (Angehrn *et al.*, 2020). Implementing continuous monitoring and audit mechanism is to detected, responded to a security incident promptly. In an intrusion detection system, log monitoring irregularity detection is helpful for an identification of unauthorised accessibility for suspicious activities. An effectiveness of an encryption protocol center to strengthen an encryption algorithm employed for a management to encrypted keys (Khashan *et al.*, 2021). A weaker encryption algorithm is used to manage and encrypt directly to performance that overheads, impacts on speed and efficiency of data transmission and its processing, in specific the real time healthcare scenario become timely accessible to patient information that is critical (Medileh *et al.*, 2020). During security audits, assessments become vital to identify and address the vulnerability, and they are often conducted periodically, leaving healthcare organisation susceptible to an emerging threat during an evaluation. While a practical solution such as encryption access to control, continuous monitoring, to a security assessment that are indispensable to protecting a patient data.

A given study fills the gap in an intersection of healthcare technology and a cyber-security, despite to increase an adoption of AI and IoT devices in healthcare, that secures device to safe-guarding patient data. Study fills out a gap that is unique security challenge by posed to rely on interconnectedness to networks and cloud based platforms by purpose to collect, transmit and analyse a data, this also encounter newer vulnerabilities such as potential data breach, unauthorized access and a tempering medical records that necessitates to tailored security solutions through best practices. In terms of dynamic nature of health environment this was characterized through a constant influx in new medical devices, updating a software, evolvement of cybersecurity threat to exacerbate threat that was needed to focusing on AI-enable IoT health services. Bridging a study gap is an essential aspect to foster collaboration in between a cybersecurity expert, policymakers and technology vendors to develop a holistic approach.

LITERATURE REVIEW

The rapid proliferation of wireless IoT devices has reached an unprecedented scale, with over 10 billion such devices already in existence and a projected surge to 30 billion by 2026 (Castillo O'Sullivan & Thierer, 2015). The integration of IoT technology into healthcare settings has opened new possibilities for enhancing patient care, but it has also raised significant security concerns that cannot be overlooked.

Managing various security elements about data management, transmission, privacy, and overall system integrity is the main challenge in IoT healthcare systems (Dang *et al.*, 2019). The possibility of data breaches is a serious risk since it jeopardises people's reputations and privacy. When hackers successfully compromise IoT

healthcare equipment, they have access to confidential information about patients. Security is still a major concern despite the IoT's rapid growth and its uses in the healthcare industry. Due to the delicate nature of the healthcare industry, protecting sensitive personal data and private health information has become a real problem (Maleh *et al.*, 2022).

The security challenges in IoT healthcare systems are multi-faceted, encompassing several key areas of concern. Maintaining the confidentiality of patient data is paramount to protecting sensitive medical information from falling into the wrong hands. Ensuring data integrity is also critical to prevent unauthorised alterations that could lead to incorrect diagnoses or treatment plans. Privacy protection is paramount to safeguard patients' personal information and maintain trust in healthcare services. Additionally, implementing robust authentication mechanisms between devices and tracking information flow is vital for secure communication within the IoT ecosystem (Dang *et al.*, 2019).

The security landscape of IoT healthcare systems faces threats from various types of attacks. According to Karloff and Wagner (2003), selective-forwarding attacks disrupt routing paths, hampering the timely transmission of critical alerts. On the other hand, sinkhole attacks manipulate traffic flow, directing valuable data to malicious nodes where it can be exploited for data theft and patient profiling. (Zhang & Hoshino, 2019) discusses that Jamming attacks target wireless communication, causing interruptions and disturbances in IoT devices' operations. The flooding attack aims to drain target resources, hindering continuous information transmission. Lastly, phishing attacks exploit user information to gain unauthorised access to IoT resources, posing serious security risks (Wallgren *et al.*, 2013).

Solutions for Ensuring Security in IoT-Enabled Environment

Addressing security concerns in patient data breaches is of paramount importance in healthcare-based IoT systems. Researchers have proposed several innovative solutions to safeguard patient data and preserve privacy. One notable approach involves lightweight authentication schemes utilising cryptographic hash functions for secure communication (Chacko & Hayajneh, 2018). These schemes are specifically designed to cater to the limited resources of wearable devices, ensuring anonymity and privacy preservation (Gupta *et al.*, 2019).

To address security concerns in IPv6-enabled IoT devices, Raza, Wallgren, and Voigt (Wallgren *et al.*, 2013) introduced the Address less IoT Server model and Secure-DAD mechanism to ensure secure communication between IoT clients and servers during the IP address configuration process (Liu *et al.*, 2020).

Cloud-based user authentication schemes have been proposed to ensure the secure authentication of medical data in IoT healthcare monitoring systems (Srinivas *et al.*, 2018). These schemes generate secret session keys, enabling secure communication between authorised users and wearable sensor nodes.

In open and public IoT deployments where devices are vulnerable to physical and closing attacks, implementing two-factor authentication schemes using physically unclonable functions (PUFs) has proven to be a promising solution (Gope & Sikdar, 2018). Such schemes enhance device authentication and bolster security.

Privacy-preserving data analytics, fog computing, and self-adaptive filters have emerged as valuable tools to facilitate secure data transmission in healthcare-based IoT systems (Anantharam *et al.*, 2015; Sharma *et al.*, 2018). These technologies enable efficient monitoring of healthcare information systems while mitigating potential privacy issues. Decentralised authentication using block-chain technology has emerged as an innovative solution to combat distributed denial of service attacks (DDoS) and ensure confidentiality, integrity, anonymity, and privacy (Akkaoui, 2021). This approach uses block-chain's inherent features to secure IoT healthcare systems and protect sensitive data(Sardar *et al.*, 2023).

Some studies have explored the integration of deep learning techniques with IoT-based healthcare systems to improve privacy protection and data analytics (Thilagam *et al.*, 2022). These techniques use convolutional neural networks (CNN) to analyse health-related data in the cloud while preserving user privacy. They also introduce safe access control components based on user attributes, achieving high accuracy levels. Other researchers have proposed deep-learning strategies based on secure searchable block-chain's, employing homomorphic encryption to allow safe data access through search (Ali *et al.*, 2022). Evaluating and compared an access controlling mechanisms with referencing models, they found that the proposed methods significantly enhance privacy, security as well as user behavior tracking in blockchain's-based IoT systems (Maleh *et al.*, 2022).

Deep learning methods have also been combined with authorised block-chain's and intelligent contracts to create secure data-sharing models (Kumar *et al.*, 2022). These models use innovative contract-based agreement methods and link related to self-attention, bio-directed long and a short-term memory (SA-BiLSTM) to enhance attack detection mechanisms. Other studies have focused on addressing security, privacy, and trust problems in IoT-based healthcare systems, particularly real-world applications (Kute *et al.*, 2022). Resolving secrecy, integrity, authentication, and access issues, they propose solutions to analyse security and privacy of healthcare information. Researchers were introduced a group theory (GT) that relies to binary spring search engine (BSS) technique by securing and tracking to different keyword-based access to datasets in blockchain's-based systems (Ali *et al.*, 2022). These methods offer secure critical revocation and improve security and safety in exchanging digital healthcare data. In cancer prediction systems using IoT and cloud computing, the AES method's encryption and decryption techniques ensure authentication and security

in dealing with sensitive patient data (Anuradha *et al.*, 2021). By focusing to make improvement in calculation and processing in healthcare, these systems facilitate secure access to encrypted blood results by doctors and nurses.

Other studies have proposed reciprocal authentication methods using lightweight cryptographic primitives to verify network devices quickly and efficiently in IoT-enabled hospitals (Gope *et al.*, 2019). These methods establish secure connections between approved devices and gateways to stop an unnecessary device to access a healthcare networks. Researchers are exploring a wide range of approaches to address security concerns in patient data breaches, leveraging innovative technologies and cryptographic techniques to ensure privacy, confidentiality, and integrity in healthcare-based IoT systems. By implementing these solutions, healthcare providers can enhance data protection and safeguard patient information in the rapidly evolving landscape of smart healthcare(Sardar *et al.*, 2023).

Key Security Problems in the Healthcare IoT Environment

This is to follow an outline of important challenges that needed to be considered when protecting patient data in an IT-enabling device by ensuring end-to-end encryption (E2E). This was relied on insight for a thorough assessment of the body of literature.

Data Management and Transfer Security

The framework should adopt secure communication protocols likewise a (Transport Layer Security) or a (Datagram Transport Layer Security) to safeguard data around an IoT devices and healthcare servers during transit. Data integrity checking, such as digital signatures or messages to an authentication code, can be implemented to detect any unauthorized alterations during transmission. By integrating these security measures, the healthcare IoT framework can establish a robust data security foundation, protecting sensitive patient information and fostering trust in the system's reliability and privacy (Sanci *et al.*, 2022).

Privacy Protection

Measures to preserve confidentiality and privacy should cover various topics, such as data anonymisation, pseudonymisation, and stringent access restrictions. Patients' personally identifiable information (PII) should be anonymised or pseudonymised to reduce the possibility that people might be identified from the data (Butpheng *et al.*, 2020).

Only authorised workers with a valid requirement for access to a particular piece of information should be able to access patient data thanks to the implementation of role-based access control (RBAC). Data minimisation practices should be used to lessen the possible effects of a data breach, ensuring that only necessary data is gathered and retained (Sharma *et al.*, 2018).

Device and System Security

The regulatory structure should impose stringent security controls, such as frequent software updates and patches to address known vulnerabilities, to guarantee the security of IoT devices and the system as a whole. Every IoT device must have a distinctive identification to prevent illegal devices from connecting to the network (Butpheng *et al.*, 2020).

IoT devices may be shielded from hacking and unauthorised alterations by incorporating secure boot and hardware-based security features like Trusted Platform Modules (TPMs). Using protocols like SSH (Secure Shell) or VPN (Virtual Private Network), secure communication routes between devices and gateways may be formed. SSL can also protect IoT devices and systems from unauthorised access and potential attacks by establishing secure communication routes between devices and gateways, enhancing overall security (Kute *et al.*, 2022).

Authentication and Access Control

The framework should implement strong authentication mechanisms, including from a multi-factor authentication to a biometric authentication, by verification to identify a user's and devices before granting access to patient data. Passwords should be securely stored using hashing algorithms with salting to prevent unauthorised access to user credentials (Anuradha *et al.*, 2021).

Access control policies should be well-defined, specifying the level of access granted to different user roles (Gope & Sikdar, 2018). Regular reviews of access rights and privileges are essential to revoke access for employees who no longer require it.

Protection against Various Types of Attacks

Machine learning-based anomaly detection can be employed to identify unusual patterns or behaviors that may indicate an ongoing attack (Kumar *et al.*, 2022). Network segmentation can also isolate critical healthcare devices from non-critical IoT devices, reducing the attack surface (Karlof & Wagner, 2003).

Resource Limitations

Considering the resource limitations of IoT devices, the framework should utilise lightweight cryptographic algorithms and protocols to minimise the computational overhead (Gope *et al.*, 2019).

Optimising data storage and transmission methods to reduce memory and bandwidth requirements will also enhance the efficiency of IoT devices. Regular performance assessments can be conducted to ensure that the resource usage of IoT devices remains within acceptable limits (Alshamrani, 2022).

By addressing these key problems cohesively, the proposed framework will provide a comprehensive approach to safeguarding patient data in IoT-enabled healthcare systems (Sanci *et al.*, 2022). Employing encryption, authentication, access control, and robust

security measures, the framework establishes a secure and privacy-aware environment for smart healthcare services, fostering patient trust and improving healthcare data protection.

Proposed Practical Framework to Ensure Data Protection

The proposed security benchmark for IoT architecture aims to address existing security gaps. It involves a comprehensive framework tailored for healthcare IoT, depicted in Figure 2. The framework emphasises confidentiality, integrity, access control, and other security themes to ensure robust protection for IoT devices and data. The key themes of our framework are briefly discussed in Table 1:

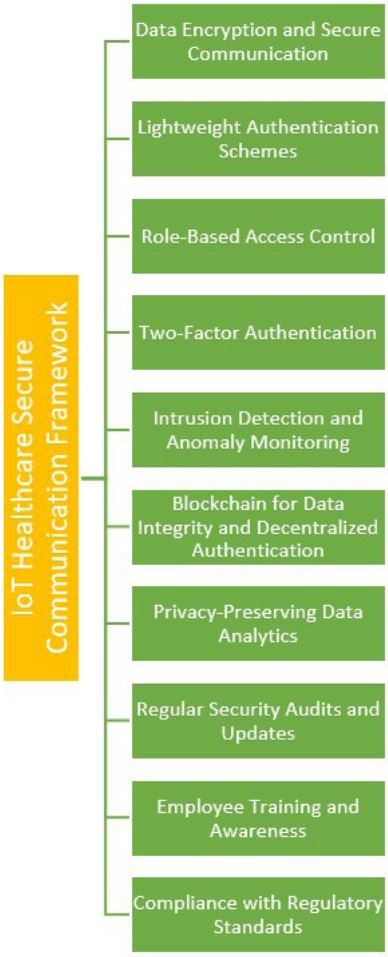

Figure 2: A proposed practical framework for IoT Architecture in Healthcare

Table 1: Themes for Ensuring Data Protection in IoT-Enabled Healthcare

Themes	Explanation
Data Encryption and Secure Communication	Utilising industry-standard cryptographic algorithms (e.g., AES, RSA) to encrypt patient data and implementing secure communication protocols (e.g., TLS, DTLS) for data transfer between IoT devices and healthcare servers.
Lightweight Authentication Schemes	Implementing lightweight authentication methods (e.g., SHA-256) for resource-constrained IoT devices, including device authentication using PSK or PKI and user authentication with HMAC-based OTP or TOTP.
Role-Based Access Control	Establishing a role-based access control system to manage and limit access to patient data based on defined roles (e.g., doctors, nurses, patients), with fine-grained access policies and regular audits for updates.
Two-Factor Authentication	Employing two-factor authentication (2FA) using physically unclonable functions (PUFs) to add an extra layer of security, combining something the user knows (e.g., password) with something the user has (e.g., physical token).

Intrusion Detection and Anomaly Monitoring	Deploying intrusion detection systems (IDS) to monitor network traffic and device behavior for potential security breaches, along with anomaly monitoring algorithms to detect abnormal patterns in IoT devices and systems.
Block-chain for Data Integrity	Utilising block-chain technology to ensure data integrity through an immutable ledger of transactions and employing decentralised authentication using smart contracts for transparent access control.
Privacy-Preserving Data Analytics	Implementing privacy-preserving data analytics techniques (e.g., differential privacy, federated learning) to protect individual privacy while enabling meaningful aggregated data analysis.
Regular Security Audits and Updates	Conducting periodic security audits, vulnerability assessments, and penetration testing to identify vulnerabilities, along with a prompt application of software and firmware updates to address known security issues.
Employee Training and Awareness	Providing continuous training and awareness programs for healthcare personnel and IoT device users to promote secure data handling, password management, and recognition of potential security threats.
Compliance with Regulatory Standards	Adhering to relevant healthcare data protection regulations (e.g., HIPAA, GDPR) to legally and ethically handle patient data, maintain data access logs, and establish data breach notification procedures.
Patient security with the help of AI adoption	Al helps analyse historical data to predict security risks and vulnerabilities in the healthcare system. AI provides a biometrics authentication system to enhance a patient's security, which requires unique physiological and behavioural characteristics to access easily.
AI algorithm and its indication	AI algorithms indicated potential threats and alerted security personnel to take appropriate actions. Adopting AI in healthcare helps analyse historical data to predict security risks and vulnerabilities in the healthcare system.
Role of threat intelligence in patient care	AI analyses patients' personal information through threat intelligence platforms that can collect, analyse, and disseminate information about an emergency cybersecurity and vulnerabilities in real-time.

Case Study Implementation

Remote patient monitoring (RPM) is an emerging healthcare approach that allows medical professionals to monitor patients' health remotely using IoT devices. IoT-enabled devices, such as wearables and smart sensors, enable continuous monitoring of vital signs and other health parameters, providing valuable data for healthcare providers to deliver timely interventions and personalised care. However, given the sensitive nature of patient data and the potential risks associated with IoT devices, implementing a secure framework is crucial to safeguard patient privacy and protect against cyber threats.

Implementation

• An implementation to a utilise industry-standard cryptographic algorithm for example AES or RSA, to encrypt all patient data transmitted between IoT devices and healthcare servers. This ensures that unauthorised entities cannot decipher even if the data is intercepted during transmission. Secure communication protocols like TLS or DTLS are employed to establish encrypted channels for data transfer, and digital certifications are used to verify the identity of the communicating parties, preventing man-in-the-middle attacks. Using industry-standard cryptographic algorithms like AES and RSA to encrypt all transmitted patient data ensures confidentiality. Even if an attacker intercepts the encrypted data between devices and servers, they could not decipher it without the encryption keys. Secure communication protocols TLS and DTLS help establish encrypted channels, preventing cybercriminals from performing man-in-the-middle attacks to snoop on unencrypted information. Digital certificates authenticate connecting parties, so only authorised devices and systems can exchange information over secure links. This strengthens the first line of defence against breaches of sensitive medical records and other confidential patient information collected by IoT sensors.

• Lightweight authentication schemes based on cryptographic hash functions, such as SHA-256, are implemented to address the resource limitations of IoT devices used for RPM. IoT devices have pre-shared keys (PSK) or device-specific credentials securely stored in hardware security modules, to ensure that only become trusted and authenticated devices can join the network. For user authentication, HMAC-that is based One-Time Passwords (HOTP) or Time-based One-Time Passwords (TOTP) are used to generate time-limited authentication tokens for secure user logins. Implementing traditional heavyweight security measures poses challenges for IoT devices with limited resources like wearables and smart home monitors. The framework adopts lightweight hash-based authentication schemes that consume low processing power and memory. SHA-256 cryptographic hashing ensures device credentials can be securely stored and validated without overburdening devices. Time-based one-time password schemes generate temporary login tokens on user devices for secure remote access, even if passwords are compromised. This balances usability with the protection of access credentials.

• A role-based access control (RBAC) system manages data access within the RPM environment. Different roles, such as doctors, nurses, and patients, are defined with specific access privileges. Access policies are fine-grained, limiting access to patient data to the minimum required for each role. Regular audits are conducted to review and update access privileges based on personnel changes or organisational requirements. Privileges are tailored according to defined roles like doctors, nurses and patients. Granular policies control what parts of electronic records each group may access based on need-to-know. Regular reviews help optimise privileges as personnel or responsibilities change. Combined with thorough auditing, it promotes the appropriate utilisation of confidential patient information while deterring unauthorised access attempts.

• In public and vulnerable IoT deployments, two-factor authentication (2FA) is implemented using physically clonable functions (PUFs). This additional layer of security generates unique identifiers for each IoT device, making it challenging for unauthorised devices to impersonate valid ones. The 2FA approach combines a user-known that was password and a user, for example, a physical token or its mobile devices, significantly reduces the risk of unauthorized access to passwords even if passwords are compromised. Two-factor authentication brings an additional layer of identity verification using hardware tokens generated via physically clonable functions. Even if passwords are phished, or software faults occur, impersonating devices is difficult without physical access. Encapsulating keys in tamper-resistant security modules reinforce device-level credentials. The dual authentication factors - something you know and have - significantly raise the bar against outsiders gaining illicit control over connected medical equipment or accessing private accounts.

By implementing this comprehensive framework, the healthcare provider can create a secure, privacy-aware IoT-enabled environment for remote patient monitoring. Encryption, authentication, access control, intrusion detection, block-chain, privacy-preserving techniques, and regular security audits and updates establish a robust defence against security threats, safeguarding sensitive patient information and fostering trust in RPM services.

MATERIALS AND METHODS

The study adopts a systematic literature review to explore and analyse existing research on securing AI-enabled IoT healthcare devices and protecting patient data. By conducting a systematic review, the study ensures a comprehensive and objective assessment of the current state of knowledge in the field, identifying key themes and practical solutions proposed by researchers and practitioners.

Systematic Model

Literature Search

The study initiates with a systematic research of academic databases, research journals, conference proceedings, and reputable sources. The keywords used for the search include "IoT healthcare security," "AI-enabled IoT healthcare," "data protection in healthcare IoT," "secure IoT communication," "block-chain in healthcare," "privacy-preserving data analytics," "intrusion detection in IoT," and related terms.

Inclusion and Exclusion Criteria

Inclusion of peer-reviewed articles published in the last 5 years.

Data Extraction

Relevant data on encryption, authentication, access control, intrusion detection, block-chain, privacy-preserving techniques, and regulatory compliance.

Analysis and Discussion

Identification of common themes and key security challenges, comparison of proposed solutions, and discussion of findings.

Case Setting

The suggested pragmatic methodology uses remote patient monitoring (RPM) employing AI-enabled IoT devices as its case study. RPM enables wearables and smart sensors by medical providers to remotely monitor patients' health, allowing individualised and prompt treatments. The systematic methodology thoroughly examines academic sources to comprehend security issues and suggested fixes in AI-enabled IoT healthcare. The framework was created with RPM in mind, guaranteeing a safe and private environment. It seeks to protect patient data and promote confidence in smart healthcare services by addressing important security topics.

Ethical Consideration

Ethics considerations come into play when integrating IoT solutions into the healthcare field. Protecting patient privacy and ensuring data security is paramount due to the sensitive health information gathered and transmitted by IoT devices. To achieve this, robust measures such as encryption, access controls, and privacy protection must be implemented to prevent unauthorised access or data breaches. Moreover, obtaining informed consent from patients before utilising their data for IoT services is imperative.

RESULTS AND DISCUSSION

RPM Framework

The proposed practical framework for ensuring data protection, as discussed in Table 1 in IoT-enabled healthcare, addresses the critical challenges and requirements of securing sensitive patient information in a connected environment. Each theme in the table represents a vital aspect of the framework, contributing to a complete security and privacy of the IoT ecosystem. This theme emphasizes the importance of encrypting patient data and establishing channels for a reason to

communicate in between IoT devices and healthcare servers. Encryption ensures that even if data is intercepted, it remains unreadable and protected from unauthorised access. Given the resource limitations of IoT devices, this theme advocates for efficient authentication methods that do not burden the devices with heavy computational overhead. By employing lightweight authentication schemes, such as cryptographic hash functions, secure and efficient device and user authentication can be achieved.

Securing data in AI-enabled IoT healthcare devices was a multi-faceted endeavour that required a comprehensive approach to addressing potential vulnerabilities to mitigate risk effectively. A robust encryption mechanism is crucial for protecting data with rest and transit. An encryption mechanism is essential to safeguard data in conditions such as rest and a transit position (Singh *et al.*, 2024). The encryption of sensitive data such as patient medical records and diagnostic data by healthcare organisation was ensured in the condition that unauthorised access could occur, and data would remain unreadable and unusable. Access to control mechanisms played a pivotal role in limiting data access to authorised personnel only. A utilisation of stronger authentication methods like a biometric authentication or multi-factorial authentication aims to enhance security by purpose to verify an identity of an individual by attempting an access the data. A role-based access control further refines access permission based on a user's specific role and responsibility in a healthcare organisation by minimising the risk of unauthorised data access.

Continuous monitoring of device activity and networking traffic is essential for the detection from responding to potential security threats promptly. Implementing an intrusion detection system to a security information and event management (SIEM) solutions enabled healthcare organisation to identify suspicious behavior or an anomaly indicating a security breach (González-Granadillo *et al.*, 2021). Real-time monitoring empowers a security team by taking immediate action to mitigate risk and protect sensitive data. Regular security assessments and audits are helpful and promptly remediate vulnerabilities in AI-enabling IoT devices (Gonçalves, 2023). A comprehensive training program is essential to foster a culture of cybersecurity and its awareness among healthcare staff. Educating employees about common cyber-security threats, best practices to protect data, and the importance of security policies and procedures strengthened an overall security posture to healthcare.

AI Adoption in Healthcare for Patient Data Protection

Adopting a multi-layered approach to security is essential to address a complex challenge that AI poses- enabled devices in healthcare. That approach directly involves not securing devices to fortify underlying networks to infrastructure and could base storage system. Regular security audits and updates are necessary for promptly identifying patch vulnerabilities to minimise the risk factor of exploitation by a malicious actor (Sakhawat *et al.*, 2024). Furthermore, educating healthcare staff about cyber-security best practices fosters a culture of vigilance that can enhance the overall security posture to AI-enabled IoT healthcare services to ensure the confidentiality and availability of patient data.

Privacy and patient data protection are important aspects of AI that enable a healthcare system, and they help safeguard patient confidentiality, including personal health information, medical records, genetic data, physical orientation, and real-time monitoring. These factors were a higher priority when handling utmost care. In addition, maintaining patient safety means respecting an individual's rights and fostering trust between patients and healthcare providers. The adoption of AI enables healthcare to rely on collecting and storing large patient data volumes. As a result, the data can become vulnerable to breaches, unauthorised access, and misuse. AI adoption is due to robust data security measures, including encryption, access to control security, storage and transmission protocols. AI for securing patient data was used for analysis and decision-making to respect patient autonomy and privacy necessities to obtain informed consent to collect, store, and use potential healthcare data [36].

AI algorithms indicated potential threats and alerted security personnel to take appropriate actions. Adopting AI in healthcare helps analyse historical data to predict security risks and vulnerabilities in the healthcare system. AI provides a biometrics authentication system to enhance a patient's security, which requires unique physiological and behavioral characteristics to access it easily. Natural language processing can be used for automatic analysis to classify text data, such as medical records and communication logs, for sensitive information [34]. This is to identify and redact or encrypt sensitive data. Furthermore, the NLP algorithm helps prevent unauthorised access to a patient's information. AI facilitates patient data through homomorphic encryption, differential privacy, and federation learning, allowing data to be analysed and shared without exposing sensitive information. AI analyses user behavior patterns to detect potential insider threats or unauthorised access to patient data.

Moreover, AI analyses patients' personal information through threat intelligence platforms that can collect, analyse, and disseminate information about emergency cybersecurity and vulnerabilities in real time. AI can dynamically adapt to measure the security measures of patients based on change threats to evolve an attack vector [35]. AI systems can adjust security and protocols to mitigate emerging risks to protect patient data that is more effective. Integrating AI technology secures the information of patients to safeguard them against cybersecurity threats and ensure compliance in the presence of regulatory requirements such as HIPAA in the US. In the absence of a standardised benchmark, it is challenging to evaluate whether a particular AI system meets a clinical requirement (gold standards), performs

betterment (improves) patient safety, or worsens (harms patients) to a similar system through provided healthcare context.

AI power visual assistance and chatbots play an important role in healthcare by providing patients with personalised health information, answering queries, and assisting in scheduling appointments. These conversation events agents utilise natural language procedures to understand and respond to patient questions for improved access to health by reducing an administrative burden [36]. AI algorithms can optimise healthcare to predict patient flow, improve scheduling, and optimise to allocate resources. In the context of patient ethics, AI helps optimise and streamline flow, reduce waiting times, and enhance operational efficacy. [37]. To prioritise patient safety, it enables a healthcare system that often involves sharing and analysing patient data for commercial, research, and collaborative reasons. AI allows attackers to identify an individual to a supposed anonymised dataset to connect multiple data sources using advanced linkage techniques [38]. In most of the hospitals in the UK, the NHS tried to resolve privacy concerns highlighted by biases or disproportionality affecting a certain individual or marginalised groups that were leading to unequal and unfair healthcare practices.

Comparative Analysis

This section evaluates the performance of current IoT solutions tailored for healthcare applications, as shown in Table 2. The evaluation centers around key security aspects, such as authentication, confidentiality, trust, resilience, data freshness, fault tolerance, and self-healing. The proposed solution, AMI architecture, is compared with existing schemes, revealing that many lack fault tolerance and self-healing features, making them less dependable in unforeseen circumstances. On the other hand, AMI architecture stands out as an all-inclusive solution that meets the required security standards, making it a trustworthy option for IoT healthcare systems. However, a challenge remains in securing communication between gateways and off-the-shelf sensors/nodes, mainly due to the use of proprietary protocols in commercial sensors. This issue requires further attention and exploration.

Table 2: Comparative analysis

IoT solution	Authentication	Confidentiality	Self-healing	Fault tolerance	Resilience	Data freshness	Trust
[16]	✓	✓	✗	✗	✗	✗	✓
[17]	✓	✓	✗	✗	✗	✗	✓
[18]	✓	✓	✗	✗	✓	✓	✓
[20]	✓	✓	✗	✗	✓	✓	✓
[21]	✗	✓	✗	✗	✗	✗	✓
[23]	✗	✗	✓	✓	✗	✗	✗
[24]	✓	✓	✗	✗	✓	✗	✓
[25]	✓	✓	✗	✓	✓	✓	✓
Proposed architecture	✓	✓	✓	✓	✓	✓	✓

CONCLUSION

Regular software updates and patch management are essential to mitigate vulnerabilities in IoT devices and software applications. This prompts the application of a security patch and updates, specifically for a healthcare organization that aims to prevent the exploitation of known vulnerabilities and create a strong defense system against cyber threats. Continuous monitoring of device activity and networking traffic is essential to detect and respond to a potential security threat promptly.

LIMITATIONS

- IoT solutions in healthcare have certain limitations that require acknowledgement.
- The interoperability challenge arises from different devices operating on varied protocols and standards, hampering seamless integration.
- Additionally, reliance on internet connectivity for IoT devices may lead to vulnerabilities and disruptions in areas with poor network coverage.

REFERENCES

Akkaoui, R. (2021). Blockchain for the management of Internet of Things devices in the medical industry. *IEEE Transactions on Engineering Management.*

Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., Teo, J., & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors, 22*(2), 572.

Alshamrani, M. (2022). IoT and artificial intelligence implementations for remote healthcare monitoring systems: A survey. *Journal of King Saud University-Computer and Information Sciences, 34*(8), 4687-4701.

Anantharam, P., Banerjee, T., Sheth, A., Thirunarayan, K., Marupudi, S., Sridharan, V., & Forbis, S. G. (2015). Knowledge-driven personalized contextual mHealth service for asthma management in children. In *2015 IEEE International Conference on Mobile Services* (pp. 228–235). IEEE.

Angehrn, Z., Haldna, L., Zandvliet, A. S., Gil Berglund, E., Zeeuw, J., Amzal, B., Cheung, S. A., Polasek, T. M., Pfister, M., & Kerbusch, T. (2020). Artificial intelligence and machine learning applied at the point of care. *Frontiers in Pharmacology, 11,* 759.

Anuradha, M., Jayasankar, T., Prakash, N., Sikkandar, M. Y., Hemalakshmi, G., Bharatiraja, C., & Britto, A. S. F. (2021). IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. *Microprocessors and Microsystems, 80,* 103301.

Butpheng, C., Yeh, K.-H., & Xiong, H. (2020). Security and privacy in IoT-cloud-based e-health systems—A comprehensive review. *Symmetry, 12*(7), 1191.

Cakir, E. (2013). Single sign-on: Risks and opportunities of using SSO (Single Sign-On) in a complex system environment with a focus on overall security aspects. In *Proceedings of the International Conference on Security and Privacy* (pp. 69–79).

Castillo O'Sullivan, A., & Thierer, A. D. (2015). Projecting the growth and economic impact of the Internet of Things. *SSRN.*

Chacko, A., & Hayajneh, T. (2018). Security and privacy issues with IoT in healthcare. *EAI Endorsed Transactions on Pervasive Health and Technology, 4*(14).

Dang, L. M., Piran, M. J., Han, D., Min, K., & Moon, H. (2019). A survey on internet of things and cloud computing for healthcare. *Electronics, 8*(7), 768.

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2022). Software security patch management-A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology, 144,* 106771.

Gonçalves, E. d. A. (2023). *Analysis of implementation of a Security Information and Events Management (SIEM) System in Public Business Entities (PBE) hospitals.*

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors, 21*(14), 4759.

Gope, P., Das, A. K., Kumar, N., & Cheng, Y. (2019). Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics, 15*(9), 4957-4968.

Gope, P., & Sikdar, B. (2018). Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. *IEEE Internet of Things Journal, 6*(1), 580-589.

Gupta, A., Tripathi, M., Shaikh, T. J., & Sharma, A. (2019). A lightweight anonymous user authentication and key establishment scheme for wearable devices. *Computer Networks, 149,* 29-42.

Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks, 1*(2-3), 293–315.

Khashan, O. A., Ahmad, R., & Khafajah, N. M. (2021). An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. *Ad Hoc Networks, 115,* 102448.

Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Islam, A. N., & Shorfuzzaman, M. (2022). Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems. *IEEE Transactions on Industrial Informatics, 18*(11), 8065-8073.

Kute, S. S., Tyagi, A. K., & Aswathy, S. (2022). Security, privacy and trust issues in internet of things and machine learning based e-healthcare. *Intelligent Interactive Multimedia Systems for e-Healthcare Applications,* 291-317.

Liu, R., Weng, Z., Hao, S., Chang, D., Bao, C., & Li, X. (2020). Addressless: enhancing IoT server security using IPv6. *IEEE Access, 8,* 90294-90315.

Maleh, Y., Lakkineni, S., Tawalbeh, L. A., & AbdEl-Latif, A. A. (2022). Blockchain for cyber-physical systems: Challenges and applications. In *Advances in blockchain technology for cyber-physical systems* (pp. 11–59). Springer.

Medileh, S., Laouid, A., Euler, R., Bounceur, A., Hammoudeh, M., AlShaikh, M., Eleyan, A., & Khashan, O. A. (2020). A flexible encryption technique for the internet of things environment. *Ad Hoc Networks, 106,* 102240.

Sakhawat, A. R., Fatima, A., Abbas, S., Ahmad, M., & Khan, M. A. (2024). Emerging technologies for enhancing robust cybersecurity measures for business intelligence in Healthcare 5.0. In *Strengthening industrial cybersecurity to protect business intelligence* (pp. 270–293). Springer.

Sanci, L., Williams, I., Russell, M., Chondros, P., Duncan, A.-M., Tarzia, L., Peter, D., Lim, M. S., Tomyn, A., & Minas, H. (2022). Towards a health promoting university: descriptive findings on health, wellbeing and academic performance amongst university students in Australia. *BMC Public Health, 22*(1), 1-24.

Sardar, A., Umer, S., Rout, R. K., Wang, S.-H., & Tanveer, M. (2023). A secure face recognition for IoT-enabled healthcare system. *ACM Transactions on Sensor Networks, 19*(3), 1-23.

Sharma, S., Chen, K., & Sheth, A. (2018). Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. *IEEE Internet Computing, 22*(2), 42-51.

Singh, N., Buyya, R., & Kim, H. (2024). Securing cloud-based Internet of Things: Challenges and mitigations. *arXiv preprint arXiv:2402.00356.*

Srinivas, J., Das, A. K., Kumar, N., & Rodrigues, J. J. (2018). Cloud centric authentication for wearable healthcare monitoring system. *IEEE Transactions on Dependable and Secure Computing, 17*(5), 942-956.

Stuurman, K., & Kamara, I. (2016). IoT standardization—the approach in the field of data protection as a model for ensuring compliance of IoT applications? In *2016*

IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 182–188). IEEE.

Thilagam, K., Beno, A., Lakshmi, M. V., Wilfred, C. B., George, S. M., Karthikeyan, M., Peroumal, V., Ramesh, C., & Karunakaran, P. (2022). Secure IoT Healthcare Architecture with Deep Learning-Based Access Control System. *Journal of Nanomaterials, 2022*.

Wallgren, L., Raza, S., & Voigt, T. (2013). Routing attacks and countermeasures in the RPL-based internet of things. *International Journal of Distributed Sensor Networks, 9*(8), 794326.

Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S., & Zhou, W. (2020). Security and privacy in 6G networks: New areas and new challenges. *Digital Communications and Networks, 6*(3), 281-291.

Zhang, X., & Hoshino, K. (2019). Implantable and wearable sensors. In S. K. Saha & S. K. Ghosh (Eds.), *Biomedical sensors and instrumentation* (pp. 489–545). Elsevier. https://doi.org/10.1016/B978-0-12-814862-4.00008-9