ISSN: 2182-2069 / E-ISSN: 2182-2077

Enhancing Security and Privacy in AI-Enabled IoT Smart Healthcare Devices: Practical Solutions for Protecting Patient Data

Baha Eldin Hamouda[1*]

[1*]Assistant Professor, Department of Information Technology, Gulf Colleges, Hafar Al-Batin, Saudi Arabia. bahahamouda@yahoo.com; bhh@gulf.edu.sa, https://orcid.org/0000-0001-5010-9635

Received: April 07, 2025; Revised: May 20, 2025; Accepted: July 10, 2025; Published: August 30, 2025

Abstract

The use of IoT devices in patient care systems is witnessing a surge. However, there are new security and privacy concerns. This paper addresses these challenges by assessing the security and privacy risks posed by healthcare IoT devices. It also offers a comprehensive framework to enhance their security. The emphasis here is placed on critical elements of security: data management, the secure transmission of data, the protection of privacy, and integrity within systems in healthcare IoT environments. The proposed solutions in the paper include some very practical measures such as data encryption, secure communication protocols, lightweight authentication, role-based access control, two-factor authentication, intrusion detection systems, and privacy-preserving data analytics. The paper also talks about how blockchain technology could help keep data safe and make it easier to verify things without a central authority. We include a case study on remote patient monitoring (RPM) to demonstrate the practical application of the framework. This case study shows how to protect patient information effectively. The paper discusses ethical concerns regarding patient consent and the proper utilization of data, aiming to reassure the reader about the responsible management of patient information and restore confidence in patients' control over their health data. Finally, the paper discusses limitations of IoT in healthcare, like interoperability issues and resource constraints. In general, this study provides intriguing thoughts and applicable options to ensure IoT healthcare devices' security and safeguard patients' private information within the changing environment of smart healthcare.

Keywords: Internet of Things (IoT), Artificial Intelligence, Smart Healthcare, Security and Privacy, Data Encryption.

1 Introduction

The Internet of Things (IoT), cloud computing, and artificial intelligence (AI) are emerging technologies that have undergone significant evolution and development over the past few years. They have come together to create a new type of healthcare called "smart healthcare." As IoT devices have become more common in healthcare, security and privacy issues have gotten worse (Saba Raoof & Durai, 2022; Jalali & Shaemi, 2015). These devices often handle sensitive patient information, and their intrusion could

Journal of Interner Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 1-17.
DOI: *10.58346/JISIS.2025.I3.001*

*Corresponding author: Assistant Professor, Department of Information Technology, Gulf Colleges, Hafar Al-Batin, Saudi Arabia.

result in substantial privacy violations, severe legal consequences, and a decline in patient trust (Butpheng et al., 2020; Shrivastav & Malakar, 2024).

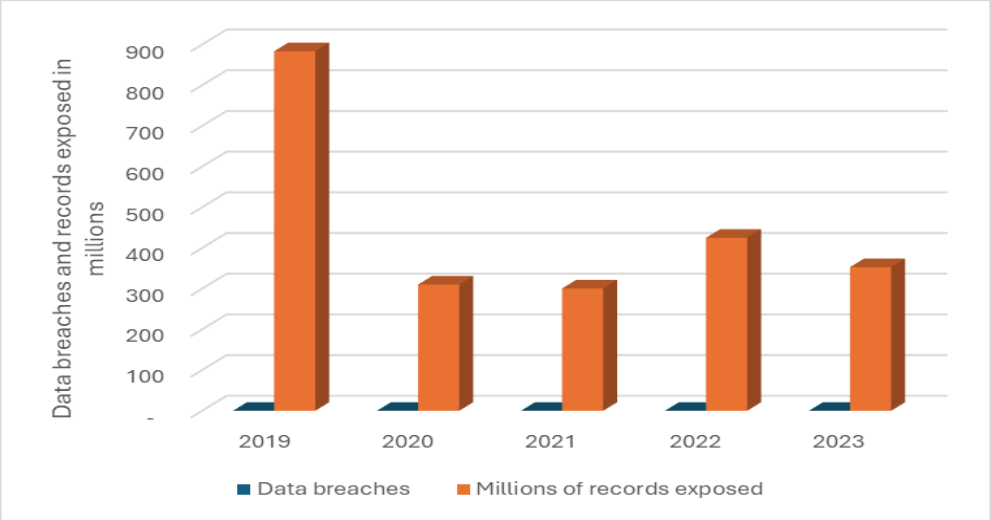


Figure 1: Data Breaches and Records Exposed in Millions from 2019 to 2023

Source: Identify Theft Resource Center. © 2024 Statista.

A flood of opportunities, notably in the field of medical services, has been opened up by the combination of AI and IoT. Medical professionals will be able to give individualized, cost-effective, and high-quality treatment thanks to AI-driven IoT (AIIoT) systems' unique insights into patient-specific data. 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 (Firouzi et al., 2022; Shenoy & Menon, 2021).

The current healthcare IoT systems are generally bound by weak data encryption, inadequate authentication protocols, and constrained computational resources, which might expose them to malicious attacks. Those will also bring concerns around patient consent and data privacy issues, which imply ethical issues demanding stringent security measures (Alshamrani, 2022).

Figure 1 shows yearly information on data breaches, the total number of leaked records, and the volume of exposed records in the healthcare sector from 2019 to 2020. Since 2019, this field has exceeded 1,000 incidents yearly, showing a consistent increasing trend in both the volume of hacked data and the number of events. Often motivated by a focus on utility rather than strong security, this increase coincides with the fast and growing spread of linked devices and digital systems in the healthcare sector. Among the key components fueling this increasing tendency are the general acceptance of Internet of Things devices such as wearables, smart pumps, and remote diagnostic tools. This widening of the attack surface results from many of these devices lacking even the most basic security elements. Apart from inadequate data encryption in old systems, phishing attacks and malware targeted at medical practitioners also cause considerable worry. Older systems lack modern security features, have poor encryption, and apply weak access control rules or encryption inefficiently. There is no common security standard that is applicable to different devices and platforms, which causes the protection to be fragmented, hence increasing the risk of security breaches. The proliferation of AI-driven IoT devices exacerbates the problem as it creates enormous potential for hackers to find a hole in the system and use it without any obstacles; thus, a major security breach may happen. This situation

creates an opportunity for high-tech attacks to be executed, particularly those stemming from insecure APIs and inadequate device authentication. Consequently, there is considerable urgency in searching for security solutions that secure devices, provide human-like threat detection, and carry out data encryption (Sadek et al., 2022).

As researchers and specialists examine AI and IoT applications for healthcare administration, defending persistent information must remain necessary. The consistent integration of AI-driven IoT into healthcare frameworks presents unparalleled openings; in any case, it is inalienably related to maintaining strong security measures and security securities (Wang et al., 2020).

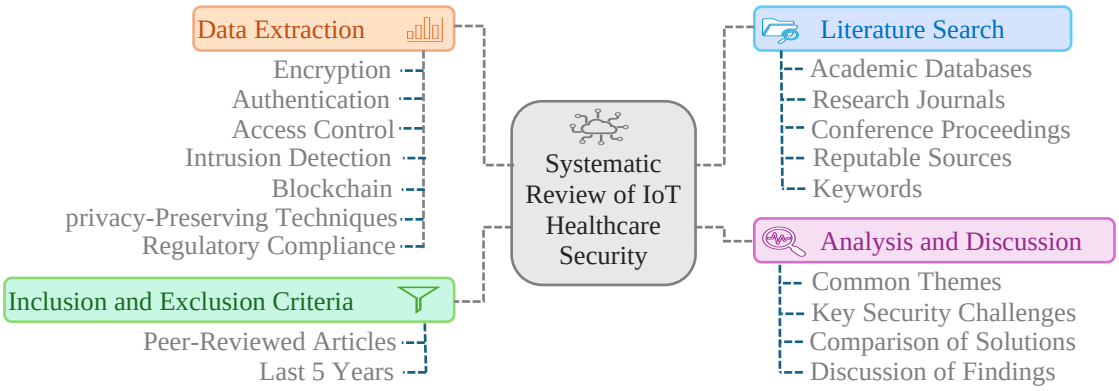
This paper discusses strategies to improve the security and security of AI-enabled IoT shrewd healthcare gadgets by actualizing successful measures to defend understanding information while recognizing the noteworthy positive impact of AI IoT on healthcare through enhancements in analysis, treatment, and quiet care (Raktur & Jea, 2024).

In this context, the most critical issues include security in information transmission, data integrity, cybersecurity, and system verification. It recognizes common-sense arrangements, such as information encryption, lightweight confirmation, role-based access control, and interruption location, that can decrease the probability of unauthorized information access and harm to the privacy of individuals.

This is often all to contribute important knowledge and arrangements to upgrade security and protection in IoT-based healthcare frameworks, making a difference to ensure sensitive, confidential data inside the increasingly interconnected healthcare environment.

2 Methodology

The study adopts a systematic literature review to explore and analyze existing research on securing 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

Figure 2: Systematic Review of IoT Healthcare Security

Figure 2 shows the systematic review process followed by the researchers to evaluate IoT security solutions in the healthcare sector, outlining the research and methodological steps involved, which include:

Literature Search: The study begins with a thorough and systematic search of academic databases, research journals, conference proceedings, and reputable sources. The keywords used for the search include "IoT healthcare security and privacy," "AI-enabled IoT healthcare," "data protection in healthcare IoT," "secure IoT communication," "blockchain 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, blockchain, 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 proposed pragmatic methodology uses remote patient monitoring (RPM) employing AI-enabled IoT devices as its case study. RPM enables wearables and smart sensors to be used by medical providers to remotely monitor patients' health, allowing for individualized and prompt treatments. In the systematic methodology, academic sources are thoroughly examined to comprehend security and privacy issues and suggested fixes in 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.

3 Literature Review

With the rapid proliferation of wireless IoT devices reaching unparalleled numbers already more than 10 billion and are estimated to reach 30 billion by 2026 (Castillo & 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.

The main hurdle in IoT healthcare systems is to handle different security aspects related to data management, data transmission, privacy, and the integrity of the whole system. Since the traditional expectation of trust is no longer valid, the potential for data breaches has become catastrophic, affecting both the reputation and privacy of individuals. If hackers manage to break into IoT medical devices, they will have access to sensitive patient details. Security remains a key issue although, with the rapid expansion of the Internet of Things (IoT) networked devices and their applications, it is now rapidly growing in the healthcare field. And because the healthcare industry is so sensitive, protecting people's private health information and personal data is a real issue (Tawalbeh et al., 2020; Nair & Rao, 2023).

The Internet of Things (IoT)-based framework in healthcare, too, has a set of challenges. In IoT, systems contrast with conventional ones. The security of persistent information and data is a must. Keeping up data secrecy is one of the most prominent challenges in IoT. Transmitting data between different healthcare systems may expose sensitive information (Debebe, 2016). Ensuring the privacy of the patients is also a necessity. The integrity of the data should also be maintained. Unauthorized modifications should not occur to the original data. Failure to do so could result in the use of inappropriate treatment methods or diagnoses. Retaining patients' privacy and data on specific trends fosters global trust in healthcare systems. A healthcare system employs a robust authentication protocol. We will track the data flow between the system and the remote devices (Dang et al., 2019).

The security of IoT healthcare systems is becoming increasingly unreliable due to various types of cyberattacks that jeopardize patient safety. For example, selective-forwarding attacks mess with routing protocols, which makes it harder to provide essential signals on time. Sinkhole attacks change the paths data takes, sending important information to malicious nodes that can be used to get into systems without permission and profile patients (Zhang & Hoshino, 2019). Jamming attacks are a mess with wireless communication, which can cause IoT devices to stop working or act strangely. On the other hand, flooding attacks try to use up a system's resources, making it very hard to send data continually. Phishing assaults worsen these vulnerabilities by focusing on client credentials for unauthorized access to IoT frameworks. Healthcare offices must execute vigorous security measures to address these modern dangers. Scrambling, upgrading, and preparing staff on IoT healthcare apps can make them more secure. Ready to better protect quiet security in a healthcare framework that's developing more associated by bringing out these issues and giving solutions (Wallgren et al., 2013).

IoT healthcare frameworks must address numerous security issues, such as information administration, transmission judgment, security laws, and framework flexibility. Information breaches are a significant concern because they can damage individuals' reputations and compromise patient privacy. In the event that somebody finds imperfections in IoT healthcare gadgets, they can access crucial medical data without authorization. IoT technologies are becoming increasingly common in healthcare, but security remains a significant concern. Such protection is often essential since well-being data is profoundly private and requires rigid security measures to defend individual information and private well-being records (Dang et al., 2019).

Solutions for Ensuring Security in IoT-Enabled Environments

Patient data breaches pose genuine dangers to the security of IoT frameworks utilized in healthcare. Researchers have created different inventive techniques to defend persistent information and keep up protection in reaction to this issue. One viable arrangement is lightweight verification plans utilizing cryptographic hash functions to secure communications (Chacko & Hayajneh, 2018). These plans are made to work with the constrained assets of wearable gadgets while keeping people's personalities and privacy secure (Gupta et al., 2019).

Privacy-protecting information investigation, haze computing, and self-adjusting channels have become important instruments to guarantee that information sent in healthcare IoT frameworks is securely secured (Anantharam et al., 2015). These technologies enable efficient monitoring of healthcare information systems with reduced risks of possible privacy issues.

On this line, blockchain technology has brought a new solution for decentralized authentication to prevent DDoS attacks and maintain confidentiality, integrity, anonymity, and privacy requirements (Akkaoui, 2021). This blockchain-based approach secures IoT healthcare systems and protects sensitive data with the inherent features of blockchain.

Some studies have explored integrating 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 analyze health-related data in the cloud while preserving user privacy. They also introduce safe access control components based on user attributes, achieving high accuracy.

Researchers have proposed advanced learning methods that enable secure data access through searches using homomorphic encryption and secure searchable blockchains. When they examined these access control procedures and compared them with reference models, they found that the proposed

methods significantly enhance user behavior tracking, security, and privacy in blockchain-based IoT systems (Kumar et al., 2022).

We have integrated deep learning techniques with authorized blockchains and smart contracts to create secure data-sharing frameworks (Kute et al., 2021). These models improve the ability to detect attacks by utilizing innovative agreement methods based on contracts and a technique known as self-attention-linked bidirectional short-term memory (SA-BiLSTM).

Other studies have examined the use of IoT-based healthcare systems for addressing security and trust issues. These challenges impact the efficiency of the healthcare system and its long-term outcomes. Researchers are evaluating enhanced encryption strategies that could be applied, as well as a greater level of verification to provide security and trust (Anuradha et al., 2021). These examples guide how to address control, security, intelligence, and verification issues, ensuring the protection and confidentiality of health information.

AES-encryption-decryption methods play a crucial role in ensuring that sensitive patient data is kept secure or that the user is who they claim to be when cloud computing, Internet of Things (IoT)-based cancer detection systems are used (Sharma et al., 2018). Healthcare systems focus on improving computing and processing capacities (Rehman & Manickam, 2017). They keep the doctors and nurses completely safe. The blood data is encoded (Anuradha et al., 2021).

Experts have researched various solutions to fill the security gaps that this patient data breach caused. The latest technologies and cryptographic approaches are being used by researchers to achieve secure, private, and authenticated data in IoT systems that are health-based. New technologies in healthcare are being produced rapidly. Healthcare practitioners can enhance security and ensure the safety of patient information via technology.

4 Key Security Problems in the Healthcare IoT Environment

The following discussion addresses the critical issues that must be considered when protecting patient data in an IoT-enabled scenario for end-to-end encryption (E2E). The information comes from lessons learned based on critical reviews of the body of literature that exists:

Data Management and Transfer Security

Secure encryption to avoid leakage and breach of sensitive data in the healthcare IoT ecosystem. These algorithms must keep the information about the patients confidential and safe when managed and sent. Focusing on these areas can ensure that we bolster the protective measures that safeguard patient data. We must encrypt data both when it's not in use and during transmission. Such encryption should be done by using strong encryption algorithms like AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and SSL (Secure Sockets Layer), etc. Authorized personnel should only have access to encrypted data after safe authentication.

Strong communication protocols should be used to keep the data safe while communicating between IoT device and healthcare systems. For connection-oriented communication, use TLS (Transport Layer Security). DTLS protocols are used as encryption protocols by most organizations. Digital signatures and message authentication codes (MACs) also ensure data accuracy. With the help of these approaches, the person who provided the data will be able to notice the change. The techniques enhance the privacy and accuracy of information shared in health ecosystems.

Unauthorized change detection can be accomplished through various data integrity checks, such as digital signatures or message authentication codes (August & Gewirtz, 2019).

Privacy Protection

It is important to make things private and secret in many areas, such as data anonymization, data pseudonymization, and access limitation. The patients' PII should either be anonymized or pseudonymized to lower the chances of them being re-identified (Butpheng et al., 2020).

Role-based access control (RBAC) ensures that only authorized employees who need to see a particular piece of information can see patients' data (Sharma et al., 2018). Data minimization practices will help mitigate the impact of a data breach by only collecting and holding the information that is actually needed (Neyja et al., 2017).

Device and System Security

It is incumbent on providers to ensure the IoT devices and the systems to which they connect are immune to unauthorized access. It is significantly important to update your software regularly, as it can fix as well as prevent a lot of problems. Also, each IoT device should have its unique ID. A unique ID significantly reduces the likelihood of an unauthorized device accessing the system. Devices that connect to the Internet can be controlled easily. A unique ID serves as the primary security measure (Raza et al., 2013).

Incorporating secure boot processes and hardware-based security features, e.g., Trusted Platform Modules (TPMs), into these basic security features will significantly improve the resilience of these devices. This procedure ensures that only software that has been verified is loaded. This lowers the risk of malware getting into the system. Using SSH (Secure Shell) protocol or VPN (Virtual Private Network) to create a secure communication channel makes it harder for anyone to tap or listen to the data being sent (Kute et al., 2021). SSL can make communication channels secure to protect IoT systems from unauthorized access and potential cyberattacks. It will make the IoT ecosystem overall secure and reliable (Liu et al., 2020).

Authentication and Access Control

Devices must incorporate strong authentication controls, including multi-factor authentication (MFA) and biometric authentication, that validate users and devices before accessing patient data. Password storage should utilize hashing algorithms with salting to prevent unauthorized access to user credentials (Srinivas et al., 2018).

Access policies should specify the intensity or degree of access allowed for users. Occasionally, review your rights and privileges and revoke access from users who no longer need it (Anuradha et al., 2021).

Protection against Various Types of Attacks

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) can be used to protect against these and other attacks in IoT healthcare systems. These actively monitor network traffic or device behavior to identify and prevent suspicious activities and possible threats (Karlof & Wagner, 2003).

Anomaly detection using machine learning can detect anomalous patterns or behavior that may indicate a current attack. Network segmentation can, on top of that, separate critical healthcare devices from non-critical IoT devices, reducing the attack surface (Gope & Sikdar, 2019).

Resource Limitations

Since IoT devices face resource constraints, the framework should be implemented with lightweight cryptographic algorithms and protocols to tame computational overhead (Gope et al., 2019). Another way efficiency can be enhanced is by optimizing data storage and transmission, which will cut the memory and bandwidth needed. The framework shall be regularly assessed to ascertain that the resource utilization of the IoT devices is within acceptable limits (Ul & Manickam, 2017).

By tackling the above-discussed key issues jointly, this proposed framework will provide an exhaustive strategy for patient data protection with an IoT-enabled healthcare system (Sadek et al., 2022). The framework will ensure a secure, privacy-aware environment for innovative medical services with encryption, authentication, access control, and sound security measures. Consequently, patient trust and health data protection will be increased (Alshamrani, 2022).

Proposed Practical Framework to Ensure Data Protection

The proposed security benchmark for IoT architecture targets current security gaps by introducing a comprehensive framework specifically designed for healthcare IoT. This framework prioritizes confidentiality, integrity, access control, and additional security themes to provide robust protection for IoT devices and data.

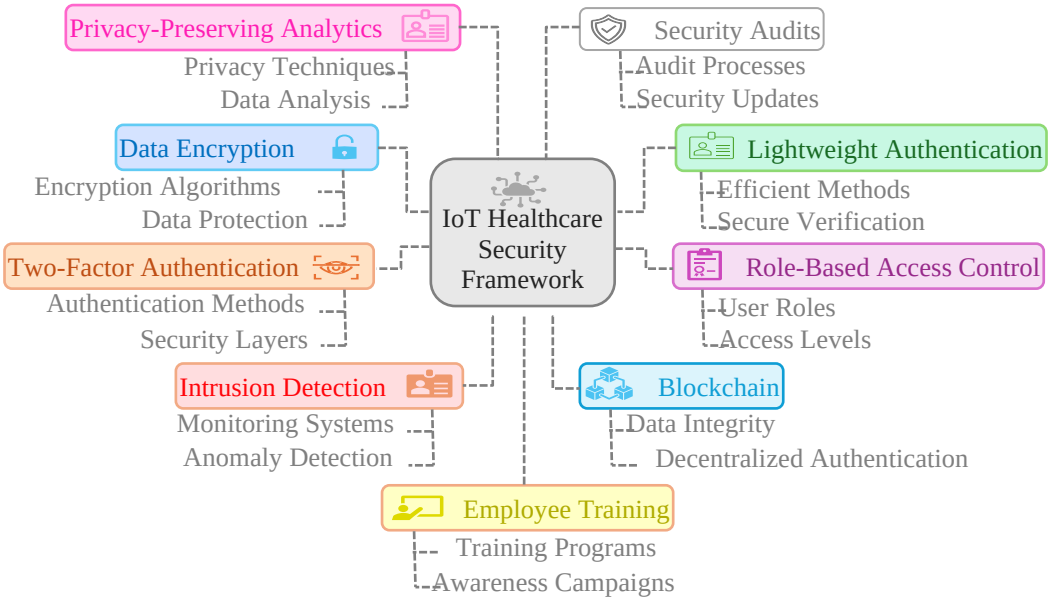


Figure 3: A Proposed Practical Framework for IoT Architecture in Healthcare

Figure 3 introduces a comprehensive and multilevel framework that significantly enhances the security of IoT technology in the medical sector. The framework starts with security concerns for the physical component by highlighting the importance of device verification and coding information. The framework ends with managing who can access the system and identifying any abnormal behavior related to the device, with detection that operates at the system and application levels. This hypothetical

framework, therefore, consists of a device level that can provide protection for innovative medical devices by verifying devices, clear codes, or identifiers for personal devices, and begin to enhance verification. It also has a network level that involves the protection of the network through the foundation of TLS 1.3, a cloud level that uses artificial intelligence to recognize undesirable access and threats, and an application level where access control systems incorporate blockchain.

This broad method connects ways to scale up future technical steps like post-quantum encryption. It balances tight security needs with few resources in medical devices. The setup also gives a changing system for regular security improvements and checks. This offers a complete answer for security problems in new medical settings. Each part of this system was picked carefully to handle the risks linked to it. Table 1 shows the suggested practical plan for IoT data security in healthcare across several key areas. This shows how complete the plan is and how it can handle different security steps.

Moreover, the table stresses the need to create technologies such as blockchain to ensure the integrity of medical records and privacy-preserving data analytics such as differential privacy. While considering practical challenges such as hardware resource constraints and strict privacy requirements, this framework offers multi-layered protection against many security threats in innovative medical environments by means of its integration of strict technical solutions (two-factor authentication, intrusion detection systems) and regulatory measures (employee training, regular updates).

The Key Themes of Our Framework are Briefly Discussed in Table 1

Table 1: Themes for ensuring data protection in IoT-enabled healthcare

Themes	**Explanation**
Data Encryption and Secure Communication	Using industry-standard cryptographic algorithms, such as AES and RSA, to encrypt data of patients, and implement communication security protocols like TLS or DTLS in the data transmission between IoT devices and healthcare servers (Ali et al., 2022).
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 (Gupta et al., 2019).
Role-Based Access Control	Set up a role-based access control system that limits and controls who can see patient data based on their role (for example, doctors, nurses, or patients). The system should have detailed access policies and regular audits to make sure they are up to date.
Two-Factor Authentication	Two-factor authentication (2FA) with physically unclonable functions (PUFs) can be used to make things safer by combining something the user knows (like a password) with something the user owns (like a physical token) (Gope & Sikdar, 2018).
Intrusion Detection and Anomaly Monitoring	For example, more advanced intrusion detection systems (IDS) can measure device behavior, monitor network traffic in greater detail, and assess possible vulnerabilities. To do this, they require advanced anomaly detection algorithms to find anomalous behavior in Internet of Things (IoT) devices and systems (and, more broadly, to reduce risk in connected environments and protect and monitor sensitive data).
Blockchain for Data Integrity	The Blockchain aspect of this system records and maintains the accuracy and honesty of transactions. All networks would also have to agree to lock each transaction in place and document that transaction unchangeably. In this system, smart contracts are used to access and authenticate users in a decentralized way. Smart contracts are contracts that automatically carry out the terms of the contract that both parties agreed to. We express the terms in code and adhere to them. This makes access control clear because the access authentication sets the permissions. Stakeholders can see and verify who has accessed the data thanks to the computer-based permissions already in place. Furthermore, constant real-time system monitoring improves security and privacy by ensuring verification happens (Gope et al., 2019).

Privacy-Preserving Data Analytics	Implementing privacy-preserving data analytics techniques (e.g., differential privacy, federated learning) to protect individual privacy while enabling meaningful analysis of aggregated data.
Regular Security Audits and Updates	Perform periodic security audits, vulnerability assessments, and penetration testing. Find the vulnerabilities and promptly apply software and firmware updates to address known security issues.
Employee Training and Awareness	Healthcare professionals and IoT device users should receive ongoing training and awareness programs to enhance secure data management, password safety, and the capacity to identify potential security threats.
Compliance with Regulatory Standards	Obeying healthcare data security standards like HIPAA and GDPR to manage patient data in a legal and moral way, keeping track of who has access to the data, and setting up rules for how to report data breaches (Ali et al., 2022).

5 Case Study Implementation

Remote patient monitoring (RPM) is a new way of monitoring the health of patients using the Internet of Things (IoT) by doctors remotely. Wearables and smart sensors are IoT devices that are important for constantly monitoring vital signs and other health parameters. They provide a constant flow of information to let doctors give personalized treatment to every patient and act quickly. The insights they provide keep the doctor informed about each patient's condition, allowing tailored delivery of care as needed. It is important to have a framework in place that ensures the privacy of the patient and keeps the cybercriminals at bay. This is all the more reason why medical data is very private, and IoT devices can pose a threat.

Implementation

- The Transport Layer Security (TLS) protocol guarantees that your system is safe. All the communication is secure. The Datagram Transport Layer Security (DTLS), like the messenger version, protects a message from tampering. Protocols create a secure link between two endpoints that are communicating. This means that if someone is not authorized to read it, they can't even if they seize it. AES is an algorithm used to secure all types of data. RSA is also another strong algorithm used frequently for providing data security. AES and RSA are primarily used to ensure the security of all patient data, which is transmitted from IoT devices to the healthcare system. Digital certificates are what make communication safe. They allow only legitimate people to communicate. Consequently, no communication is possible, and intermediary attacks cannot occur.
- When it comes to remote patient monitoring, resource limitations that IoT devices encounter can be solved using lightweight mitigations and the cryptographic hash function SHA-256. These methods ensure security credentials (PSKs) or device-specific credentials are securely stored in Internet of Things devices' hardware security modules; only verified and trusted devices would use them to connect to the network. Time-based One-Time Passwords (TOTP) and HMAC-based One-Time Passwords (HOTP) generate temporary codes that a legitimate user can produce to authenticate themselves.
- RBAC (Role-Based Access Control) is a system that controls who can access data in the RPM (Remote Patient Monitoring) environment. It gives different access rights based on specific roles. The access policies clearly define these roles, including doctors, nurses, and patients. Each role has access only to the specific information about the patient that it requires. Audits are

periodically conducted to check and update access rights in response to personnel or other changes. As a result, security and oversight become both ongoing and temporary processes.

- Two-factor authentication (2FA) is employed with physically unclonable functions (PUFs) in public vulnerable IoT (Internet of Things) deployments to enhance security. This approach assigns unique IDs to all IoT devices, making it more difficult for unauthorized devices to impersonate legitimate ones. To use the 2FA system, the user must provide two different things – something they have, such as a token or a mobile device, and something they know, like a password. It lowers the chance of getting access in case of a password compromise.
- Intrusion Detection Systems (IDS) track network traffic and device behavior for indications of suspicious activity or security compromise. The methods are signature-based detection, anomaly-based detection, and behavior-based detection. Anomaly monitoring algorithms look at the behavior of IoT devices and healthcare systems. They search for odd behavior that signals a security incident.
- A record of all amendments is kept to ensure the integrity of the information and to make it immutable. Data relating to a patient, for instance, treatment procedures or medical records, are stored on a blockchain and so, cannot be tempered. Blockchain enables decentralization and, as such, allows users to authenticate themselves independently without a central authority. When you define permissions and access using smart contracts, it enhances efficiency and productivity. Using a consensus mechanism facilitates transparent and auditable access control.
- They employ methods that maintain data privacy. These methods are differential privacy and federated learning. Differential privacy achieves individual confidentiality protection and allows privacy-preserving analysis of at least aggregate data by introducing noise to the data. Federated learning enables the development of machine learning models on various Internet of Things devices without the need to exchange raw data. This supports data privacy at the level of the devices while also improving the models' overall accuracy.
- RPM system security audits are run regularly to discover any potential weaknesses and vulnerabilities. Vulnerability assessments and penetration tests measure system strength against malicious attacks and hackers. Updates to software and firmware are done quickly to address known security holes and add security patches. Automated update systems also ensure that all IoT devices on the network receive their updates on time.
- Continuing education and awareness programs are always targeted at those busy in healthcare and using an IoT device. This training program is important because it helps you learn to handle data safely, manage passwords effectively, and identify potential threats. Security awareness training is a must! The organization regularly reminds members and provides best practices to change behavior, thereby improving security protocols and fostering a security culture.
- Our RPM framework, foundational to our organization’s mission, follows crucial healthcare data protection mandates such as HIPAA and GDPR. This standardization ensures the legal and ethical handling of patient data. We have lots of data access and protocols for notifications of requirements for those involved in the data breach, which allows immediate reporting of a security incident.

This complete framework would allow the medical community to construct a protected, privacy-preserving, IoT-based remote patient monitoring system. While Encryption, Authentication, Access Control, Intrusion Detection, Blockchain Technology, Privacy-Preserving Technologies, and regular

security Audits ensure security, they all must work together in a layered security system for protection against any kind of attack. This arrangement is essential for building trust in RPM data.

6 Results and Discussion

RPM Framework

Sensitive patient data security in a connected environment is one of the significant challenges addressed by the proposed workable framework for data protection in IoT-enabled healthcare. A crucial component of the framework that contributes to enhancing the general security and privacy of the IoT ecosystem is highlighted by each theme in Table 1.

Data Encryption and Secure Communication: This theme points out the urgent need to encrypt patient data and establish secure communication channels between healthcare servers and IoT devices. If your client's data is intercepted, encryption guarantees that it will be illegible to anyone else.

Lightweight Authentication Schemes: Due to the resource limitations of Internet of Things (IoT) devices, this proposal presents an efficient authentication method that does not impose a heavy computational burden on these devices. Lightweight authentication schemes, particularly cryptographic hash functions, can provide efficient and secure device and user authentication, thereby warranting the performance of IoT devices.

Role-Based Access Control: Patient data will be governed through role-centric access management. Healthcare roles have assigned access rights so that only the concerned individual can view specific data. The system enhances trust that safeguards patient information.

Two-Factor Authentication: People can use two-factor authentication systems to access devices or medical records. In this regard, two-factor authentication systems can limit malware access to devices. Furthermore, it can also help prevent unauthorized access to medical records in a hospital. Furthermore, the use of physically unclonable functions improves and authenticates devices.

Intrusion Detection and Anomaly Monitoring: It is crucial to identify possible intrusions and anomalies in healthcare IoT. Systems that detect intrusions, anomaly monitoring algorithms, and other similar approaches continuously analyze network traffic and device behavior to identify potential threats.

Blockchain for Data Integrity: Blockchain technology helps ensure an unchangeable ledger, which guarantees the integrity of data. Decentralized authentication through smart contracts increases the transparency and security of user access.

Privacy-Preserving Data Analytics: Data analytics, which preserves privacy, is essential in Healthcare IoT, as it can protect personal privacy while facilitating efficient data analysis. Approaches that facilitate the secure use of private data enable secure analytics and strengthen patient confidentiality.

Regular Security Audits and Updates: Conducting regular security audits and vulnerability assessments, as well as updating software and firmware, are essential to protecting against actively evolving threats.

Employee Training and Awareness: Training healthcare professionals and IoT device users on security protocols fosters a culture of security awareness and reduces the likelihood of human-related security incidents.

Compliance with Regulatory Standards: Complying with data protection laws facilitates the proper handling of patient data and fosters trust among patients and healthcare professionals.

The themes above, when incorporated into the proposed framework, will help healthcare providers design a safe and privacy-preserving IoT environment. This whole strategy reduces security risks, protects private patient information, and enhances trust in modern healthcare solutions. The framework needs to be updated constantly to meet the new security threats and laws as they come up.

7 Comparative Analysis

Current IoT solutions have been evaluated for their potential application in healthcare, as shown in Table 2. Security issues, including authentication, confidentiality, trust, resilience, freshness, fault tolerance, and self-healing, will be primarily examined in this review. Many existing architectures lack features for fault tolerance and self-healing when compared with the proposed AMI architecture. This affects their functioning in unexpected scenarios. The AMI architecture can successfully meet essential security requirements suitable for IoT healthcare systems. It is now challenging to ensure that gateways communicate securely with traditional sensors or nodes. The proprietary protocols of commercial sensors are mainly responsible for the problem. Therefore, it is essential to conduct continuous studies and targeted efforts to solve the problem.

Table 2: Comparative Analysis

IoT solution	Confidentiality	Authentication	Self-healing	Resilience	Trust	Data freshness
Alshamrani, 2022	✗	✗	✓	✗	✗	✗
Debebe, 2016	✓	✓	✗	✗	✓	✗
Castillo O'Sullivan, & Thierer, 2015	✓	✓	✗	✓	✓	✓
Chacko & Hayajneh, 2018	✓	✓	✗	✗	✓	✗
Firouzi et al., 2020	✓	✗	✗	✗	✓	✗
Kumar et al., 2022	✓	✓	✗	✓	✓	✓
Proposed architecture	✓	✓	✓	✓	✓	✓

Ethical Consideration

IoT healthcare technology raises ethical concerns in its application, and ethical issues arise. Specifically, because IoT devices will collect and share sensitive and private health information about individuals, security implications concerning patient privacy are crucial. Responsible design inspired by the duty of care will entail practical elements of security: encryption, access limitations, and privacy protection techniques that eradicate or reduce the risk of unauthorized access, use, or theft of sensitive patient private information. Additionally, patients must provide informed consent before their data is used to deliver IoT services at any level. Above all, the transparency of information must be considered in all aspects, including the sharing and use of private patient information and the associated risks. Being open will help keep the patient's faith in the healthcare practice.

Limitations

We must be aware of the big issues with IoT solutions in healthcare. One specific problem area is interoperability. Interoperability is the term for devices that don't connect due to different protocols and standards. In addition, since Internet of Things devices rely on the internet connection, they can also

cause issues. This may be especially true where network coverage is poor. Some IoT gadgets may not have the ability to deal with it due to low-power and low-cost constraints. Another major concern is the security and privacy risk of using third-party vendors when it comes to IoT devices and services, if not researched well.

8 Conclusion

In conclusion, the growing number of IoT devices presents both opportunities and challenges to the medical field. For the successful functioning of IoT in this field; safety and security are essential. The suggested design of AMI seems to be an all-in-one solution for many security issues. A reliable framework for Internet of Things (IoT) healthcare systems. A structured approach to tackling the security issues in healthcare IoT systems. Also, it is successful due to the application and enforcement of complex theoretical principles.

The research has three main contributions: First, the paper discusses the creation of an integrated security architecture incorporating behavioral analysis, an efficient biometric authentication system, and stronger encryption. Second, the design of pragmatic solutions for immediate use in many health care settings, including the development of remote monitoring systems and electronic medical records. Third, we must develop a roadmap for the policy regulation for the future development of this indispensable sector, including research.

The study developed a standard executive guide and a real-time security monitoring tool, alongside a dynamic encryption model suitable for various types of data and a comprehensive authentication system for wearable monitoring devices. The report also distinguishes itself by proposing a detailed training schedule for medical staff and a legislative framework for consistent security standards.

The study's primary contribution addresses balancing security and energy consumption through the innovative integration of blockchain and artificial intelligence technologies. This comprehensive perspective closely connects technical, administrative, and organizational elements, making the study a valuable resource for academics and practitioners in digital healthcare. It also provides a strong basis for future studies that can expand on these findings to provide more sophisticated solutions fulfilling the evolving needs of the digital age healthcare industry.

To fully leverage IoT's potential, healthcare stakeholders must confront these ethical considerations, limitations, and challenges, working collaboratively to establish secure, interoperable, and ethically responsible IoT implementations in healthcare. This will ultimately enhance patient outcomes and streamline healthcare processes while preserving patient privacy and data security.

Acknowledgements

The author would like to thank Gulf Colleges, Saudi Arabia, for providing support for this research.

References

[1] Akkaoui, R. (2021). Blockchain for the management of Internet of Things devices in the medical industry. *IEEE Transactions on Engineering Management*, *70*(8), 2707-2718. https://doi.org/10.1109/TEM.2021.3097117

[2] Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors*, *22*(2), 572. https://doi.org/10.3390/s22020572

[3] Ali, A., Pasha, M. F., Ali, J., Fang, O. H., Masud, M., Jurcut, A. D., & Alzain, M. A. (2022). Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography. *Sensors*, *22*(2), 528. https://doi.org/10.3390/s22020528

[4] 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. https://doi.org/10.1016/j.jksuci.2021.06.005

[5] Anantharam, P., Banerjee, T., Sheth, A., Thirunarayan, K., Marupudi, S., Sridharan, V., & Forbis, S. G. (2015, June). Knowledge-driven personalized contextual mhealth service for asthma management in children. In *2015 IEEE international conference on mobile services* (pp. 284-291). IEEE. https://doi.org/10.1109/MobServ.2015.48

[6] Anuradha, M., Jayasankar, T., Prakash, N. B., Sikkandar, M. Y., Hemalakshmi, G. R., 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. https://doi.org/10.1016/j.micpro.2020.103301

[7] August, G. J., & Gewirtz, A. (2019). Moving toward a precision-based, personalized framework for prevention science: Introduction to the special issue. *Prevention Science*, *20*(1), 1-9. https://doi.org/10.1007/s11121-018-0955-9

[8] 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. https://doi.org/10.3390/sym12071191

[9] Castillo O'Sullivan, A., & Thierer, A. D. (2015). Projecting the Growth and Economic Impact of the Internet of Things. *Available at SSRN 2618794*.https://doi.org/10.2139/ssrn.2618794

[10] Chacko, A., & Hayajneh, T. (2018). Security and privacy issues with IoT in healthcare. *EAI Endorsed Transactions on Pervasive Health and Technology*, *4*(14). https://doi.org/10.4108/eai.13-7-2018.155079

[11] Dang, F., Li, Z., Liu, Y., Zhai, E., Chen, Q. A., Xu, T., ... & Yang, J. (2019, June). Understanding fileless attacks on linux-based iot devices with honeycloud. In *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services* (pp. 482-493). https://doi.org/10.1145/3307334.3326083

[12] 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. https://doi.org/10.3390/electronics8070768

[13] Debebe, B. (2016). Levels, Trends and Determinants of Under-Five Mortality in Amhara Region, Ethiopia, Evidence from Demographic and Health Survey (2000 - 2011). *International Academic Journal of Social Sciences, 3*(2), 96–112.

[14] Firouzi, F., Farahani, B., Barzegari, M., & Daneshmand, M. (2020). AI-driven data monetization: The other face of data in IoT-based smart and connected health. *IEEE Internet of Things Journal*, *9*(8), 5581-5599. https://doi.org/10.1109/JIOT.2020.3027971

[15] 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. https://doi.org/10.1109/JIOT.2018.2846299

[16] 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. https://doi.org/10.1109/TII.2019.2895030

[17] 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. https://doi.org/10.1016/j.comnet.2018.11.021

[18] Jalali, Z., & Shaemi, A. (2015). The impact of nurses' empowerment and decision-making on the care quality of patients in healthcare reform plan. *International Academic Journal of Organizational Behavior and Human Resource Management, 2*(1), 60–66.
Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks*, *1*(2-3), 293-315. https://doi.org/10.1109/SNPA.2003.1203362

[19] 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. https://doi.org/10.1109/TII.2022.3161631

[20] Kute, S. S., Tyagi, A. K., & Aswathy, S. U. (2021). Security, privacy and trust issues in internet of things and machine learning based e-healthcare. In *Intelligent interactive multimedia systems for e-healthcare applications* (pp. 291-317). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-16-6542-4_15

[21] 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. https://doi.org/10.1109/ACCESS.2020.2993700

[22] Nair, M., & Rao, A. (2023). Blockchain for Terminology Traceability in Decentralized Health Systems. *Global Journal of Medical Terminology Research and Informatics*, *1*(1), 9-11.

[23] Neyja, M., Mumtaz, S., Huq, K. M. S., Busari, S. A., Rodriguez, J., & Zhou, Z. (2017, December). An IoT-based e-health monitoring system using ECG signal. In *GLOBECOM 2017-2017 IEEE Global Communications Conference* (pp. 1-6). IEEE. https://doi.org/10.1109/GLOCOM.2017.8255023

[24] Raktur, H., & Jea, T. (2024). Design of Compact Wideband Wearable Antenna for Health Care and Internet of Things System. *National Journal of Antennas and Propagation*, *6*(1), 40-48.

[25] Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. *Ad hoc networks*, *11*(8), 2661-2674. https://doi.org/10.1016/j.adhoc.2013.04.014

[26] Rehman, S. U., & Manickam, S. (2017). Improved mechanism to prevent denial of service attack in IPv6 duplicate address detection process. *International Journal of Advanced Computer Science and Applications*, *8*(2). https://doi.org/10.14569/IJACSA.2017.080209

[27] Saba Raoof, S., & Durai, M. S. (2022). A comprehensive review on smart health care: applications, paradigms, and challenges with case studies. *Contrast Media & Molecular Imaging*, *2022*(1), 4822235. https://doi.org/10.1155/2022/4822235

[28] Sadek, I., Codjo, J., Rehman, S. U., & Abdulrazak, B. (2022). Security and privacy in the Internet of Things healthcare systems: Toward a robust solution in real-life deployment. *Computer Methods and Programs in Biomedicine Update*, *2*, 100071. https://doi.org/10.1016/j.cmpbup.2022.100071

[29] 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. https://doi.org/10.1109/MIC.2018.112102519

[30] Shenoy, K., & Menon, A. (2021). A Healthcare Model Using Blockchain Technology to enhance Security and Data Sharing. *International Academic Journal of Science and Engineering*, *8*(2), 6–10.

[31] Shrivastav, P., & Malakar, U. (2024). Exploring Barriers to Medication Adherence Among Patients with Chronic Diseases. *Clinical Journal for Medicine, Health and Pharmacy*, *2*(3), 21-31.

[32] 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. https://doi.org/10.1109/TDSC.2018.2828306

[33] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102. https://doi.org/10.3390/app10124102

[34] Thilagam, K., Beno, A., Lakshmi, M. V., Wilfred, C. B., George, S. M., Karthikeyan, M., ... & Karunakaran, P. (2022). Secure IoT Healthcare Architecture with Deep Learning-Based Access Control System. *Journal of Nanomaterials*, *2022*(1), 2638613. https://doi.org/10.1155/2022/2638613

[35] 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. https://doi.org/10.1155/2013/794326

[36] 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. https://doi.org/10.1016/j.dcan.2020.07.003

[37] Zhang, J. X. J., & Hoshino, K. (2019). Implantable and wearable sensors. *Molecular Sensors and Nanodevices*, 489-545. https://doi.org/10.1016/B978-0-12-814862-4.00008-9

Author Biography

Baha Eldin Hamouda holds a Ph.D. in Information Technology from Alneelain University, Sudan. He is currently an Assistant Professor in the Department of Information Technology at Gulf Colleges, Hafar Al-Batin, Saudi Arabia. His primary research interests include Cybersecurity, IoT Security, Cryptography, Data Privacy, and AI Security. He has authored several publications in reputable international journals and conferences.