IoT Data Breaches and Privacy Issues in Healthcare Systems

Mohamad Nur Hidayat Zarkia @ Zakaria[1]& Sahnius Usman[2]

[1]*Faculty of Artificial Intelligence*

[2]*Malaysia-Japan International Institute of Technology*

[1]*mohamadnurhidayat@graduate.utm.my,* [2]*sahnius.kl@utm.my*

Article history

Received:
4 May 2025

Received in revised form:
10 May 2025

Accepted:
20 May 2025

Published online:
27 June 2025

*Corresponding author:
mohamadnurhidayat@graduate.utm.my

Abstract

The integration of the Internet of Things (IoT) devices in the healthcare system has enhanced patient care through remote monitoring, wearable devices, smart medical systems, and other embedded systems that track patients' health. These advancements have boosted operational efficiency, cut costs, enabled real-time patient monitoring, and improved patient outcomes. However, the widespread adoption of IoT in healthcare also introduces significant privacy risks and vulnerabilities, exposing sensitive patient data to unauthorized access and breaches. This study aims to explore the threat related to the data breaches associated with healthcare IoT systems, review existing mitigation strategies, and propose future research directions to address these challenges. Using a literature review of publications published from 2019 to 2024, consisting of 25 articles selected, the keyword-related study is identified. The study examines IoT applications such as remote patient monitoring (RPM), wearable devices, and telemedicine, highlighting their role in improving patient outcomes while underscoring the associated risks of data exposure. Advanced solutions, including blockchain technology, federated learning, and AI-driven threat detection, were identified and evaluated as potential mitigation strategies. Findings reveal that IoT-enabled healthcare systems face persistent challenges, including a lack of standardized security protocols, resource constraints in IoT devices, and the complexity of maintaining data privacy across interconnected networks. By addressing current gaps and implementing advanced solutions, IoT devices can significantly enhance healthcare delivery without compromising patient privacy and data security.

Keywords: *IoT, Healthcare, Data Breaches, Privacy, IoT Security*

1. Introduction

Rapid technological advancements in this new era have revolutionized healthcare, driving innovation that improves both patient care and hospital operations. Innovations such as remote monitoring, wearable devices, and smart sensors have helped to reduce the cost for the management of managing healthcare and operations. While the Internet of Things (IoT) devices in healthcare platforms offer user benefits such as effective monitoring, they also pose significant privacy and data breach risks. The case related to the IoT data breaches identified by Censys mentions about 14,004 unique IP addresses, healthcare devices, and data systems that are potentially exposing sensitive medical information on the public internet. This exposure significantly increases the risk of unauthorized access and exploitation. Nearly 50% of these exposed hosts (6,884) are in the United States,

* Corresponding author. mohamadnurhidayat@graduate.utm.my

DOI: 10.11113/oiji2025.13n1.327

followed by 10.5% (1,476) in India. In contrast, the United Kingdom had only 200 publicly available hosts, possibly reflecting its more centralized healthcare infrastructure.

IoT devices in the healthcare system change in how humans think and practice taking care of their healthy lifestyles. To address the IoT devices in healthcare security, several studies have proposed solutions, such as encryption methods, blockchain-based frameworks, and anomaly detection, that will be covered in the next section. The vulnerability in IoT devices requires the security mechanism to be implemented into the IoT devices to ensure that the security of the devices, nodes, network, and data privacy remain protected, and data breaches can be prevented.

This study aims to explore and review privacy issues related to the data breaches which are associated with IoT devices in healthcare applications, focusing on the vulnerabilities and implications for patient privacy. It emphasizes the background of related works on IoT devices in healthcare applications and implementation, highlighting user benefits. The IoT sector's vulnerability and threats are reviewed, highlighting privacy issues and data breaches. Technical countermeasures to secure the Internet of Things (IoT) devices against privacy issues and data breaches are also emphasized in this paper. This paper has been organized as follows: First, in Section 2, the background of the case study is presented. Next Section 3 briefly explains IoT devices in healthcare as well as data breaches and privacy issues concerns. Then, Section 4 discusses challenges and future directions of research in a healthcare system. Finally, in Section 5, provide a brief conclusion on the paper.

1.1. Methodology of this review

This subsection mentions the literature review of the IoT devices in healthcare privacy issues and data breaches, identifying the key important issues in this research. This article reviews existing articles from 2019 to 2024, which is 5 years backward. By searching for the required article, the literature review is conducted by utilizing existing libraries such as IEEE Explore, Science Direct, Google Scholar, and SpringerLink. The keyword search uses terms such as “IoT”, “Internet of Things”, “Privacy”, “Data Breaches”, and combines them with one of the following keywords ‘‘healthcare’’, ‘‘health services’’, ‘‘medical services’’, and ‘‘health-related services’’. To narrow down the result, we will exclude duplicates of the article, focusing on the specific topic. The exclusion criteria are related to the IoT Blockchain, and certain articles are selected. Lastly, 25 articles are being selected. Each of the papers was examined properly to ensure all the questions related to the research could be answered and fulfilled the requirements.

2. Background

The complexity of the IoT devices structures makes user hard to maintain security on a large scale of attack vectors. The possibility of the attack comes from any consequences, such as intruders or hackers who have access remotely to IoT devices, which requires to implement a security solution to put in place. The five layers of IoT application structure, such as the physical object layer, connectivity layer, middleware layer, big data analytics layer, and application layer, also have different technologies that bring security problems, risk, and vulnerability. This

paper focuses on privacy issues and data breaches relating to the IoT in healthcare applications.

Healthcare services in the United States, as an example, have spent a huge amount of nearly $10.348 per person in 2016, showing the increasing healthcare costs and the growth of the population (Rathee et al., 2020). Technology development significantly enhances the quality of patient care and reduces costs efficiently. IoT devices can also offer a service worldwide with interconnected devices without the need to be human intervention in place.

The development of IoT devices has led to an increase in interconnected devices, which is expected to exceed 50 billion by 2025 (Sun et al., 2024). The growth of this technology has brought significant security and privacy challenges in IoT operating systems, which are crucial for managing and driving intelligent and smart devices. The security and privacy of these systems are important, especially related to healthcare, as they handle sensitive data and ensure the proper functioning of IoT devices. IoT devices have limited resources and no security, as well as self-protection, which can be exploited by other parties or hackers. At the same time, the open network environment makes handling data integrity and privacy crucial (Sun et al., 2024).

The traditional healthcare system is prone to data breaches, where in 2014, there was a cyberattack on US Health Insurer Anthem, where 80 million people's data was stolen. It also mentions the 2019 HIPAA breaches, where 34.9 million US citizens' protected health information was compromised. The research emphasizes the importance of healthcare data being protected from unauthorized access and manipulation (Tariq et al., 2020). According to the Karunarathne et al. (2021) Aruba Research Agency stated that security breaches related to the IoT devices exceeded 84% in 2019 because of their design using low energy, limited processing, storage capacity, and lack of user friendliness, making the complex for an engineer to focus on the security matters.

The healthcare industry has revolutionized, starting from early stages in healthcare 1.0, where they used manual records, and currently the healthcare industry is in healthcare 4.0, which is using cloud computing (CC), fog computing (FC), IoT devices, and telehealth care technologies to share technology. However, the use of secure techniques in healthcare 4.0, which is challenging, also leads to data breaches of patient data, which hackers can gain access to the user account and record without authorization (Hathaliya & Tanwar, 2020).

3. IoT Related Data Breaches and Privacy Issues

3.1. IoT Application in Healthcare

The IoT devices has changed existing traditional methods in healthcare into smart devices to assist the user in collecting the required information for easy decision-making processes (Ahmad et al., 2023). The H-IoT platform plays a significant role in healthcare applications by enhancing the monitoring of the patient, decision making, and optimizing healthcare services. The key application can be described as follows:

a. Remote Patient Monitoring (RPM): Continuous monitoring can be done using the RPM for health signs such as blood pressure, heart rate, and glucose levels, providing timely efficiency and reducing hospital visits and appointments to help, especially the elderly and chronically ill patients (Parihar et al., 2024). The monitoring of patients will also trigger vital signs using wearable devices and sensors (Kumar et al., 2023).

b. Wearable Devices: Collect and transmit health data in real-time monitoring, providing insight into patient healthcare and self-proactive care. They can use devices, such as smartwatches and fitness trackers, for personal use (Parihar et al., 2024).

c. Smart Pill Dispensers: The use of this device is to ensure patients take the medication on time by sending reminders and alerts, reducing non-compliance in medication intake, therefore improving health outcomes (Parihar et al., 2024).

d. Smart Medical Devices: IoT devices integrate with medical devices such as glucose meters and ECG monitors to collect and analyze patient data (Parihar et al., 2024).

e. Equipment and Drug Tracking: Help in tracking medical equipment and medication that can assist healthcare businesses, such as proper usage of medicine, reducing cost with lost or expired items (Parihar et al., 2024). It can also help manage drug supply chain management (Khan et al., 2024).

f. Ambulance Telemetry: Medical intervention during transport of an ambulance to the hospital can be taken in real-time (Parihar et al., 2024).

g. Data Analytics and Automation: IoT devices leverage data analytics and machine learning to process and analyze the health data, improving patient health care. Machine learning can assist in protecting the healthcare infrastructure from cyber threats (Khatun et al., 2023; Parihar et al., 2024). It can also use big data to predict patient visits, disease progression, and treatment outcomes (Parihar et al., 2024). It can also help the healthcare provider to do clinical research (Khan et al., 2024).

h. Electronic Health Records (EHR): Digitized patient records that improve data accessibility and reduce paperwork (Kumar et al., 2023). It can also secure the sharing of medical records and patient data management, payment, and insurance (Khan et al., 2024).

i Real-Time Alerting: Immediate notifications to healthcare providers about significant changes in patients' health status (Kumar et al., 2023).

j. Tele-Healthcare: Remote delivery of healthcare services, reducing the need for hospital visits (Kumar et al., 2023).

k. Medical Imaging: Enhanced data analysis and storage of medical images using big data techniques.

IoT-enabled homes are increasingly used for smart healthcare, integrating digital healthcare facilities with edge devices and wearable technologies (Popoola et al., 2024). In IoT-based healthcare systems, for example, the use of wearable sensors to collect bio-signals from patients and transmit data to cloud servers. As a result,

medical professionals can access this data via mobile applications or internet browsers, improving work efficiency and addressing the shortage of medical personnel. Using edge computing and FC can enhance the security of healthcare IoT systems by enabling real-time data processing and reducing latency (Hathaliya & Tanwar, 2020; Nguyen et al., 2024).

IoT in healthcare generates large amounts of health data and is required for secure and efficient management (Tariq et al., 2020). IoT technology requires a network of physical objects, a communication protocol, and sensors that collect and transmit data. Key components in IoT technology include devices or sensors, connectivity, cloud, and applications.

3.2. Data Breaches and Privacy Risk in IoT Healthcare Systems

H-IoT systems generate large amounts of data used which can be exposed to data breaches and unauthorized access by third parties, leading to severe consequences for patient privacy, healthcare providers, insurance companies, vendors, and compliance with regulatory frameworks. H-IoT technology connects physical devices to the internet using protocols like Constrained Application Protocol (COAP), Message Queuing Telemetry Transport (MQTT), Zigbee, and Bluetooth to increase productivity, decrease expenses, and enhance user experience. IoT devices also face security risks due to their decentralized nature. The separation of data provided by healthcare and the complexity of the healthcare system make it challenging to ensure data privacy (Ahmad et al., 2023).

The use of IoT devices also introduces new vulnerabilities and complexities affecting the healthcare data management landscape. In addition, traditional security measures used by the organization, which are dynamically changing, are hard to equip against novel threats and the increasing data collection by IoT devices. The sophisticated threats make the security of healthcare data and privacy hard to detect and mitigate, necessitating for more resilient and adaptive security framework (Dahiya et al., 2024).

The advancement of IoT technology in healthcare brings four ethical issues such as data privacy, consent, algorithmic fairness, regulatory compliance, and ethical design. Wearable devices and telemedicine, for instance, collect large amounts of personal health data, raising concerns about privacy and security, especially in data breaches, unauthorized access, and data ownership (Wakili & Bakkali, 2025).

Patients are also concerned with the privacy health health-related data in healthcare 4.0 using cloud and FC, which involves third parties and service providers (Hathaliya & Tanwar, 2020). The use of this technology, using open access like the internet, can potentially be exploited by hackers if the security techniques are not properly handled. It can cause the stakeholders and patients to lack trust in the respective system.

Privacy challenges in IoT-based healthcare are discussed in the collection of sensitive patient data, where it can be shared across multiple devices, systems, and healthcare providers. For example, fitness trackers that collect data on user habits and sleep patterns make it possible to infer sensitive health information. Researchers also mention the lack of transparency and control for data sharing because a user may overlook and not be aware of how their data is being used or shared with

healthcare providers without their consent. IoT in healthcare also uses unsecured communication to transfer data, leading to privacy risk and data breaches. It is because possible data may be intercepted and potentially exposed to sensitive patient information. The data can also possibly be used for discriminatory purposes, such as genetic data that could discriminate against patients. For example, insurance companies may use it to counter the patient's request for their covered disease without patient consent (Parihar et al., 2024).

3.3. Possible attacks, vulnerabilities, and weaknesses

IoT devices are vulnerable to security and privacy exploits due to their operating environment. In this section, the possible attacks, vulnerabilities, and weaknesses in the IoT devices, focusing on healthcare, are introduced. IoT applications have their limitations, such as a lack of security, high latency, energy inefficiency, and centralized data storage. However, with the integration of edge computing with blockchain into IoT devices, it is proposed to address the limitation (Nguyen et al., 2024). Traditional IT and existing IoT security methods are currently overlooked, such as complex intercommunication, dynamic system change, and resource constraints (Beyrouti et al., 2024).

Based on the Beyrouti et al. (2024) The case study evaluates the critical vulnerability regarding privacy issues, including insufficient privacy protection (OWASP Category C6), which the IoT ecosystem may be used insecurely, improperly handled, and accessed without permission. Specific Critical Weakness (CWE) focuses on IoT devices, which are CWE-359 (Exposure of Sensitive Information to an Unauthorized Actor) and CWE-200 (Exposure of Sensitive Information), due to the exposed vulnerabilities in IoT systems are also highlighted as related to privacy issues.

According to the Parihar et al. (2024) IoT devices operate using certain protocols and wireless state make them vulnerable to interception and attacks such as Men-In-The-Middle (MitM) and botnet attacks, leading to misuse. The threats that affect privacy concern such as:

a. Perception layer: In the perception layer, threats are also vulnerable to physical attack, impersonation, service denials, and routing attacks. Attackers can tamper with sensors, inject malicious code, and use fake identities to gain unauthorized access to the data.

b. Transportation layer: During the transportation layer, this layer is also probably causing routing attacks, denial of service, and data transit attacks. It can also lead to a breach of patient data, causing compromised data during transit.

c. Application layer issues: It is related to the end user and computing data. It faces risks such as data leakage, denial of service, and malicious code injection. Unauthorized access at this level can lead to breaches of the patient’s privacy.

d. Public Network Exposure: The use of public networks can increase the risk of data interception. The attackers can also get remote access to stored data and compromise patient information if any malicious software is used.

e. Profile Creation and Consent: The awareness of exposing and giving data is given by the public without notifying the importance of protecting their data.

This willingly offered data can bring organization for credit analysis, leading to a privacy violation.

f. Ethical concerns: Service providers and data analysts should handle data in a proper ethical manner. Mental health facilities are one of the high-risk areas; the misuse of sensitive data can affect and have consequences for the patients.

Privacy and data breach issues are also mentioned by the Sun et al. (2024) can be described as follows:

a. Smart Homes: Smart home devices store and use personal data such as private information, including fingerprints, passwords for authentication, and daily life data. The lack of privacy data usage standards and awareness of privacy protection leads to serious privacy data leakage.

b. Intelligent Healthcare: Medical IoT devices collect and share extensive user privacy information with other medical units, increasing the risk of data breaches. Protecting this data and monitoring device operations in real-time is crucial.

c. Data Security Mechanisms: IoT operating systems must implement robust data security mechanisms, including data confidentiality and data integrity protection. Methods used, such as lightweight encryption schemes and access control, are required to prevent unauthorized access and data breaches. Encryption protects patient data from unauthorized access. Using TLS and SSL can secure the data of healthcare organizations (Obaid & Salman, 2022).

d. Network Safety Maintenance: Anti-firewall technologies and secure communication protocols like IPSec are necessary to protect the security of the data during transmission and prevent unauthorized access and interception from third parties.

e. Memory Management Security: Memory management security can be enhanced through technologies such as Stack Guard, NoExecute bit (NX), and Address Space Layout Recommendation (ASLR), which can prevent buffer overflow attacks and protect existing sensitive data.

f. Isolated Storage: The use of sensitive data is gradually increasing, which brings privacy and security issues to the user. Secure storage strategies are vital for protecting sensitive data on IoT devices. Platforms such as Trusted execution environments (TEEs) provide a secure platform for the trust chain, and hardware-based security measures can further enhance data protection.

Healthcare data also exposes itself to the threat, which is that the data is difficult to access, change, or store without authorization and consent (Said, 2022). In other research, according to the Javed et al. (2022) in IoT-based healthcare systems, there are also security issues mentioned, such as:

a. Node Capturing: IoT nodes can be hacked and control the IoT system, leading to a data breach.

b. Malicious code injection attack: Injecting malicious code into the nodes will allow the IoT devices to be monitored and controlled by hackers.

c. False Data Injection Attack: Nodes can be controlled by hackers to generate fake results, causing system failures and data integrity issues.

d. Side-Channel Attacks: Attackers can control nodes by passing them to third parties, compromising privacy.

e. Eavesdropping and Interference: Attackers can capture data during data transfer and processing, leading to data theft. According to Kritik J G Nivedh T S et al. (2022) highlights vulnerabilities in data transmission from IoT sensor devices to network routers, leaving room for intruders to misuse sensitive information.

f. Phishing Attack: Attackers can exploit IoT devices to access with minimal effort.

g. Access Attack: An individual can access IoT devices by gaining access to the same network and stealing critical information.

h. Data Transit Attack: Stealing data by attackers during transfer from one location to another.

i. Routing Attacks: Malicious nodes can alter data paths, leading to a data breach.

j. Data theft: Acquire user data through various stages. The incident can lead to a data breach.

k. Sniffing attacks: Attackers monitor network activities and steal sensitive data.

l. Reprogram Attack: Attackers reprogram IoT devices due to insecure programming practices.

In addition, the researcher also mentions that the centralized system faces significant problems, such as a single point of failure (SPOF), where it is vulnerable to cyberattacks and other failures, leading to data breaches. The cases related to the accidental data exposures in October 2017, exposure of 47GB of patient data in an Amazon Database affecting 150,000 patients, highlight the risk of this centralized system. The use of Remote Patient Monitoring (RPM) led to data breaches and privacy issues because of data generation continuing to increase, centralized data storage, which created SPOF, data transmission vulnerabilities such as interception, modification, or loss, lack of robust security measures, resource constraints, and lack of anonymity and privacy concerns (Dwivedi et al., 2019).

Privacy requirements also arise because of different healthcare infrastructures running with non-standardization of devices. Big data is also one of the issues in which data integrity can impact the accuracy and consistency of the training model in prediction for training diagnosis and treatment (Ahmad et al., 2023). The threats, such as unauthorized access or disclosure, are caused by inadequate security controls, malicious attacks, and human error. In another way, data breaches in the industry, such as the anthem data breaches, including third-party vendors and service providers, which act as an insider threat, pose patient to a privacy risk. Using mobile devices and remote access technology also exposes the patient to privacy risk. Patient data can be threatened by inadequate data anonymization or de-identification because, for research or other purposes, the data should be anonymized to prevent others from knowing the data's actual is. If not, the privacy data will be exposed. Cyber criminals can also use many methods, such as phishing

emails, malware, or social engineering, to access the healthcare system (Obaid & Salman, 2022).

The Karunarathne et al. (2021) mention based on their research, there are still unresolved areas such as handling extensive data, third-party sharing, and the need for robust wireless connectivity solutions. Hence, wearable wireless sensor networks (WWSN) in healthcare highlight data breaches and security concerns on interception and manipulation of the data during transmission, lack of awareness, weak regulation, and inconsistencies, which can cause data breaches. This research also mentions that by using a public blockchain it can also be vulnerable, which can cause the data to be lost or compromised during transmission. Fig. 1 shows possible attacks in the application layer, communication layer, and physical layer, which will affect the cybersecurity of the healthcare system.

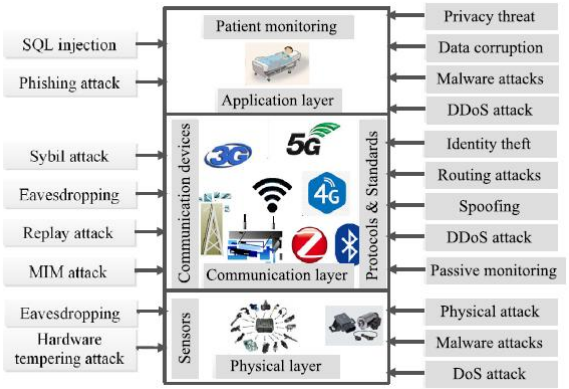

Fig. 1. Possible attack in different layers (Source: Karunarathne et al., 2021)

3.4. Solution and Mitigation

The increasing number of IoT devices in smart homes has led to increasing privacy threats and attacks. It highlights the need for privacy protection through the data management value chain, including data acquisition, processing, storage, and usage (Popoola et al., 2024). One of the requirements of 6G XR in the Ahmad et al. (2023) research is a privacy solution at different data interfaces, following privacy regulations such as HIPAA, and a privacy solution by design.

In previous work, the researchers Dahiya et al. (2024) had proposed blockchain as a solution to address these challenges. To mitigate the risks of data breaches and unauthorized access, the nature of this solution can provide a decentralized nature, immutability, and consensus-driven operation for ensuring data integrity, access control, and transparency. Blockchain can manage healthcare data by ensuring data integrity, privacy, and resilience against attacks. It can also improve data sharing, interoperability, and patient data ownership, as it reduces the risk of data breaches in ensuring data integrity and privacy (Tariq et al., 2020). Blockchain technology and implementation consensus mechanisms must be used to enforce data integrity, although it brings a performance challenge (Ahmad et al., 2023). Blockchain-based decentralization architecture can enhance security and privacy issues related to the healthcare 4.0 (Hathaliya & Tanwar, 2020). Table 1 shows the use of the blockchain concept in data privacy.

Table 1. Blockchain concept in data privacy

Component	Description
Smart Contracts	Automating access control and data processing can prevent unauthorized access and potential data breaches.
Encryption and data integrity	Ensure that patient data is securely logged and immutable once recorded, hence protecting it from tampering and breaches. Advanced Encryption Techniques and zero-knowledge proof enable sharing without exposing actual data, preserving privacy, during the data processing.
Identity Management	Decentralized identity verification mechanism.

According to the Popoola et al. (2024), Reviews existing solutions such as lightweight cryptographic algorithms, secure data storage, and fine-grained access control using smart contracts. It emphasizes the need for a combination of IoT device security techniques and blockchain to achieve privacy preservation. In other research, according to Madanian et al. (2024) There are also mitigation strategies recommended by the researchers, such as using encryption data at all layers, implementing strong access control, regular updates with the latest security patches, and training and awareness for the end users. Karunarathne et al. (2021) The review covers technologies such as blockchain, fog computing, and lightweight authentication schemes that can enhance existing security. To address this risk Obaid & Salman (2022) mention about the importance of encryption, access controls, and consent management.

Karunarathne et al. (2021) proposes several frameworks and technologies to mitigate these challenges, including blockchain technology, differential privacy, and AI/ML for detecting and mitigating vulnerabilities. It emphasizes the need for standardized security and privacy protocols and the importance of integrating these measures from the start. Hathaliya & Tanwar (2020) highlights to defend the network attacks from an adversary because of the open network, the researcher recommended using a cryptography algorithm.

Healthcare organizations should provide regular training to their employees related to the best privacy and data management practices, as well as establish a clear security policy to protect their data (Obaid & Salman, 2022). They must have an awareness to develop patient best practices into the culture. It is continuous because human error and lack of awareness are subjective due to the employees' keep changes, and probably, they will keep making mistakes.

Another technology can be used to ensure the security of the data; homomorphic encryption can allow the computation to be conducted during the encryption without decrypting it. So, it can protect from the privacy being compromised. Technology such as data loss prevention (DLP), intrusion detection prevention system (IDPS), and secure storage solutions is developed to address these privacy and data breach issues (Obaid & Salman, 2022).

In addition, Obaid & Salman (2022) highlight that security devices such as Firewalls, IDS, IPS, and endpoint security technology, such as anti-virus software and malware protection, can protect the ICT infrastructure from cyber threats,

especially causing privacy risk and data breaches. Privacy technology for IoT-based technologies, such as pseudonymization, involves replacing identifiable information while preserving data integrity. Another privacy technology, such as Data masking, which alters data values to hide sensitive information while preserving data integrity. Privacy Enhancing Technology (PET) involves obfuscating data in various ways to protect patient privacy while allowing data analysis.

The evaluation by Wakili & Bakkali (2025) of the solution including cryptography, blockchain, machine learning, and fog edge computing which the summary of the evaluation can be summarized as follows:

a. Cryptography: Offers high security but faces scalability and efficiency challenges.
b. Blockchain: Decentralization and robustness, but struggles with efficiency and energy consumption.
c. Machine Learning: Provides high performance and adaptability but raises privacy concerns.
d. FC/Edge Computing: Delivers low-latency processing and high scalability, but can be complex and costly to manage.

4. Discussion

4.1. Research Challenges

The adoption of IoT technology presents challenges that are facing in healthcare extend beyond the technological challenges. One of the challenges faced by the patients is that they didn't know where the data was being used and shared because of a lack of transparency, hence leading to trust issues with the devices themselves. IoT devices face resource constraints such as limited processing power, storage capacity, and SPOF, where implementing high security features is challenging.

Challenges also include ensuring data privacy, interoperability, fault tolerance, and the integrity of healthcare big data. The complexity of the system and lack of standard use also introduce the vulnerability of the infrastructure itself. The ongoing issues that need to be addressed are mentioned by the Hathaliya & Tanwar (2020) are ethical challenges, user authentication, data ownership, and data protection policies are highlighted in the research.

IoT devices generate and share data across interconnected systems, making them vulnerable to data breaches and exploitation. In addition, it can provide security challenges because IoT devices generate large amounts of data that expose them to attackers, who can launch various security attacks (Hathaliya & Tanwar, 2020). The IoT data, which can be accessed through the cloud server, is potentially vulnerable the data breaches and unauthorized access by attackers.

In summary, challenges that are faced when implementing IoT technology in healthcare can be described as follows:

a. Ethical challenges: Some ethical challenges, like data privacy, data access control, are key elements to ensure the exchange of information and data flow

that can obstruct the operation. Data privacy is important because of large amount of data is shared, our data needs to be protected, and if not managed in the right way will cause a data breach and be used by another party.

b. Lack of standardization and interoperability between IoT devices and systems: As more IoT devices are produced from various sources and standards, it is more challenging to keep devices and data privacy secure. We can see that the IoT devices act as an embedded system which have dedicated tasking for a specific purpose. Lack of resources in terms of memory and processing affects the security implementation to the devices which require to implement necessary security features for the respective devices.

c. Unauthorized access: Only authorized users can access patient personal information. However, the attacker can still access patient information by identifying the vulnerability in the IoT devices to access it. It is also difficult to verify unauthorized access when the malware or injection is persistent. Some of the IoT devices can also be a victim of the adversary, as the devices are part of zombie devices that are used to attack other devices by using their resources

d. Shortage of cybersecurity practice and privacy experts in the healthcare industry: Short of expertise causes the devices in the healthcare is hard to maintain devices, making the data vulnerable to cyberattacks and breaches. The IoT devices require maintaining the updated features as well as the security features that need to be implemented by having the necessary features to implement them.

e. Data Protection Policies: The healthcare data, such as diagnosis, needs for security protection, and strict administration. Security of the data is a priority where the data cannot be altered or lost to ensure the integrity, so that doctors can use accurate data to analyze, diagnose, and predict consequences of the patient's health.

f. Advancement of the technology on privacy and AI: Security and privacy technologies must continually develop and enhance to keep update with the new threats and vulnerabilities/weaknesses. AI technology can assist in protecting the privacy of patient data in real time (Obaid & Salman, 2022). The data can be used by AI ethically and with the user's consent to give information and suggest to the doctor to conduct a diagnosis and check the patients. The doctor needs to be responsible for the decisions they have made because the AI cannot replace humans in terms of decision-making.

4.2. Future Directions

The rapid evolution of IoT technology in healthcare offers transformative potential, but its deployment also introduces complex challenges related to privacy, security, and system efficiency. To address these issues, the following future directions are proposed:

a. Standardization of Security Protocols and framework: The lack of universal security standards for IoT technology for healthcare systems makes interoperability challenging and increases vulnerabilities. Future research should focus on developing globally accepted frameworks, such as integrating

ISO/IEC 27001 with healthcare-specific standards like HIPAA, to create robust security protocols tailored to IoT device environments.

b. Blockchain Integration: Blockchain technology holds promises for enhancing data integrity, privacy, and decentralized control in IoT technology for healthcare systems. Future studies should explore novel consensus mechanisms that reduce computational overhead while maintaining security, enabling scalable blockchain adoption in resource-constrained IoT devices.

c. Federated Learning for Privacy Preservation: The adoption of federated learning models can help mitigate privacy concerns by allowing decentralized training of machine learning models across multiple IoT devices without sharing raw data. Future research should enhance these models to improve their robustness against adversarial attacks.

d. Quantum-Resistant Encryption: The advent of quantum computing poses a significant threat to traditional encryption methods. Developing and implementing quantum-resistant encryption algorithms for IoT technology for healthcare systems is essential to future-proof these systems against emerging cryptographic vulnerabilities. It is also important for the IoT to use lightweight encryption because of its limited capabilities.

e. AI-Driven Threat Detection: AI and ML can significantly enhance the detection and mitigation of IoT-specific threats. Future work should focus on developing adaptive AI-driven systems capable of identifying anomalies in real-time, reducing response times to security breaches.

f. Technology Analytics: Reviewing new technology is required as our technology keeps emerging, and advancements need us to prepare for any consequences and threats. In another research by Ahmad et al. (2023), there is a lack of reviews focusing on Big 6 G-based data analytics and DL for healthcare services provisioning. Existing literature often relies on 5G characteristics, and there is a need for real-time implementation using actual 6G environments.

g. Edge and FC: Incorporating edge and FC can enhance the real-time processing capabilities of IoT systems while reducing latency and dependency on centralized cloud infrastructures. Future research should explore optimized architectures for integrating these computing with IoT technology for healthcare systems.

h. Ethical and Regulatory Enhancements: As IoT technology in healthcare grows, addressing ethical issues such as data ownership, informed consent, and algorithmic fairness becomes critical. Future initiatives should aim to align technological advancements with evolving regulatory frameworks, ensuring compliance and fostering trust among stakeholders.

i. Privacy Enhancing Technologies (PET): PET, including homomorphic encryption, should be further explored for their potential to protect sensitive patient data. Future research should focus on their scalability and applicability in IoT technology ecosystems with constrained resources.

j. Resilience Against Sophisticated Threats: As cyberattacks become increasingly sophisticated, developing IoT systems with built-in resilience to threats like ransomware, insider threats, and distributed denial-of-service (DDoS) attacks will be crucial. Proactive threat modeling and penetration testing can help anticipate and mitigate such risks.

k. Collaborative Frameworks for IoT Security: Establishing collaborative frameworks among governments, industries, and academia can drive innovation in securing IoT technology in healthcare systems. Joint initiatives can focus on knowledge sharing, research funding, and developing open-source solutions for common challenges.

By addressing these future directions, the IoT technology for healthcare ecosystem can be optimized to deliver secure, efficient, and privacy-preserving solutions that benefit patients, healthcare providers, and stakeholders alike.

5. Conclusion

IoT technology has transformed the healthcare landscape in healthcare 4.0 by enabling real-time monitoring, predictive analytics, and enhanced patient care. However, its limited resources and extensive data handling capabilities introduce substantial risks to privacy and security. This review identified critical vulnerabilities and weaknesses in IoT healthcare systems, such as unauthorized access, data breaches, and inadequate privacy safeguards. Advanced technologies such as blockchain, federated learning, access control, and AI-driven solutions show how the implementation of this technology can assist in addressing these challenges. Despite these advancements, significant gaps remain, including a lack of global standards, resource limitations in IoT devices, and the need for scalable security solutions. Future efforts should prioritize the development of standardized frameworks, robust encryption methods with a minimum requirement of IoT devices, and privacy-preserving technologies to ensure the secure deployment of IoT in healthcare. By mitigating privacy risks and enhancing data security measures, healthcare organizations can build trust with patients and stakeholders, ensuring the safe and efficient use of IoT technologies. This study lays the groundwork for future research and development to safeguard IoT-enabled healthcare systems against emerging threats, particularly in terms of privacy risks and data breaches.

Acknowledgement

The authors acknowledge the Universiti Teknologi Malaysia (UTM), Kuala Lumpur campus, for giving the authors guidance, support, and facilities to accomplish this paper.

Conflicts of Interest

The author declares that there is no conflict of interest regarding the publication of this paper.

References

[1] Ahmad, H. F., Rafique, W., Rasool, R. U., Alhumam, A., Anwar, Z., & Qadir, J. (2023). Leveraging 6G, extended reality, and IoT big data analytics for healthcare: A review. In Computer Science Review (Vol. 48). Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2023.100558

[2] Aski, V. J., Dhaka, V. S., Parashar, A., kumar, S., & Rida, I. (2023). Internet of Things in healthcare: A survey on protocol standards, enabling technologies, WBAN architectures, and open issues. Physical Communication, 60. https://doi.org/10.1016/j.phycom.2023.102103

[3] Beyrouti, M., Lounis, A., Lussier, B., Bouabdallah, A., & Samhat, A. E. (2024). Vulnerability-oriented risk identification framework for IoT risk assessment. Internet of Things (Netherlands), 27. https://doi.org/10.1016/j.iot.2024.101333

[4] Dahiya, R., Samal, L., Samal, D., Kumar, J., Sharma, V., Kumar Sahni, D., & Singh Bhati, N. (2024). A Blockchain-Based Security system framework in the Healthcare Domain using IoT. In J. Electrical Systems (Vol. 20, Issue 3).

[5] Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. Sensors (Switzerland), 19(2). https://doi.org/10.3390/s19020326

[6] Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. In Computer Communications (Vol. 153, pp. 311–335). Elsevier B.V. https://doi.org/10.1016/j.comcom.2020.02.018

[7] Javed, L., Yakubu, B. M., Waleed, M., Khaliq, Z., Suleiman, A. B., & Mato, N. G. (2022). BHC-IoT: A Survey on Healthcare IoT Security Issues and Blockchain-Based Solution. International Journal of Electrical and Computer Engineering Research, 2(4), 1–9. https://doi.org/10.53375/ijecer.2022.302

[8] Karunarathne, S. M., Saxena, N., & Khan, M. K. (2021). Security and Privacy in IoT Smart Healthcare. IEEE Internet Computing, 25(4), 37–48. https://doi.org/10.1109/MIC.2021.3051675

[9] Khan, I., Majib, Y., Ullah, R., & Rana, O. (2024). Blockchain Applications for Internet of Things - A Survey. In Internet of Things (Netherlands) (Vol. 27). Elsevier B.V. https://doi.org/10.1016/j.iot.2024.101254

[10] Khatun, M. A., Memon, S. F., Eising, C., & Dhirani, L. L. (2023). Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation. IEEE Access, 11, 145869–145896. https://doi.org/10.1109/ACCESS.2023.3346320

[11] Kritik J G Nivedh T S, Siva Bharath S, Dr. Radhamani.A.S., & Mr. V. Ramanathan. (2022). Data Security in Healthcare using IoT. IJEAST, 3, 79–82. https://doi.org/10.1109/ACCESS.2015.2437951

[12] Kumar, M., Kumar, A., Verma, S., Bhattacharya, P., Ghimire, D., Kim, S. H., & Hosen, A. S. M. S. (2023). Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues. In Electronics (Switzerland) (Vol. 12, Issue 9). MDPI. https://doi.org/10.3390/electronics12092050

[13] Madanian, S., Chinbat, T., Subasinghage, M., Airehrour, D., Hassandoust, F., & Yongchareon, S. (2024). Health IoT Threats: Survey of Risks and Vulnerabilities. In Future Internet (Vol. 16, Issue 11). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/fi16110389

[14] Nguyen, T., Nguyen, H., & Nguyen Gia, T. (2024). Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications. In Journal of Network and Computer Applications (Vol. 226). Academic Press. https://doi.org/10.1016/j.jnca.2024.103884

[15] Obaid, O. I., & Salman, S. A.-B. (2022). Security and Privacy in IoT-based Healthcare Systems: A Review. Mesopotamian Journal of Computer Science, 29–40. https://doi.org/10.58496/mjcsc/2022/007

[16] Parihar, A., Prajapati, J. B., Prajapati, B. G., Trambadiya, B., Thakkar, A., & Engineer, P. (2024). Role of IOT in healthcare: Applications, security & privacy concerns. In Intelligent Pharmacy. KeAi Publishing Communications Ltd. https://doi.org/10.1016/j.ipha.2024.01.003

[17] Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2024). A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: Problems, challenges and solutions. Blockchain: Research and Applications, 5(2). https://doi.org/10.1016/j.bcra.2023.100178

[18] Rathee, G., Sharma, A., Saini, H., Kumar, R., & Iqbal, R. (2020). A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimedia Tools and Applications, 79(15–16), 9711–9733. https://doi.org/10.1007/s11042-019-07835-3

[19] Said, O. (2022). LBSS: A Lightweight Blockchain-Based Security Scheme for IoT-Enabled Healthcare Environment. Sensors, 22(20). https://doi.org/10.3390/s22207948

[20] Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data Protection and Privacy of the Internet of Healthcare Things (IoHTs). In Applied Sciences (Switzerland) (Vol. 12, Issue 4). MDPI. https://doi.org/10.3390/app12041927

[21] Sun, P., Wan, Y., Wu, Z., & Fang, Z. (2024). A survey on security issues in IoT operating systems. In Journal of Network and Computer Applications (Vol. 231). Academic Press. https://doi.org/10.1016/j.jnca.2024.103976

[22] Tahir, M., Sardaraz, M., Muhammad, S., & Khan, M. S. (2020). A lightweight authentication and authorization framework for blockchain-enabled IoT network in health informatics. Sustainability (Switzerland), 12(17). https://doi.org/10.3390/SU12176960

[23] Tariq, N., Qamar, A., Asim, M., & Khan, F. A. (2020). Blockchain and smart healthcare security: A survey. Procedia Computer Science, 175, 615–620. https://doi.org/10.1016/j.procs.2020.07.089

[24] Wakili, A., & Bakkali, S. (2024). Internet of Things in healthcare: An adaptive ethical framework for IoT in digital health. Clinical E-Health, 7, 92–105. https://doi.org/10.1016/j.ceh.2024.07.001

[25] Wakili, A., & Bakkali, S. (2025). Privacy-preserving security of IoT networks: A comparative analysis of methods and applications. Cyber Security and Applications, 3, 100084. https://doi.org/10.1016/j.csa.2025.100084