Mesopotamian Journal of Artificial Intelligence in Healthcare
Vol.2024, **pp**. 135–169
DOI: https://doi.org/10.58496/MJAIH/2024/016; ISSN: 3005-365X
https://mesopotamian.press/journals/index.php/MJAIH

Review Article

A Comprehensive Review on Cryptographic Techniques for Securing Internet of Medical Things: A State-of-the-Art, Applications, Security Attacks, Mitigation Measures, and Future Research Direction

Wamusi Robert [1], Asiku Denis [1], Adebo Thomas [1], Aziku Samuel [1], Simon Peter Kabiito [1], Zaward Morish [1], Guma Ali [1*]

[1] *Department of Computer and Information Science, Faculty of Technoscience, Muni University, Arua, Uganda*.

ARTICLEINFO

Article History
Received 05 Aug 2024
Accepted 08 Sep 2024
Accepted 08 Oct 2024
Published 03 Nov 2024

Keywords
IoMT
Healthcare
Cryptography
Cryptographic Techniques
Security Attacks

ABSTRACT

As healthcare becomes increasingly dependent on the Internet of Medical Things (IoMT) infrastructure, it is essential to establish a secure system that guarantees the confidentiality and privacy of patient data. This system must also facilitate the secure sharing of healthcare information with other parties within the healthcare ecosystem. However, this increased connectivity also introduces cybersecurity attacks and vulnerabilities. This comprehensive review explores the state-of-the-art in the IoMT, security requirements in the IoMT, cryptographic techniques in the IoMT, application of cryptographic techniques in securing the IoMT, security attacks on cryptographic techniques, mitigation strategies, and future research directions. The study adopts a comprehensive review approach, synthesizing findings from peer-reviewed journals, conference proceedings, book chapters, Books, and websites published between 2020 and 2024 to assess their relevance to cryptographic applications in IoMT systems. Despite advancements, cryptographic algorithms in IoMT remain susceptible to security attacks, such as man-in-the-middle attacks, replay attacks, ransomware attacks, cryptanalysis attacks, key management attacks, chosen plaintext/chosen ciphertext attacks, and side-channel attacks. While techniques like homomorphic encryption enhance security, their high computational and power demands pose challenges for resource-constrained IoMT devices. The rise of quantum computing threatens the efficacy of current cryptographic protocols, highlighting the need for research into quantum-resistant cryptography. The review identifies critical gaps in existing cryptographic research and emphasizes future directions, including lightweight cryptography, quantum-resistant methods, and artificial intelligence-driven security mechanisms. These innovations are vital for meeting the growing security requirements of IoMT systems and protecting against increasingly sophisticated threats.

1. INTRODUCTION

The IoMT has transformed healthcare by connecting devices such as wearable health trackers, implantable sensors, and network-connected medical systems. Iqbal et al. [1], Arefin et al. [2], and Fiore et al. [3] define the IoMT as the network of tiny sensors, actuators, smart medical devices, software applications, and health products and services that use wired or wireless communication networks to collect, process, disseminate, and analyze health data, that enhances clinical decision-making. IoMT has evolved from the Internet of Things (IoT), encompassing the technologies employed in medical and healthcare information technology applications [4]. The widespread use of wireless medical sensor networks in the healthcare sector has driven the development of IoMT [5]. IoMT devices, such as wearable health monitors (like smartwatches, fitness trackers, and wearable biosensors), smart ventilators, smart thermometers, blood pressure monitors, smart infusion pumps, home monitoring devices, and connected imaging machines, continuously collect data. This continuous flow of information enables proactive healthcare management [6][9].

The development of smart sensors, devices, and advanced lightweight communication protocols has enabled the interconnection of patients, doctors, and medical devices with hospital equipment, diagnostic tools, and wearable technology. This interconnected system allows for monitoring biomedical signals and diagnosing patients' diseases without human intervention [4][5]. In IoMT, various sophisticated sensors are placed on patients to monitor their physiological parameters while ensuring comfort continuously. The collected data is transmitted to centralized servers or cloud platforms for further processing and analysis using artificial intelligence, machine learning, and big data techniques. This analysis provides

*Corresponding author. Email: a.guma@muni.ac.ug

clinical insights that help doctors make informed medical decisions [1][4][7][8]. Doctors can access the analyzed data, including vital signs, health measurements, medical histories, and other relevant parameters, through handheld devices like tablets and smartphones for patient diagnosis and treatment. With this information, doctors can more thoroughly assess the patient's health status using mobile health applications and make better-informed medical decisions [10][11].

Analysts project that the global IoMT market will rise at a CAGR of 9.91%, increasing from a valuation of US$84 billion in 2024 to US$370.9 billion by 2032 [12]. The healthcare industry will generate 30% of the total IoT data volume by 2025, with this share projected to increase by 10% by 2030 [13]. The main reasons for the growth include the emergence of innovative products and the rising adoption of remote patient monitoring devices. The United States, expected to generate US$29.64 billion in revenue in 2024, is projected to lead globally in this domain [14].

IoMT enables real-time monitoring of patients in both hospital and home settings, allowing for the early detection of health issues, the creation of personalized treatment plans, and the prevention and management of diseases. It supports the development of smart hospitals, enhances communication and collaboration among healthcare professionals, and aids in tracking infectious diseases. Additionally, IoMT facilitates telemedicine, remote consultations, and efficient resource management while ensuring the secure exchange of medical information [15-17]. It enhances diagnostic accuracy, enables real-time drug prescriptions and diagnoses, and minimizes errors, ultimately improving the efficiency, quality, and accessibility of healthcare services. It optimizes patient outcomes, reduces healthcare costs, and facilitates accurate diagnoses and timely interventions. By fostering effective interactions between patients and physicians, the IoMT supports tailored care strategies and remote patient monitoring, offering new opportunities for medical process improvements. It accelerates diagnoses and therapies, reduces unnecessary hospital visits, and strengthens clinical decision-making, all while enhancing patient safety. The technology empowers healthcare providers with near-real-time data, enabling timely responses to emergency biomarker alterations. Healthcare professionals make better decisions and provide timely medical interventions using this proactive approach, transforming care delivery [18-30].

Despite its transformative benefits, the increasing reliance on IoMT raises significant security and privacy concerns due to the sensitivity of medical data and its vulnerability to cyberattacks [10]. Naeem et al. [31] reported that in 2021, IoMT and healthcare-related sectors generated 72% of all malicious traffic. Healthcare cyberattacks rose by 40% that year, with 81% of providers acknowledging at least one compromised IoMT system. The urgent need for robust security measures becomes evident as these statistics emphasize protecting patient information within IoMT systems and networks. Strong security measures, particularly cryptographic techniques, are critical to safeguarding patient data, maintaining system integrity, and fostering trust in these technologies because they offer diverse tools to address these challenges, such as authenticating devices and users, safeguarding data in transit and at rest, and guaranteeing the confidentiality and integrity of medical records [32-34]. The most widely used cryptographic methods in IoMT include symmetric cryptography (e.g., Blowfish, Data Encryption Standard [DES], Triple DES, and Advanced Encryption Standard [AES]), asymmetric cryptography (e.g., Rivest–Shamir–Adleman [RSA], Digital signature algorithm [DSA], and Elliptic curve cryptography [ECC]), hash functions (e.g., Secure Hash Algorithm 1 [SHA-1], SHA-2, and SHA-3), and digital signatures [35-38].

These traditional encryption models secure data confidentiality and integrity, provide non-repudiation through Blockchain and digital signatures, enhance privacy with homomorphic encryption and differential privacy, and secure communication protocols using secure sockets layer (SSL) and transport layer security (TLS) [39-42]. However, these models were not designed to accommodate the limited processing power, memory, and battery life of IoMT devices [43]. Implementing cryptographic protocols faces numerous challenges due to vulnerabilities such as man-in-the-middle attacks (MitM), side-channel attacks, replay attacks, cryptanalysis, brute-force attacks, key management attacks, insider attacks, denial-of-service (DoS) attacks, social engineering attacks, chosen plaintext/chosen ciphertext attacks, malware injection attacks, ransomware and data corruption attacks, firmware tampering, and quantum computing threats. IoMT devices' resource constraints—limited energy, processing power, and storage—further complicate the development of robust security solutions. Additionally, the heterogeneous and distributed architecture of IoMT systems poses barriers to creating universal security measures [44-48]. These security attacks jeopardize sensitive patient data's confidentiality, integrity, availability, privacy, and functionality of IoMT devices, leading to disruptions in healthcare services, misdiagnoses, incorrect treatments, and potential patient harm [49][50]. The growing importance of IoMT systems in healthcare underscores the urgent need to enhance their security. This study seeks to bridge significant gaps in the literature by comprehensively analyzing the state-of-the-art in the IoMT, security requirements in the IoMT, cryptographic techniques in the IoMT, application of cryptographic techniques in securing the IoMT, security attacks on cryptographic techniques, mitigation strategies, and future research directions for securing IoMT systems.

Several studies have explored cryptographic techniques to secure IoMT systems. For example, Chen et al. [51] proposed a privacy-preserving multi-factor authentication scheme with post-quantum security. Abikoye et al. [52] recommended a hybrid cryptographic scheme for safeguarding critical user information. Adil et al. [53] presented an AI-enabled hybrid lightweight authentication scheme for IoMT-based cyber-physical systems. Srivastava and Debnath [54] proposed a multivariate-based certificateless signature scheme for IoMT applications. However, these studies did not extensively

examine the security vulnerabilities in cryptographic techniques for IoMT. This comprehensive review aims to fill this gap by analyzing security attacks on IoMT cryptographic methods, identifying mitigation mechanisms, and proposing future research directions.

This review makes several key contributions. It examines the state-of-the-art in the IoMT, including its evolution, architecture, practical applications, and security requirements. It explains various cryptographic algorithms for IoMT security and describes how these techniques protect IoMT devices and data. Additionally, it explores security attacks targeting cryptographic techniques in IoMT and highlights reliable methods for safeguarding these cryptographic approaches. Finally, the review identifies future research directions for advancing the use of cryptographic algorithms in securing IoMT systems.

The paper is structured as follows: Section 2 covers materials and methods, Section 3 reviews the state-of-the-art, Section 4 explores the security requirements in the IoMT, Section 5 describes the cryptographic techniques in the IoMT, Section 6 outlines the application of cryptographic techniques in securing the IoMT, Section 7 discusses security attacks on IoMT cryptographic techniques, Section 8 details robust mechanisms for securing IoMT cryptographic methods, Section 9 presents future research directions, and Section 10 concludes the study.

2. MATERIALS AND METHODS

This paper examines cryptographic methods to secure the IoMT. It focuses on the state-of-the-art in the IoMT, security requirements in the IoMT, cryptographic techniques in the IoMT, application of cryptographic techniques in securing the IoMT, security attacks on cryptographic techniques, mitigation strategies, and future research directions. The study adopts a comprehensive review approach to gather, evaluate, and synthesize existing literature, enabling a thorough understanding of the field's current trends, challenges, and developments.

The review utilized relevant keywords and searched various academic databases and digital libraries, including PubMed Central, Emerald Insight, ACM Digital Library, BioMed Central, Wiley Online Library, SAGE, Taylor & Francis, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, IGI Global, Pearson, and Google Scholar, to compile pertinent literature. The sources comprised journal articles, conference proceedings, book chapters, Books, and websites. Their extensive coverage informed the choice of these digital libraries of peer-reviewed publications and leading computer science and engineering journals. The literature review spans several critical aspects of the IoMT and focuses on publications from 2020 to 2024 to ensure the analysis is current and relevant.

To search, combinations of keywords such as "Internet of Medical Things," "IoMT," "cryptography," "cryptographic techniques," "IoMT security," "data encryption," "authentication protocols," "security attacks on cryptographic techniques," "privacy threats," "encryption algorithms," "Blockchain," "future trends," and "research directions" were employed. The researchers used Boolean operators such as AND and OR to refine the search process, and relevant references were manually identified by reviewing the bibliographies of selected studies. Researchers iteratively adjusted the scope of the search to ensure inclusivity and precision.

The researchers rigorously applied inclusion and exclusion criteria to ensure the study's quality and relevance. These criteria, outlined in Table 1, specify the parameters used to select appropriate research papers. This comprehensive review approach ensures that the survey captures a balanced and extensive overview of the field.

TABLE I. SUMMARY OF INCLUSION AND EXCLUSION CRITERIA USED IN SELECTING THE RELEVANT RESEARCH PAPERS.

S/No	Inclusion Criteria	Exclusion Criteria
1	The researchers considered only research papers written in English.	We excluded publications in non-English languages due to translation constraints and the risk of misinterpretation.
2	The researchers included studies focused on integrating cryptographic methods to address IoMT security vulnerabilities, those examining security attacks on cryptographic techniques in IoMT, and their mitigation strategies.	We also omitted papers focusing on general IoT security without emphasizing medical devices.
3	We selected peer-reviewed journal articles, conference papers, book chapters, eBooks, and reputable technical reports.	Additionally, we excluded studies published in predatory journals or conferences that lack peer review.
4	We also included reviews and meta-analyses that offered significant insights into the field.	We disregarded reviews and meta-analyses that failed to provide substantial insights into the field.
5	Additionally, the researchers prioritized research papers with transparent methodologies and well-documented result selection.	The researchers excluded research studies with vague methodologies or inconclusive results.
6	The researchers included only studies published between 1 January 2020 and 30 November 2024.	Finally, we excluded research papers published before 1 January 2020, except one published in 2014.

Eight authors independently retrieved relevant materials from selected research databases based on predefined critical parameters. These included details such as the title, authors, and publication year; objectives and research questions; study design; methods of analysis; results; conclusions; IoMT; security requirements; cryptographic techniques; applications of

cryptographic techniques in securing IoMT; security attacks on cryptographic techniques; robust mechanisms for securing cryptographic techniques in IoMT; and future research directions. The researchers systematically organized and cross-verified the extracted data to ensure consistency and accuracy.

The review process followed a structured approach consisting of several stages. Initially, over 3,200 publications were identified through academic search engines and databases. The team removed duplicates and screened abstracts, narrowing the dataset to 950 publications. They then assessed eligibility, reducing the number to 435. Finally, they selected 173 publications that met the inclusion criteria for the study. Fig. 1 shows the distribution of selected research publications based on paper type.

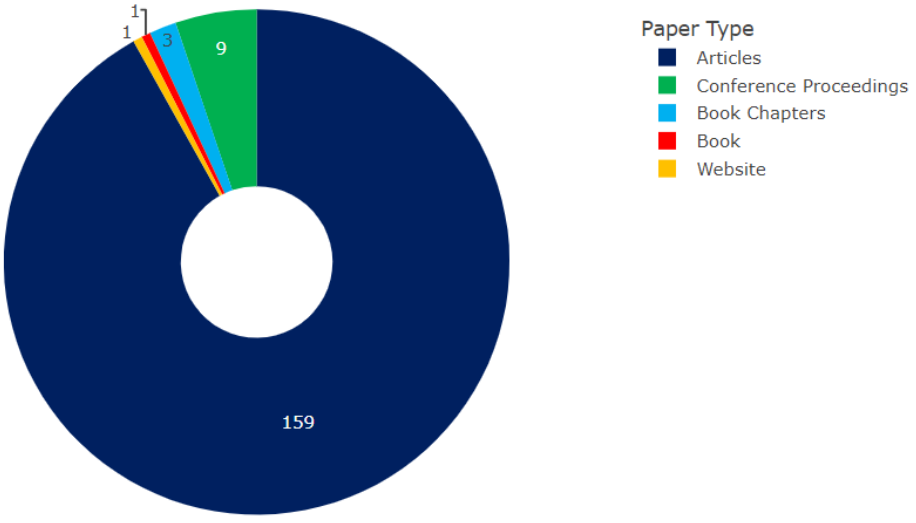


Fig. 1. Shows the distribution of selected research publications based on paper type.

Among the 173 publications, the breakdown by source included one paper from PubMed Central, one from Emerald Insight, two from ACM Digital Library, one from BioMed Central, six from Wiley Online Library, three from SAGE, two from Taylor & Francis, fifteen from Springer, twenty-one from ScienceDirect, fifty-four from MDPI, forty-three from IEEE Xplore Digital Library, three from IGI Global, one from Pearson, and twenty from Google Scholar. The researchers thoroughly evaluated, categorized and assessed these publications for their relevance to the study objectives. Fig. 2 visually represents the distribution of selected research publications across various digital libraries.

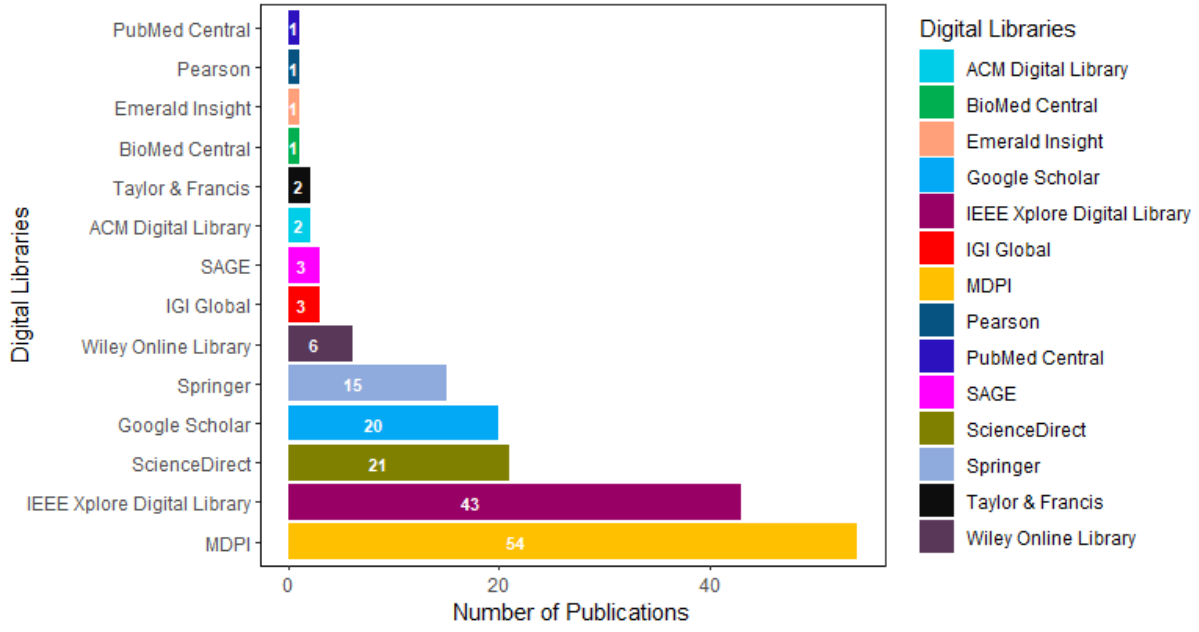


Fig. 2. Depicts the distribution of selected research publications across digital libraries.

Fig. 3 displays the distribution of the selected research papers across various digital libraries, organized by the paper type.

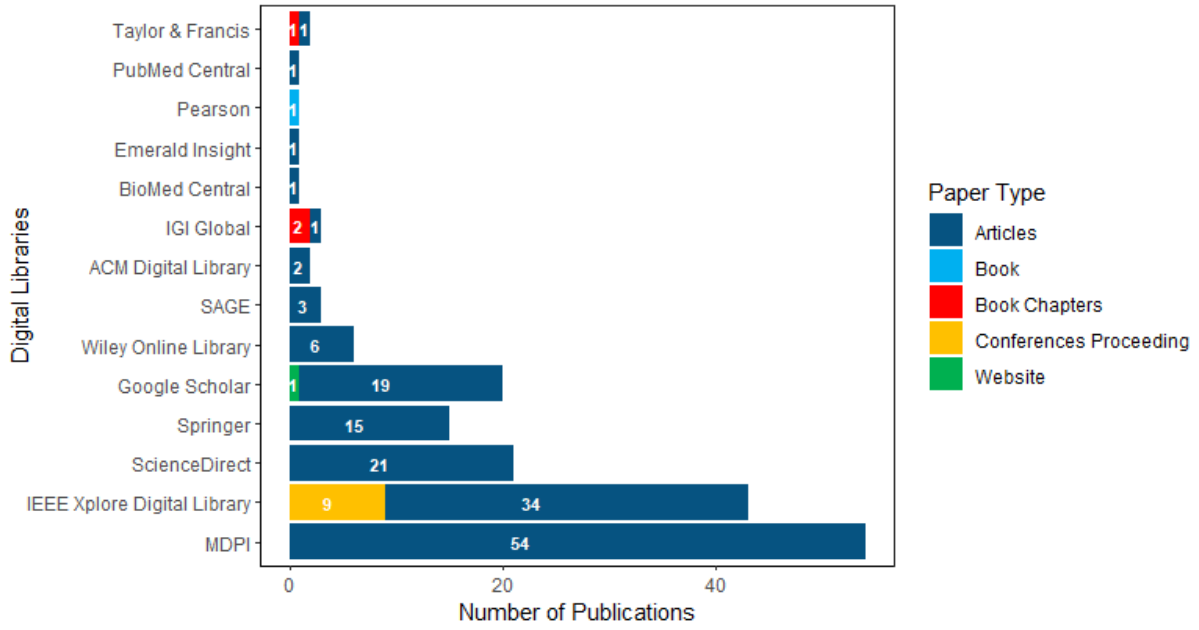


Fig. 3. Displays the distribution of the selected research papers across various digital libraries organized by the paper type.

Fig. 4 illustrates the distribution of the selected research papers across various digital libraries, organized by their year of publication.

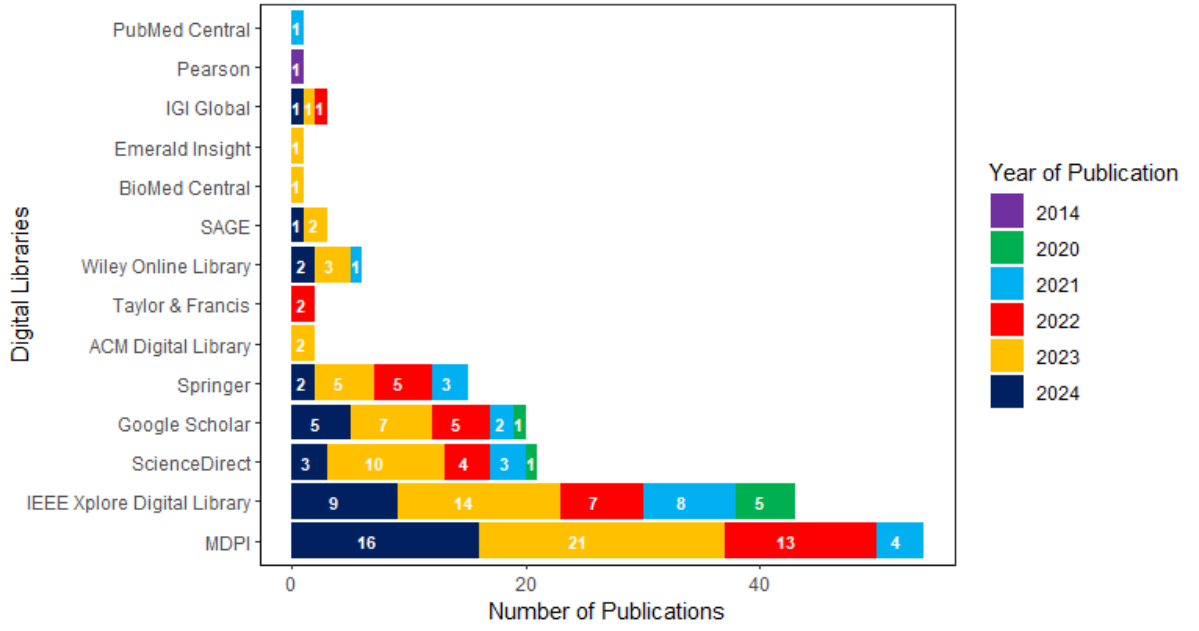


Fig. 4. Shows the distribution of selected research papers across digital libraries according to the year of publication.

The researchers systematically extracted essential data from each selected paper to develop a comprehensive understanding of the topic. Key elements included the types of cryptographic techniques employed (e.g., symmetric encryption, asymmetric encryption, lightweight cryptography, homomorphic encryption), specific IoMT use cases (e.g., patient monitoring, pregnancy monitoring, athletic performance monitoring, etc.), reported vulnerabilities or security attacks in cryptographic techniques used in IoMT systems, improvements or modifications to existing cryptographic protocols, and trends or future research directions highlighted by the authors.

Several criteria, such as relevance, methodological rigor, coherence, validity, reliability, peer-review status, the credibility of sources, potential bias and confounding variables, timeliness, citations, and references, guided the selection of research papers. The researchers employed these criteria to ensure the validity and reliability of the findings. After querying databases, they created a unique reference database, recorded all references, and used a reference management tool to remove duplicates. The team shortlisted research papers through a multi-step process, including full-text assessments, title and abstract screening, and keyword analysis. They excluded studies that failed to meet the eligibility criteria and documented the primary reasons for rejection. Finally, they compiled the selected studies into a final database for analysis.

The researchers synthesized and analyzed the gathered data using thematic analysis and qualitative synthesis methods. They validated their findings by consulting domain experts, cross-referencing results with previous studies, and rigorously evaluating the validity of the conclusions. The final selection included only high-quality research papers, assessed through a scoring system that evaluated the methodology's robustness, results reliability, and contribution to cryptographic techniques for IoMT security. This study did not require ethical approval, as it relied on existing literature. Nevertheless, the researchers upheld moral standards by citing all sources adequately and avoiding plagiarism.

The study acknowledges several potential limitations. First, it might have missed some relevant studies if not included in the selected databases. Second, the study recognizes the potential impact of publication bias, where research with positive findings is more likely to be published. Third, the review might not comprehensively address attacks on cryptographic techniques in IoMT. Fourth, the absence of quantitative analysis or empirical data might limit the robustness of the review, as qualitative evaluations may only partially substantiate the claims. Fifth, the review may focus on theoretical applications while underemphasizing real-world implementation challenges, such as cost, scalability, and user acceptance. Finally, the field of cryptographic techniques and attacks evolves rapidly, potentially outpacing the literature reviewed.

3. STATE of the ART

This section explores the evolution of the IoMT, delving into its architectural framework and practical application of IoMT architecture.

3.1 Evolution of the IoMT

The IoMT has evolved into a transformative force in healthcare, reflecting the broader development of IoT. It began with essential sensor-based monitoring and has advanced to sophisticated, artificial intelligence-powered systems that deliver individualized and predictive healthcare. The several phases of IoMT's evolution are explained in detail below, with advancements introduced at each stage:

3.1.1 The early years of remote monitoring and telemedicine (1970s-1990s)

In the 1970s, experts first proposed delivering healthcare remotely through telecommunications. Over time, video conferencing replaced phone consultations as a tool for providing expert assistance in remote locations. Advances in medical devices, such as Holter monitors and early pacemakers, enabled remote patient monitoring. However, communication and data-sharing limitations restricted these technologies' full potential [55].

3.1.2 Wearable medical technology's ascent in the 2000s

Fitness trackers, heart rate monitors, and glucose monitors are personal health monitoring gadgets that became popular in the early 2000s. For the most part, these were standalone devices with poor connectivity. The first IoT-enabled health devices were made possible by the advancement of cellular, Bluetooth, and Wi-Fi technology, which allowed these devices to send data to central systems [55].

3.1.3 IoT's entry into the healthcare industry in the 2010s

As IoT applications tailored to the healthcare industry began to appear, the name IoMT gained popularity. The term "IoMT" describes a networked ecosystem of healthcare systems, applications, and medical devices that interact with one another to improve patient outcomes. Wearable Electrocardiogram monitors, intelligent inhalers, insulin pumps, and connected implants are examples of connected devices. Based on the data they gather, these devices continuously monitor and modify therapies. Healthcare providers could access continuous data streams by integrating IoMT devices with electronic health record systems, which improved patient monitoring, diagnosis, and treatment. The ability to store, analyze, and share vast amounts of health data produced by IoMT devices from any location has made cloud services essential [55].

3.1.4 Developments in predictive healthcare, artificial intelligence, and data analytics (late 2010s to 2020s)

Predictive analytics and individualized care are now possible because of the application of artificial intelligence algorithms to massive volumes of data gathered by IoMT devices. Systems powered by artificial intelligence can identify early warning indicators of illnesses, forecast medical occurrences (such as heart attacks), and recommend preventative actions. The emphasis switched to ongoing monitoring of patients with chronic diseases, like diabetes and hypertension, outside clinical

settings to decrease the need for frequent hospital stays. Telemedicine enables doctors to provide more thorough remote consultations using IoMT devices to access real-time health data. This real-time data allows doctors to make better decisions during consultations [55].

3.1.5 Integration of cutting-edge technologies (2020s)

IoMT devices can now quickly send massive amounts of data with low latency because of the advent of 5G networks, which made connections faster and more dependable, crucial for applications like remote surgery and real-time diagnostics. Researchers and developers are exploring Blockchain to securely manage IoMT data, ensuring tamper-proof records and traceability. Edge computing, which processes data closer to the device rather than depending on central cloud systems, has begun to gain traction in the IoMT, which lowers latency and allows for real-time decision-making, essential for applications that save lives. Personalized treatment plans, predictive analytics, and diagnostics powered by artificial intelligence have gained popularity. Artificial intelligence models were trained using large datasets from IoMT devices, increasing their precision in predicting diseases and suggesting treatments. Cybersecurity risks increased in tandem with the growth of IoMT use. Research into secure IoT frameworks tailored for medical devices arose due to the growing importance of preventing breaches of the enormous volume of sensitive health data [55].

3.1.6 Future trends

Precision medicine, in which therapies are customized based on a patient's genetic profile and health data, is anticipated to be driven by combining the IoMT data and genetic information. IoMT-enabled digital treatments will deliver software-driven interventions that give patients immediate direction and feedback, which can include mental health treatments as well as the management of chronic illnesses. Surgeons can operate on patients from different geographic areas using real-time data from IoMT devices thanks to 5G and sophisticated robotic equipment. Using IoMT devices for everything from infection control and resource management to patient monitoring, healthcare facilities will become increasingly automated and networked [55]. Fig. 5 illustrates the evolution of IoMT.

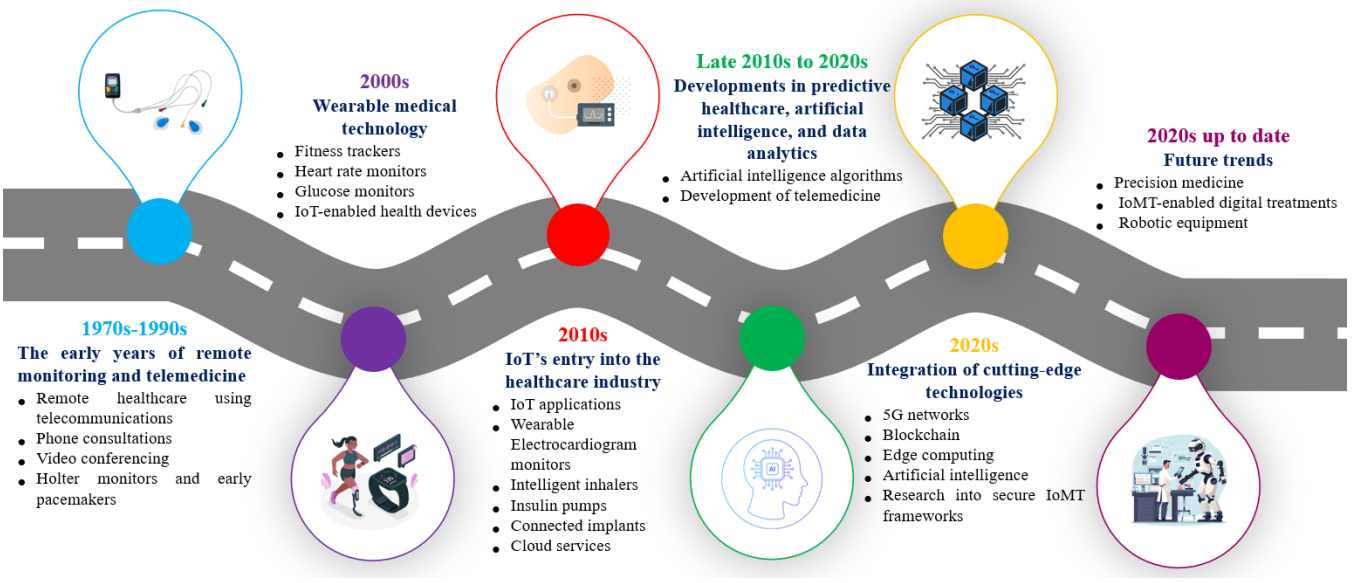


Fig. 5. Shows how the IoMT evolved and advanced technologically from the 1970s to the present.

The growing trend toward data-driven, individualized healthcare is reflected in the evolution of IoMT. Patient care has changed due to the IoMT, becoming more proactive, ongoing, and accessible. By combining cutting-edge technologies like Blockchain, 5G, and artificial intelligence, the IoMT can completely transform the healthcare sector and provide better patient outcomes and a more effective healthcare system.

3.2 The Architecture of the IoMT

The architecture of the IoMT integrates advanced and intelligent technologies into healthcare infrastructure to enhance the efficiency, effectiveness, and quality of healthcare services. A conceptual IoMT architecture organizes its structure into eleven layers: perception or sensor, network, edge computing, fog computing, gateway, cloud computing, Blockchain, data analytics, security, application, and regulatory. Each layer plays a critical role, including collecting patient medical data via sensors and wearable devices, safeguarding this sensitive data, storing it securely, analyzing it for insights, and presenting it

meaningfully to patients and healthcare professionals [56][57]. Together, these layers form a cohesive system that underpins the functionality and reliability of IoMT applications. Fig. 6 depicts the main layers in the IoMT architecture.

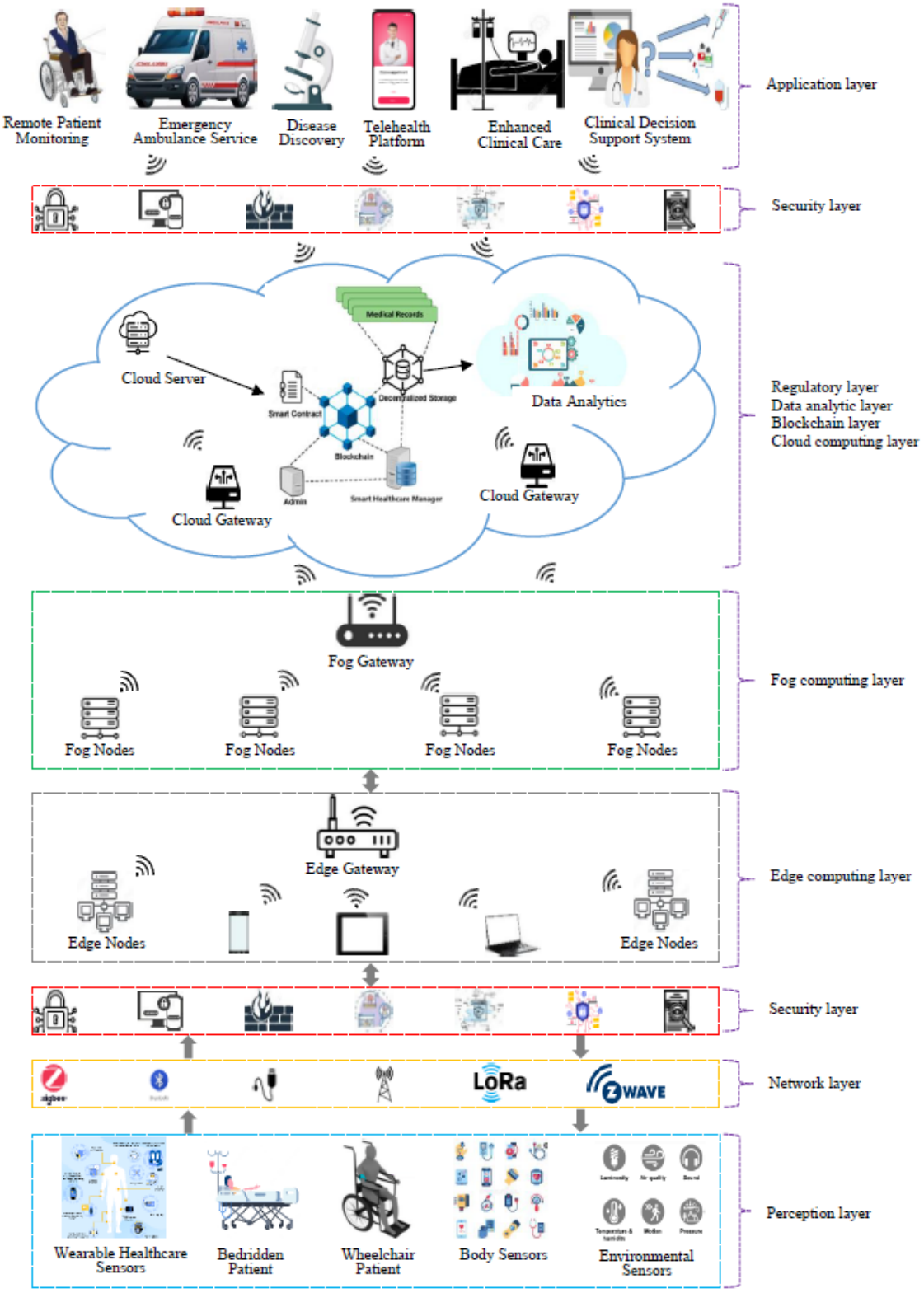


Fig. 6. Depicts the main layers of the IoMT architecture.

3.2.1 Perception or sensor layer

The perception layer includes wearable sensor devices, implanted sensor devices, ambient sensor devices, controllers, intelligent medical devices, and other non-invasive devices. The sensors collect real-time medical data and vitals, such as blood oxygen saturation, respiratory rate, temperature, blood pressure, electrocardiogram, heart rate, glucose levels, movement and activity, sleep patterns, electroencephalogram, skin conductance, and pulse wave velocity from the patient body, and transmit the raw data to local server nodes using wired or wireless networks and communication technologies for edge and fog computing, as well as to the cloud through a gateway [58-61]. They also gather environmental information such as humidity, temperature, light, noise, and air quality [62-67]. These devices are controlled and connected to IoMT networks for remote monitoring. Protecting their security is critical since they gather and transmit sensitive patient medical data [68].

3.2.2 Network layer

The network layer sends data between the perception and gateway levels. It consists of wired and wireless networks that connect perception, application, and other network devices to transmit the collected medical data from the sensor layer to the upper layers for further processing using short-range or medium-range communication technologies and network protocols [58-63]. Bluetooth, ZigBee, Wi-Fi, near-field communication, long-range-wide area network, message queuing telemetry transport, ultra-wideband, RFID, RuBee, constrained application protocol, Z-Wave, and cellular networks are used in the network layer to ensure secure and efficient medical data transmission within the IoMT ecosystem [64][68-69]. Some variables to consider while selecting network protocols are data transfer rate, transmission range, number of supported IoMT devices, energy consumption, interference caused by the coexistence of multiple technologies, and security features [68].

3.2.3 Edge computing layer

The edge computing layer is a distributed computing infrastructure that brings computational resources closer to where medical data is generated to reduce transmission delays and data load on backbone networks caused by high bandwidth consumption while improving computing performance [58-61]. This layer is between the perception layer and fog computing and is responsible for sensor medical data preprocessing, analysis, and transformation. Higher computation layers then process the results further [67][70-72].

3.2.4 Fog computing layer

Because of the cloud layer's latency, bandwidth, and privacy constraints, the fog computing layer in IoMT architecture is a decentralized computing infrastructure that extends cloud computing capabilities to the network's edge. This layer sits between the edge devices and the core cloud infrastructure. The medical data from the perception and edge layers is filtered, cleaned, analyzed, processed, and aggregated through the fog computing layer [58-61]. It also inspects packet content, performs network and data level analytics and thresholds, and generates events [67][70][71]. The fog computing layer comprises (1) fog servers, which are responsible for computing, communicating, storing, and processing medical data, and (2) the fog scheduler, which is connected to IoMT devices to execute medical data analysis, access medical data from resource and patient record databases, and manage resource scheduling [72][73]. Despite the longer transmission latency in the fog computing layer than the edge computing layer, it has more storage and computational power. Therefore, results from the fog computing layer can be transferred directly to cloud computing for additional processing.

3.2.5 Gateway layer

The Gateway layer connects the fog devices and the cloud server. It processes and filters incoming medical data from the fog computing layer before sending it to the cloud computing layer. It collects and organizes medical data from many sensor devices for efficient processing, performs early analytics and data preparation to reduce data load on the cloud, and transforms medical data into a format suitable for cloud-based processing [58-62]. The gateway layer supports communication and data transfer between the fog computing and cloud layers, where data is stored, processed, or analyzed while ensuring a secure and efficient information interchange [64]. The gateway devices use communication protocols like Wi-Fi and cellular networks to send the acquired medical data to the cloud [68].

3.2.6 Cloud computing layer

The cloud computing layer comprises a centralized computing infrastructure, services, and platforms that enable medical data storage, processing, management, and delivery of healthcare services and applications via the Internet [58-61]. A proxy server establishes the transmission medium between the cloud server and fog nodes [73]. The cloud computing layer receives massive amounts of preprocessed historical and real-time medical data from the fog computing layer, uses cloud-based resource devices to complete tasks left unfinished in the fog layer, analyzes and stores the medical data to perform big data computation tasks such as disease diagnosis, and caregivers use the cloud to track patient medical analysis results [67][71][73]. Amazon Web Services, IBM Cloud, Oracle Cloud, Salesforce Health Cloud, Google Cloud Platform, Microsoft Azure, and Dell EMC Elastic Cloud Storage are some of the most popular cloud computing and storage systems used in IoMT. Cloud computing platforms use filtering and selective storing strategies to permanently store patients' medical data

[70]. Patient medical data are regularly uploaded and retrieved from the cloud as a backup in case of a system failure, breach, or vulnerability [62].

3.2.7 Blockchain layer

The Blockchain layer acts as a decentralized and immutable ledger, securely recording and tracking transactions and medical data transfers across various entities in the IoMT ecosystem. The Blockchain layer's major components include the distributed ledger, smart contracts, consensus mechanism, identity and access management, encryption and data privacy, and integration of other systems [74]. The Blockchain securely stores non-malicious medical data or files in a decentralized and immutable ledger. The Blockchain disseminates the ledger across all members, including healthcare provider entities. It notifies all members if a cybercriminal attempts to alter the recorded medical data, enhancing robust IoMT transparency [75]. A smart contract validates patient medical data based on predefined requirements, ensuring validation occurs when the healthcare practitioner meets those conditions. The InterPlanetary File System receives the data, hashes the raw medical data, and improves the Blockchain network's response time. The Blockchain stores hashed medical data shielded against data integrity threats [76]. Integrating Blockchain technology into IoMT architecture can improve security, data integrity, and interoperability.

3.2.8 Data analytics layer

The data analytics layer extracts insights, patterns, and valuable information from the massive volumes of medical data generated by the sensor layer within the IoMT ecosystem. The components and functions of the data analytics layer include collecting, storing, preprocessing, cleaning, integrating, analyzing, mining, visualizing, and reporting medical data, instant analytics, ensuring medical data security and privacy, improving healthcare system scalability and performance, and providing feedback and continuous improvement. The layer uses algorithms, machine learning models, and analytics tools to extract meaningful insights from medical data, perform instant medical data processing and analysis, enable predictive analytics, detect anomalies, and help healthcare professionals make decisions [77]. Big data analytics techniques analyze and aggregate medical data, extracting knowledge to inform ambulance services and doctors about patients needing diagnoses and health checkups [70].

3.2.9 Security layer

The security layer consists of protocols, technologies, and practices used to protect sensitive medical data generated by the sensor layer from unauthorized access or tampering, ensure compliance with privacy regulations, protect against cybersecurity threats, and ensure the integrity, confidentiality, and availability of information within the system [75]. The security layer of IoMT architecture employs a variety of protocols, technologies, and measures, including encryption mechanisms, access control, authentication and authorization systems, audit trails and logging, firewalls, intrusion detection/prevention systems, TLS and SSL, endpoint security, data loss prevention, and regular security assessments, updates, and penetration testing [64].

3.2.10 Application layer

The application layer is a system layer located at the top of other layers in which diverse healthcare software applications and services work together to provide particular functions and solutions to enhance healthcare delivery, patient care, and overall efficiency in the IoMT ecosystem [58-61][78]. It comprises all entities for whom the medical data is intended, such as medical devices, hospitals, pharmacies, laboratories, medical institutions, ambulances, and government healthcare organizations that use validated medical data from the sensor layer for rapid drug development, early diagnosis, easy tracking and reporting of disorders, and faster clinical trials [69][76][77]. The application layer comprises many software programs, platforms, and services that provide communication, data processing, analysis, and decision-making within the IoMT ecosystem [63][78]. Some of the software applications and platforms in the application layer of IoMT architecture include electronic health records systems, telehealth platforms, telemedicine and remote monitoring platforms, clinical decision support systems, health information exchange platforms, wearable devices, and health apps, data analytics and business intelligence, patient engagement platforms, and population health management systems [64][78]. Through these applications, healthcare professionals, patients, and caregivers can interact and access instant patient medical data collected by the IoMT devices, allow healthcare professionals to visualize medical data and prompt alerts, permit healthcare professionals to monitor and diagnose patients on a smart device, monitor patients' health status, enables instant patient health updates and healthcare data insights, allow caregivers to monitor patient's vital signs on their smart device, and make informed decisions concerning diagnosis and treatment [64][65].

3.2.11 Regulatory layer

The regulatory layer is an organized framework of policies, guidelines, standards, and laws regulating IoMT's design, development, deployment, and operation. This layer guarantees that healthcare practitioners follow legal and ethical guidelines, preserve patient privacy and confidentiality, and maintain the integrity and security of medical data. The primary goal of this layer is to ensure that the IoMT complies with regulations such as the Health Insurance Portability and

Accountability Act (HIPAA), Food and Drug Administration (FDA), and General Data Protection Regulation (GDPR), therefore guaranteeing the IoMT's safety, effectiveness, and compliance with healthcare requirements [64]. The regulatory layer includes data privacy and security regulations, interoperability standards, clinical governance, ethical guidelines, compliance monitoring and auditing, risk management, adherence to healthcare regulations, and legal and regulatory compliance training.

These layers collaborate to form a comprehensive and efficient IoMT architecture that uses cutting-edge technology to improve healthcare delivery and outcomes.

3.3 Practical applications of IoMT architecture

The architecture of the IoMT integrates diverse technologies and methodologies designed to enhance the efficiency, accessibility, and quality of healthcare services. By leveraging interconnected devices, communication protocols, data management systems, and advanced analytics, IoMT architecture enables seamless monitoring, diagnosis, and treatment processes. Table 2 summarizes the practical applications of this architecture, showcasing its transformative impact on modern healthcare.

TABLE II. PRACTICAL APPLICATIONS OF IOMT ARCHITECTURE.

S/No	Application of IoMT architecture	Description	References
1	Remote patient monitoring	Patients with chronic diseases, such as diabetes or heart disease, are given intelligent wearable devices with sensors that monitor vital indicators, including heart rate, blood pressure, blood glucose, and activity levels.	[26][27][29][60][61] [79][80]
2	Monitoring pregnancy	In-home self-monitoring, one of the essential components of prenatal healthcare, enables pregnant women to use pregnancy-related wearable technologies such as fetal monitors and multi-functional health screening tools to manage and monitor maternal health indicators such as blood pressure, fetal blood sugar, fetal heart rate, oxygenation, pulse, lipids, and electrocardiograms.	[26-28][79]
3	Monitoring sports athletics	Wireless technologies, body sensors, and fitness trackers in the exercise space substantially influence life efficiency and health systems' reliability. Wearable devices evaluate and analyze physiological considerations, advance health, enhance exercise compliance among diverse groups, from patients to expert athletes, and monitor heart rate, respiratory rate, and exercise rhythm continuously and instantly.	[26][28][79][81]
4	Telemedicine	The IoMT facilitates remote consultations by integrating communication channels and diagnostic technologies. Devices that transmit data to clinicians for remote review include portable ECGs and digital stethoscopes. By lowering physical obstacles, it provides high-quality care to underserved locations and gives doctors access to comprehensive patient metrics during consultations.	[60][61][80][81]
5	Personalized healthcare	The IoMT uses data-driven insights to provide customized treatment strategies. Smart pillboxes alert patients and caregivers to ensure they follow recommended prescriptions. Wearable technology tracks lifestyle behaviors (e.g., sleep and activity) and recommends changes.	[55][60][61]
6	Optimization of hospital workflow	In healthcare facilities, the IoMT helps automate and streamline clinical processes. Systems with RFID capabilities monitor the whereabouts and usage of vital equipment, such as wheelchairs and ventilators.	[60][61][82]
7	Early warning systems and real-time diagnostics	IoMT devices use artificial intelligence algorithms to identify irregularities and send alerts for prompt action. Devices automatically alert emergency services when they detect heart attacks or arrhythmias. Hospital biosensors detect infections or check for pollutants in the air. Wearable ECG and Electroencephalography scans for anomalies in heart or brain activity.	[81]
8	Therapy and rehabilitation	IoMT uses adaptive and interactive technologies to help rehabilitation programs. Wearable technology allows for real-time regimen adjustments and progress tracking. Interfaces between the brain and machines enable people to recover from brain injuries or strokes. Transcutaneous electrical nerve stimulation units deliver targeted therapy effectively.	[55][83]
9	Drug delivery and medication systems	IoMT interfaces with sophisticated medication delivery systems to guarantee exact time and dosage. Insulin pumps automatically modify insulin dosage in response to ongoing blood glucose testing. Sensors for inhalers track and report medication adherence for chronic obstructive pulmonary disease or asthma. Implantable drug systems release medications for ailments like cancer or chronic pain in a controlled, programmable manner.	[81][82]

10	Systems for responding to emergencies	In emergency scenarios, IoMT improves response efficiency. Wearable panic buttons provide instant alerts for older people or those in danger. While traveling, IoMT-enabled ambulances provide real-time patient data to hospitals. IoMT sensors monitor environmental risks and casualties.	[55][81]
11	Clinical trials and research	IoMT devices make it easier to collect data in various real-world contexts. Real-time data lessens reliance on self-reports. IoMT devices facilitate remote involvement, broadening the pool of candidates. Ongoing monitoring produces long-term, thorough datasets.	[34][58]
12	Epidemic management and public health	The IoMT helps with reaction planning and extensive health monitoring. Wearable technology monitors possible infectious disease exposure, and sensors compile data on population health. Digital platforms plan follow-ups and guarantee compliance.	[60][61][81][82]
13	Home medical care	Because of the IoMT, patients can receive medical care and monitoring in the convenience of their own homes. Doctors receive readings from thermometers, glucometers, and blood pressure monitors.	[60][61]
14	Remote surgery	Skilled medical professionals can operate on patients remotely from a distance using robotic arms and related technologies. The remote surgeon commands and controls the robots at the surgical site. Through this facility, patients worldwide can access the knowledge of qualified surgeons without going to the surgical site. The widespread use of IoMT applications and its communication network makes this feasible.	[80][82]
15	Treatment and detection of diseases	Through sensor-based medical devices that continuously monitor patients' vital parameters, such as blood pressure, temperature, blood sugar, oxygen level, etc., and notify the healthcare service provider via the IoMT communication network, the IoMT aids in the early detection of several diseases. By employing colorful wearable clothing with sensors, the IoMT assists in identifying the early signs of a fatal illness, such as breast cancer, and its recurrence even after successful treatment and cure. Heart attack symptoms can be easily recognized by tracking and monitoring wearable smart devices, such as smartwatches and intelligent pacemakers, and alerting medical professionals and the patient's skin. A smart inhaler helps prevent and reduce asthma attacks by alerting users to potential triggers, such as dust, smoke, or pollen, enabling them to take precautions in advance. Through the IoMT communication network, patients can receive prompt advice and treatment from knowledgeable medical professionals in addition to preventing and identifying these illnesses.	[60][61][81][82]
16	Secure drug supply chain management	With smart devices like intelligent tags affixed to drug bags, IoMT helps expedite and enhance the process of managing the drug supply and guarantees the safety and security of drugs delivered from being counterfeited. To ensure that patients receive their prescribed, high-quality medications safely, these smart tags aid in appropriately distributing, monitoring, and preventing drug duplication. The smart device notifies the relevant authority in charge of ensuring the security of drug supply change management if someone attempts to exchange the medications for duplicates.	[82]

3.4 Security Requirements in the IoMT

Given the sensitivity of healthcare data and the critical nature of its applications, ensuring robust security in the IoMT environment is of utmost importance. This section explores the essential security requirements for communication within the IoMT ecosystem.

3.4.1 Confidentiality

In the IoMT context, confidentiality involves safeguarding medical information and ensuring the privacy of sensitive patient data transmitted across the communication environment. Protecting healthcare data is crucial to prevent unauthorized access, eavesdropping, or interference by malicious entities that could compromise patient safety or misuse sensitive medical information. Encryption techniques, such as AES and RSA, are vital for securing medical data at rest and during transmission. Secure communication protocols like TLS/SSL can also prevent unauthorized access. While policies provide general guidelines, implementing network access controls and data encryption is critical to maintaining confidentiality within the IoMT ecosystem [79][82][84][85].

3.4.2 Privacy

Privacy protects patients' data from unauthorized disclosure and illegal exploitation. Many countries have implemented specific regulations such as GDPR and HIPAA to govern patient health data collection and storage and uphold privacy

standards. The IoMT system adheres to these regulations, enabling users to access their private data while complying with legal requirements [79][85].

3.4.3 Integrity

Integrity in the IoMT communication network refers to ensuring the accuracy and consistency of data transmitted between entities, preventing it from being altered or manipulated. Data modifications can occur accidentally or intentionally, often due to malicious actions by unauthorized users. The integrity property guarantees that data remains intact during wireless transmission and at rest, safeguarding it from unauthorized alterations or deletions. It is particularly critical in healthcare, where data represents diagnoses, treatments, and health statuses [82][84]. Implementing robust security measures like digital signatures and cryptographic hash algorithms like SHA-256 ensures data integrity and prevents unauthorized modifications. Additionally, integrity-checking mechanisms are necessary to detect and mitigate tampering attempts [79][85].

3.4.4 Availability

Availability refers to the ability of network services and resources in the IoMT communication environment to remain accessible to legitimate users whenever needed, even in the face of attacks such as DoS attacks [82][84]. Ensuring availability involves maintaining the continuous operation of IoMT systems through regular updates, performance monitoring, and promptly addressing any issues. Additionally, implementing redundant data storage and alternative transmission routes can help mitigate the impact of DoS attacks and ensure uninterrupted access [79][85].

3.4.5 Non-repudiation

Non-repudiation holds authorized users accountable for their actions within the IoMT communication environment. It guarantees that no system activity can be denied by providing proof that the intended source sent the messages, the correct recipient received them, and the integrity of the transmitted messages was maintained [82][84]. This property prevents users from denying their involvement in previous system activities or commitments, requiring them to take responsibility for their actions and consequences. Non-repudiation also allows the system to confirm the presence or absence of specific actions. Digital signature techniques are a straightforward and effective method for achieving non-repudiation [79][85].

3.4.6 Authentication

Authentication ensures the genuineness of entities, such as users, smart devices, servers, and gateways, and the authenticity of messages exchanged within the IoMT communication environment. By validating the identity of communicating entities, authentication enables these entities to mutually verify one another and establish secure session keys before transmitting any messages, thereby mitigating potential attacks [79][82][84][85]. Given the limited memory and processing power of specific IoMT devices, lightweight authentication algorithms have become increasingly prevalent. These algorithms overcome the computational challenges posed by traditional cryptographic protocols while ensuring that only authorized devices and users can access the IoMT network.

3.4.7 Authorization

Authorization determines the access rights and privileges assigned to authenticated users or devices, enabling them to access and use specific resources within the IoMT communication framework. Authorization typically follows authentication in any secure network to improve security and safeguard against potential attacks [82]. In this context, only trusted entities with the necessary skills or expertise should be allowed to perform critical actions, such as issuing commands to medical IoMT devices, updating software, or installing security patches on these devices [79][85].

3.4.8 Anonymity

The IoMT system protects privacy by concealing the identities of patients and physicians when unauthorized users interact. This anonymity is maintained during communication between patients and physicians, preventing their identities from being disclosed. Even in the presence of passive attacks, which can observe actions but not identify individuals, the system safeguards the confidentiality of both parties [79][85].

3.4.9 Accountability and auditability

In IoMT systems, accountability ensures that entities are responsible for their actions, making it possible to trace activities back to them, which holds them accountable for safeguarding the security and privacy of healthcare professionals and patient data. All healthcare information is meticulously recorded within the IoMT, requiring every stakeholder to recognize their role in protecting confidential patient data and preventing unauthorized access, data breaches, or misuse of IoMT systems. These recorded logs serve as valuable tools for identifying users responsible for specific actions or tracing IoMT devices in the event of security issues. Auditing involves continuously recording, tracking, and monitoring user behavior within IoMT systems to assess security measures and ensure compliance with legal regulations, industry standards, and best practices. Intelligent healthcare systems log user activities chronologically, such as login times, access events, and data modifications, holding users accountable for their interactions with IoMTs and sensitive patient information. Auditing protects patient data

and ensures the security and integrity of healthcare systems and devices. However, it also detects unauthorized access, monitors potential data breaches, evaluates system vulnerabilities, and verifies adherence to regulatory and industry standards [79].

3.4.10 Access control

Access control manages and restricts access to IoMT devices, sensitive patient data, and other resources, ensuring that only authorized entities can gain entry. Healthcare users are assigned specific access levels based on their roles and responsibilities. The policy defines these access levels based on the privileges and rights granted to each healthcare professional by the patient or a trusted third party. Patients can control who has access to their sensitive healthcare records through consent. By enforcing access restrictions according to user roles and permissions, access control ensures that users can only view the information necessary for their tasks, adhering to the principle of least privilege. Role-based and attribute-based access controls are commonly implemented in IoMT systems and applications to protect sensitive patient data, maintain the integrity of IoMT devices, and ensure compliance with regulations such as HIPAA and GDPR [79].

3.4.11 Reliability

Reliability in IoMT systems refers to their capacity to consistently provide accurate and timely healthcare services while upholding the confidentiality, integrity, and availability of sensitive health data, even in the face of various network issues, system or hardware failures, and fluctuating environmental conditions. This quality is especially crucial in intelligent healthcare networks, where IoMT devices are responsible for sensing, collecting, and transmitting healthcare data in high-risk environments. Reliability guarantees the continuous delivery of secure, trustworthy healthcare services while safeguarding sensitive patient information and privacy [79].

3.4.12 Resiliency

Resilience refers to the ability of IoMT devices and processes to withstand and adapt to challenges, disruptions, and unexpected events while maintaining their functionality and performance. Intelligent healthcare systems rely on interconnected IoMT devices, networks, and healthcare data to provide efficient and effective services. The IoMT systems must withstand system outages, cyberattacks, natural disasters, and other emergencies without compromising patient safety or the integrity of medical information to ensure uninterrupted patient care and data security. Resilience also involves safeguarding IoMT devices against physical tampering, theft, or unauthorized access, using tamper-evident hardware and secure fundamental storage mechanisms. Resilient IoMT systems promote redundancy, robustness, flexibility, and adaptability, ensuring consistent delivery of high-quality healthcare services, even in challenging situations. This resilience enhances patient safety, privacy, and trust in intelligent healthcare environments while preserving patient data and healthcare systems' confidentiality, integrity, and availability [79].

3.4.13 Fault tolerance

Fault tolerance is the ability of an IoMT system to maintain its functionality and continue delivering healthcare services despite faults or failures caused by technological malfunctions, human errors, or malicious attacks. Many IoMT systems rely on IoT, cloud computing, and big data analytics technologies to enhance patient care, streamline healthcare operations, and improve efficiency. However, these technologies can introduce vulnerabilities that adversaries might exploit, raising significant cybersecurity concerns. Fault tolerance ensures that an IoMT system provides services in the presence of defects. Healthcare providers prioritizing fault tolerance as a fundamental cybersecurity principle can enhance system resilience, reduce potential risks, and ensure the uninterrupted delivery of high-quality healthcare services while protecting patient data and privacy [79].

3.4.14 Freshness

Freshness refers to the ability of entities in the IoMT to quickly transmit new, up-to-date, and relevant healthcare data, ensuring that the information exchanged is freshly generated rather than a replay of outdated messages, which helps defend against replay attacks in the IoMT network, where attackers may attempt to intercept and resend old messages [82]. By linking sensitive patient healthcare data and IoMT devices to IoMT networks, freshness ensures that healthcare systems and data remain accurate and current, supporting effective patient care, medical research, and decision-making processes [79][85].

3.4.15 Third-party protection

Third-party protection involves securing network resources and sensitive patient information within the IoMT communication environment from potential harm or interference by external parties [82]. It ensures that external entities, such as service providers, cloud platforms, and vendors, are properly vetted and secured when interacting with medical devices or patient data. This protection helps safeguard against potential vulnerabilities introduced by third parties, such as unauthorized access, data breaches, and malicious attacks.

3.4.16 Forward secrecy

Forward secrecy ensures the security of past communications between IoMT devices, patients, and healthcare professionals, even if the encryption key used for those communications is later compromised. Attackers cannot decrypt previously encrypted communications if they access the encryption key [79][84][85]. This mechanism prevents attackers from accessing exchanged data, even if they capture a device [82]. Additionally, forward secrecy safeguards future transmissions of data and keys, ensuring that even if older data or keys are compromised, the security of new communications remains intact.

3.4.17 Backward secrecy

Backward secrecy in the IoMT focuses on protecting previously exchanged messages when a new intelligent healthcare device joins the communication network. It ensures that past communications remain confidential, thus safeguarding the privacy of healthcare data [82][84]. Even if cybercriminals later obtain long-term private keys, they cannot decrypt previous messages or access historical healthcare data [79][85]. Time-based authentication mechanisms, such as time-sensitive keys, achieve backward secrecy by generating valid keys only when the clocks of both communicating nodes are synchronized.

3.4.18 Robustness

Robustness in the context of IoMT refers to the capacity of devices to sustain their operation and performance despite facing various challenges, uncertainties, and adverse conditions. It ensures that IoMT systems can deliver services accurately, swiftly, and securely while effectively addressing the inherent challenges, uncertainties, cyber threats, and attacks within healthcare environments, maintaining functionality and integrity. To achieve this, IoMT incorporates strong security measures and complies with regulations, industry standards, and best practices to minimize cybersecurity risks, protect sensitive healthcare data, and ensure the system's security, integrity, and availability [79].

3.4.19 Revocation

Revocation refers to removing or invalidating access privileges or digital certificates for healthcare users, IoMT devices, or entities no longer authorized to access specific innovative healthcare resources or systems. For instance, a patient can revoke a healthcare professional's permission to access their medical records [79][85].

In the IoMT network, ensuring security typically requires a combination of cryptographic methods, robust protocols, physical protections, and adherence to industry standards. This integrated approach helps establish a secure and resilient healthcare data and devices ecosystem.

4. CRYPTOGRAPHIC TECHNIQUES IN THE IOMT

Cryptographic techniques encompass various methods and algorithms designed to ensure secure communication, protect data integrity, and maintain the confidentiality and authenticity of information [86]. These techniques are central to the field of cryptography, which involves encrypting and deciphering data to prevent unauthorized access [86]. Cryptographic algorithms employ advanced mathematical and logical techniques to secure and protect data and communications. One of their primary applications is data encryption, which ensures that data are encrypted at the source and decrypted only at the destination, preventing unauthorized access during transmission [33]. In the IoMT, several cryptographic schemes facilitate secure peer-to-peer communication by safeguarding the confidentiality and integrity of health records over public networks [32][87]. Cryptographic techniques are employed to protect healthcare data privacy and ensure the authenticity of healthcare information. These include symmetric-key, asymmetric-key, and hash-based cryptography [88]. These methods often work with digital signatures and cryptographic primitives such as identity-based encryption, predicate/hierarchical pantograph encryption, and fully homomorphic encryption. The cryptographic algorithms used in the IoMT include DES, Triple DES, AES, RSA, ECC, DSA, and hash functions like SHA-2 and SHA-3. Hash-based Message Authentication Codes (HMAC), digital certificates, and quantum cryptography are also essential in securing healthcare data. These cryptographic techniques are critical in protecting healthcare data at various stages, whether at rest, in transit, or during backup processes. They ensure that data remains secure when transmitted to the cloud or between storage systems and transmission points. Moreover, cryptographic methods are integrated into IoMT devices and sensors to support safe communication [79]. Symmetric-key cryptography, asymmetric-key cryptography, hash functions, and digital signatures are the categories of cryptographic techniques in the IoMT [79].

4.1 Symmetric key cryptography

Symmetric encryption is one of the simplest and most widely recognized data encryption methods, relying on a single secret shared key for encryption and decryption [84]. In this method, the sender encrypts the plaintext using a secret key to produce ciphertext, which the recipient then decrypts back into plaintext using the same key. This approach, known for its simplicity and longevity, depends on the sender and recipient sharing the same secret key, which must remain confidential. A symmetric encryption scheme typically consists of five key components: plaintext, encryption algorithm, secret key, ciphertext, and decryption algorithm [86]. Fig. 7 illustrates the simplified symmetric encryption model.

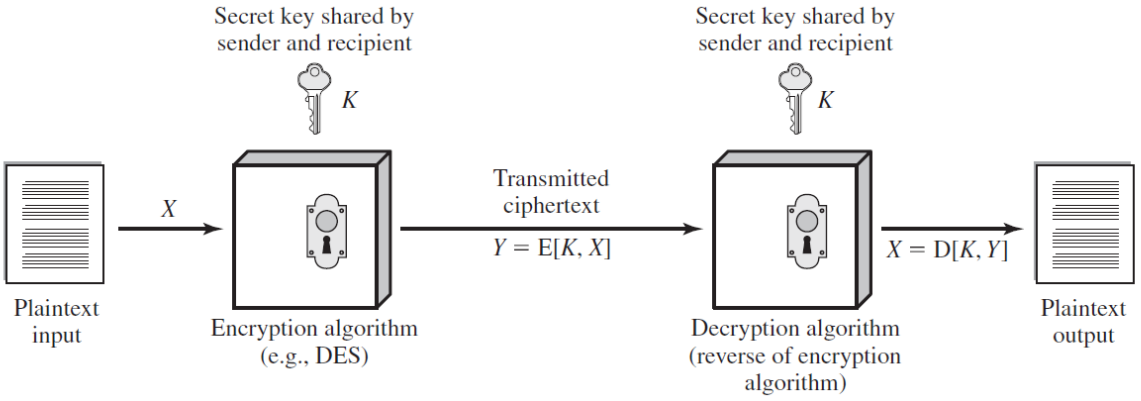
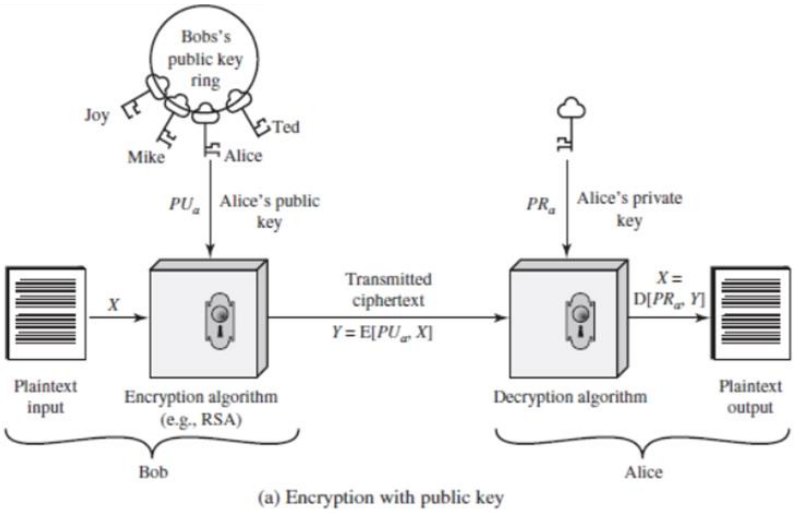


Fig. 7. Illustrates the simplified symmetric encryption model [86].

Well-known examples of symmetric encryption algorithms include Blowfish, AES, DES, RC5, and RC6 [37]. In the IoMT context, symmetric encryption addresses the challenges posed by resource-constrained devices and the need for real-time data transmission. Since symmetric encryption uses the same key for encryption and decryption, it is efficient and fast, making it well-suited for IoMT devices with limited computational capabilities. However, managing encryption keys in distributed IoMT systems can be complex [37][88]. Among the various symmetric encryption techniques, AES stands out as the most commonly used algorithm in IoMT due to its high speed and low resource consumption. Symmetric encryption is crucial in ensuring the security of sensitive medical data transmitted between IoMT devices, such as wearable health trackers and central servers. It also protects patient information stored on edge devices or in the cloud and secures communication between healthcare sensors, thus maintaining data confidentiality and integrity.

4.2 Asymmetric Key Cryptography

Asymmetric key cryptography, or public-key cryptography, uses a pair of keys—public and private keys—to facilitate secure communication [84]. In this system, the sender encrypts the message using the recipient's public key, ensuring that only the recipient can decrypt it with the corresponding private key. The public key is shared openly with others, and the private key remains known only to its owner. The two cryptographic keys are distinct but mathematically related, and they have significant implications for confidentiality, key distribution, and authentication. A typical public-key encryption system comprises six essential components: plaintext, the encryption algorithm, the public and private keys, ciphertext, and the decryption algorithm [86]. Fig. 8 illustrates the public-key cryptography.



(a) Encryption with public key

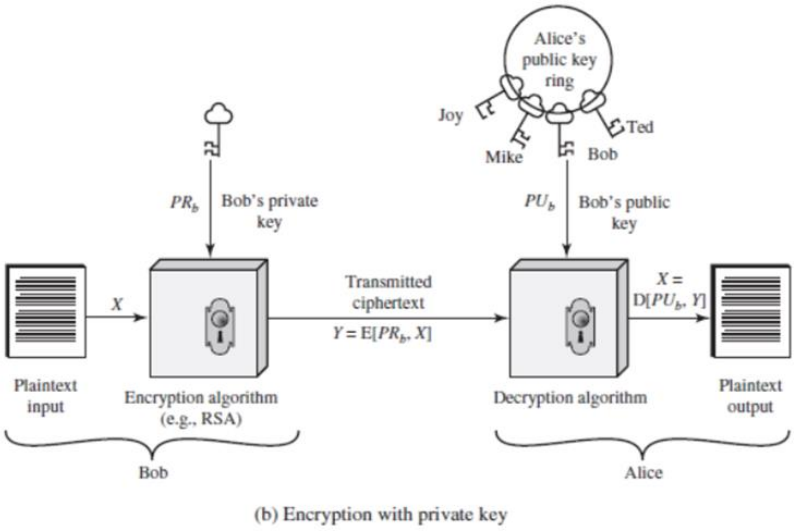


Fig. 8. Shows asymmetric key cryptography [86].

Popular asymmetric encryption algorithms, such as ElGamal, DSA, RSA, and ECC, are widely used in IoMT systems [4]. ECC underpins robust authentication schemes in the IoMT, enabling secure key exchange, strong authentication mechanisms, and resilience against cyber threats. Using ECC, IoMT systems safeguard medical data's confidentiality, integrity, and availability while ensuring seamless connectivity and interoperability within the healthcare ecosystem [4][89]. Although asymmetric cryptography provides higher security than symmetric methods, it requires more computational resources, making it less suitable for energy-constrained IoMT devices [36]. For example, RSA has notable performance limitations, ten times slower than ECC at 128-bit security levels. At 256-bit security levels, this gap widens, with RSA performing 50 to 100 times slower than ECC [4]. Most IoMT systems depend on conventional cryptographic algorithms such as RSA and ECC. However, these algorithms, reliant on the complexity of integer factorization, are highly susceptible to quantum computing attacks [30]. Lightweight lattice-based cryptography offers a solution by enhancing IoMT authentication protocols to withstand quantum attacks. This approach ensures robust security, efficiently generates keys, and supports the scalability and performance needs of IoMT devices [30]. Algorithms like the Low Energy Algorithm (LEA) and SPECK protect IoMT systems while minimizing energy consumption effectively. Homomorphic encryption represents a significant advancement in data security, enabling computations directly on encrypted data without decryption, generating an encrypted output that matches the results of a plaintext operation once decrypted [33][90]. This approach ensures that data privacy and integrity remain intact, even when third-party systems process or analyze the data, effectively preventing unauthorized access or interpretation of sensitive information [33]. This feature is essential for IoMT cloud-based systems, where secure data processing is necessary. RSA's high computational cost continues to pose a significant barrier to adopting IoMT technologies [38]. In the IoMT, asymmetric cryptography is crucial in establishing secure connections, authenticating medical devices and servers, and facilitating the secure exchange of symmetric keys for ongoing communication. While particularly effective for applications requiring robust authentication and secure key exchange, asymmetric encryption is typically slower than symmetric encryption [91].

4.3 Hashing Functions

Hash functions are cryptographic algorithms designed to generate a fixed-length hash value or message digest from an input message, ensuring data security and integrity through properties such as collision resistance, irreversibility, and the avalanche effect [33][90]. Hash-based cryptography is effective for data encryption because it is challenging to deduce the input from a given output, and the probability of two different inputs producing the same output (a hash collision) is very low. Finding a hash collision requires searching the entire search space, which is computationally infeasible with classical computers [33][90]. Cryptographic hash functions are fundamental tools in cryptography, serving various security purposes such as ensuring authenticity, enabling digital signatures, generating pseudo-random numbers, supporting steganography, and facilitating time stamping [86]. These functions fall into two main categories: keyed hash functions, which use a secret key and are commonly called Message Authentication Codes (MACs), and unkeyed hash functions, which do not rely on a secret key and are generally referred to as hash functions. Unkeyed hash functions can be further classified based on their properties into one-way hash functions, collision-resistant hash functions, and universal one-way hash functions, each offering specific security guarantees. Standard hash functions include Message Digest 5 (MD5), SHA variants (SHA-1, SHA-2, and SHA-3), BLAKE2, RIPEMD, and WHIRLPOOL. Fig. 9 illustrates the process of hashing data using the SHA-256 algorithm to produce a unique, fixed-length hash value.

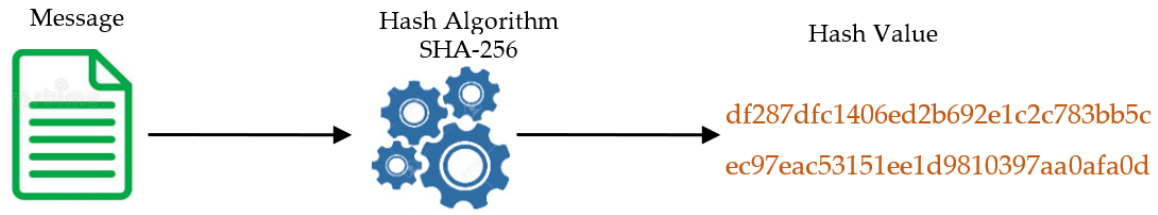


Fig. 9. Illustrates the process of hashing data using the SHA-256 algorithm to produce a unique, fixed-length hash value [92].

In the IoMT, these functions play a critical role in verifying the accuracy and legality of stored or transmitted data, offering faster execution in software than traditional encryption algorithms like DES. Hash functions secure medical data, such as patient records and imaging files, by enabling integrity verification through recalculated hashes. An information security scheme for the IoMT integrates AES-256, RSA, SHA3-512, and Least Significant Bit embedding to enhance the protection of medical scans and images [93]. Cryptographic hash functions, such as SHA-256, are widely used in IoMT systems to safeguard sensitive medical information and verify message integrity due to their strong resistance to collisions and ensure the secure transmission of medical data across networks while maintaining user authentication and data confidentiality [93-96]. They underpin secure protocols like TLS/SSL, facilitating encrypted and authenticated communication between IoMT devices and servers. Hash functions ensure data integrity during transmission, securely store sensitive information like hashed patient passwords, and detect tampering with medical records or diagnostic data.

4.4 Digital Signature

A digital signature is a cryptographic method to ensure digital data's integrity, authenticity, and non-repudiation. It verifies that the data is unchanged, confirms the sender's identity, and prevents the sender from denying their involvement in the transaction. It is a mathematical method comparable to a handwritten signature but significantly more secure. Digital signatures rely on asymmetric cryptography to authenticate data and maintain its integrity. They are crucial in ensuring non-repudiation, an essential aspect of information security. As highlighted by Bhushan et al. [84], they widely prove the origin and integrity of data, making it difficult for the sender to deny their involvement in a transaction or communication, ensuring accountability and trust in digital interactions, especially in sensitive or high-stakes environments. The significant characteristics of digital signatures include authentication, integrity, non-repudiation, and legal binding. A digital signature consists of three main components: (1) a hash function, which generates a fixed-size hash value (such as SHA-256 or SHA-3) from the data, ensuring that even minor alterations to the data result in a drastically different hash; (2) public key cryptography, where the hash is encrypted and decrypted using algorithms like RSA or ECC, providing security for the signature; and (3) a certificate authority (CA), which issues and verifies digital certificates to authenticate the ownership of the public key, ensuring the integrity and authenticity of the signature. Fig. 10 illustrates the step-by-step process involved in generating a digital signature.

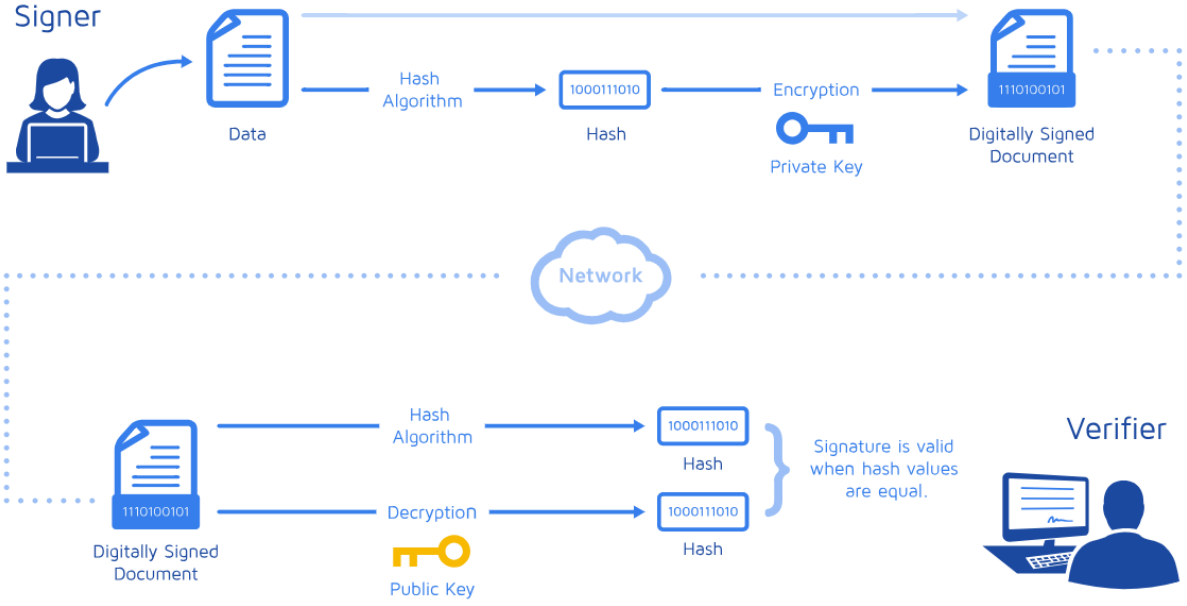


Figure 10. Illustrates the step-by-step process involved in generating a digital signature.

In the IoMT, digital signatures enhance online and offline security. They safeguard IoMT devices by leveraging the sender's private key to generate signatures and the corresponding public key for verification, ensuring data authenticity and integrity. Digital signatures protect against unauthorized firmware updates by requiring signed firmware, authenticating data from IoMT devices integrated into electronic health records, and verifying the legitimacy of data exchanges between patients and healthcare providers. They prevent unauthorized device-to-device data sharing between wearable ECG monitors and cloud servers and verify user identities before granting access to IoMT systems. Additionally, digital signatures authenticate devices and data sources, ensure the integrity of software patches, and help comply with medical data security regulations like HIPAA and GDPR. To address the resource constraints of IoMT devices, elliptic curve digital signature algorithms (ECDSA) are widely adopted due to their efficiency in preserving data privacy and enhancing security. For instance, sensor firmware in IoMT systems can integrate digital signatures with add-on software shims to intercept and validate wireless communications, relying on stored public keys of authorized users, such as medical staff, for verification. This approach not only ensures robust security but also addresses the unique challenges of healthcare applications, leveraging edge computing for secure communication between IoT devices and the cloud [6][79][84].

5. APPLICATION OF CRYPTOGRAPHIC TECHNIQUES IN SECURING THE IOMT

Table 3 summarizes the primary applications of cryptographic techniques in securing the IoMT.

TABLE III. SUMMARY OF THE MAIN APPLICATION OF CRYPTOGRAPHIC TECHNIQUES IN SECURING THE IOMT.

S/No	References	Application of cryptographic techniques	Brief description
1	[69][97-100]	Ensuring data confidentiality	Cryptographic techniques are used in IoMT to ensure the confidentiality of sensitive healthcare data. Encryption techniques such as AES and RSA transform medical data into unreadable formats, allowing only authorized entities to decrypt and access the data.
2	[42][101]	Ensuring data integrity	Cryptographic hash algorithms, such as SHA-256, ensure data integrity by verifying that transmitted data remains unaltered. These hash functions generate unique digital fingerprints for data; even the slightest change in the data will result in a different hash value. This capability helps prevent cybercriminals from modifying or falsifying sensitive information, such as health data. By detecting any corruption or tampering, IoMT systems can identify compromised data during transmission and when stored, thus safeguarding against unauthorized changes.
3	[4][78][102][103]	Authentication and access control	Cryptographic techniques, such as digital signatures and asymmetric encryption, play a crucial role in authentication by verifying the identities of devices, users, and systems. Digital signatures provide message certification, ensuring the communication has not been tampered with and originates from a specific sender. Hospitals use ECC-based authentication to secure access to electronic health records stored on cloud servers. Medical devices, including patient monitors and infusion pumps, are assigned verified ECC credentials, ensuring secure access and transmission of patient data over the network.
4	[104][105]	Non-repudiation	Non-repudiation ensures that neither the sender nor the recipient can deny the origin or transmission of data. In IoMT systems, digital signatures and cryptographic keys provide this assurance, confirming that communications and medical data come from authenticated and reliable sources. This is crucial for maintaining accountability in medical exchanges and preventing disputes related to data integrity. By guaranteeing that data can be traced back to its source, non-repudiation is vital in safeguarding trust and transparency within healthcare systems.
5	[40][41]	Secure data transmission	Cryptographic protocols like TLS ensure secure data transfer between IoMT devices, servers, and healthcare systems. They secure data while it travels via potentially weak channels and provide end-to-end encryption. In IoMT systems, TLS ensures data integrity and confidentiality while in transit. Because TLS encrypts network connections, it also helps to remove concerns related to eavesdropping and MitM attacks. Additionally, it protects against illegal access and interception of private medical information during communication.
6	[39][106][107]	Ensuring data privacy	Cryptographic algorithms, particularly homomorphic encryption, safeguard sensitive data during computations. It enables operations to be performed on encrypted data, producing an encrypted result that, when decoded, matches the outcome of performing the calculation on the plaintext. Additionally, differential privacy techniques introduce random noise to data, allowing for comprehensive analysis without compromising individual privacy. When applied to the IoMT systems, differential privacy ensures that healthcare professionals can analyze large datasets while protecting patients' identities and sensitive information. This approach preserves patient privacy and allows researchers, healthcare providers, and other stakeholders to conduct studies without endangering personal data.
7	[108][109]	Resource-efficient security for IoMT devices	Lightweight cryptographic algorithms that offer security without draining device resources are essential since many IoMT devices have constrained processing and storage capacities. Even devices with limited resources can safely send and store data

			thanks to lightweight encryption techniques like ECC and lightweight block ciphers (like PRESENT and SPECK), designed for usage in constrained IoMT contexts.
8	[110-112]	Protection against emerging threats	Cryptographic approaches are constantly evolving to combat new threats. Post-quantum cryptography methods aim to protect IoMT systems from upcoming quantum-based attacks. As computational power increases, these strategies will be essential to maintaining the security of the IoMT systems.
9	[113-115]	Ensuring trust in IoMT networks	Blockchain-based cryptographic approaches build trust in decentralized IoMT systems. Cryptography in Blockchain and IoMT systems can facilitate secure, transparent, and impenetrable data transfers between several devices and healthcare stakeholders, lowering the possibility of fraud, data manipulation, or unauthorized alterations. A cryptographic hash, which confirms the data source and tasks conducted, secures each transaction on the Blockchain.
10	[116-118]	Ensuring the availability of healthcare services	Cryptographic approaches can enhance availability by offering safe backups and protected data recovery methods. Secure recovery procedures guarantee the availability of vital healthcare services in the case of a system failure, cyberattack, or device compromise, which is especially crucial in IoMT since patients' health and well-being may be at risk if a device or service is unavailable.

Advancements in quantum computing technology have exposed significant security vulnerabilities in symmetric-key cryptography, asymmetric-key cryptography, hash functions, and digital signatures [33]. As quantum computing evolves, these cryptographic methods are increasingly at risk, challenging their ability to secure sensitive data effectively.

6. SECURITY ATTACKS ON CRYPTOGRAPHIC TECHNIQUES IN SECURING THE IOMT

In the IoMT context, cryptographic techniques are vital in securing sensitive health data transmitted between devices, servers, and healthcare professionals. However, these cryptographic methods are susceptible to security threats that undermine patient data privacy, integrity, and availability [119][120]. Below are some detailed security attacks targeting cryptographic techniques within the IoMT ecosystem.

6.1. Man-in-the-middle (MitM) Attacks

In a MitM attack, cybercriminals intercept and manipulate the communication between two parties, such as a medical device and a healthcare server, compromising the integrity and security of the data exchange [121]. This attack targets cryptographic protocols used for secure communication (e.g., SSL/TLS) and key exchanges (Diffie-Hellman or RSA) [121][122]. If the cryptographic techniques are weak or improperly implemented, attackers may exploit these vulnerabilities to decrypt messages or inject harmful data. Weak key exchange protocols, for instance, can allow attackers to impersonate legitimate entities. In insecure public key infrastructure, attackers can produce fake or vulnerable certificates that make IoMT systems trust the attacker's equipment, granting them access [48][79]. For example, an attacker could intercept the communication between an intelligent insulin pump and a hospital's server, potentially modifying dosage instructions sent from the healthcare provider and posing a risk to the patient's safety [123].

6.2. Side-Channel Attacks

Side-channel attacks exploit the physical characteristics of a device, such as power consumption, electromagnetic emissions, or execution time, to extract cryptographic keys or other sensitive information. They focus on exploiting the physical implementation of cryptographic systems rather than attacking the cryptographic algorithm itself. These attacks can involve techniques like timing analysis, power consumption analysis, or electromagnetic leakage to extract information about cryptographic keys. If an IoMT device's cryptographic module is exposed to such analysis, attackers could access sensitive information, including private keys, for encrypting or decrypting health data [18]. The attackers can use differential power analysis to analyze power consumption during encryption or decryption phases to obtain private keys [124]. Based on timing leakage, power analysis takes advantage of fluctuations in power drawn by a device to infer details about the cryptographic keys implemented [79]. It targets cryptographic algorithms implemented in IoMT devices and devices that perform encryption or decryption, especially those with weak physical protections. For example, an attacker can use differential power analysis to analyze the power consumption of a wearable cardiac monitor during its cryptographic operations, eventually deducing the encryption key [123].

6.3. Replay Attacks

Replay attacks occur when an attacker captures and retransmits valid data communications, misleading the recipient into believing the message is legitimate, leading to unauthorized access, or executing fraudulent commands [125]. This attack targets encrypted data transmission without time-sensitive validation and cryptographic protocols lacking nonce or timestamp mechanisms. Any device in the IoMT that uses either weak tokens or tokens that never expire for authentication purposes is highly susceptible. The attackers can steal these tokens and use them to gain unauthorized access to medical data [79][126]. The attackers can capture the primary authentication session token before transmitting it to the target IoMT devices. Later, they can use the replay attack to get into a legitimate connection between an IoMT device and the cloud server

[127]. If encryption or digital signatures lack mechanisms like timestamps or session keys, attackers could exploit this vulnerability to replay messages without detection. For example, an attacker captures a valid login session from a remote heart monitor and replays the authentication message to gain access to unauthorized patient data or device control.

6.4. Cryptanalysis Attacks

Cryptanalysis involves exploiting weaknesses in cryptographic algorithms to recover secret keys or plaintext data [128]. Attackers can use brute-force attacks, differential cryptanalysis, or linear cryptanalysis to break block ciphers or uncover the relationship between plaintext, ciphertext, and keys [129]. This attack targets weak or outdated encryption algorithms like DES, weak implementations of AES, and poorly implemented cryptographic libraries [128][130]. Attackers can potentially retrieve sensitive health data if IoMT devices use outdated or vulnerable cryptographic algorithms—such as those employing weak key sizes (e.g., 56-bit DES). For example, an attacker performs a differential cryptanalysis attack on an outdated IoMT device using the DES algorithm to recover encryption keys and access patient data.

6.5. Brute-Force Attacks

In brute-force attacks, attackers attempt all possible key combinations to decrypt encrypted data. Although modern cryptographic algorithms are computationally resistant to brute-force attacks, weak encryption algorithms with short key lengths or poor random number generation can make such attacks viable. If an IoMT device uses weak or predictable keys (e.g., DES, short AES key lengths) for encryption, attackers might successfully perform a brute-force search to find the correct key and decrypt the data [79][131]. For example, a glucose monitoring device using a weak encryption algorithm like 56-bit DES is susceptible to brute-force attacks, eventually enabling attackers to decrypt patient data.

6.6. Key Management Attacks

Maintaining the security of cryptographic systems relies heavily on effective key management. Attacks targeting key management—such as key theft, improper storage, or misuse—can compromise encrypted data [38]. It targets IoMT devices with weak or hardcoded cryptographic keys and poor key distribution methods, such as unsecured key exchanges. If IoMT devices retain cryptographic keys without traceable key storage methods, attackers can directly extract them from their memory, enabling them to decrypt protected data. This vulnerability remains prevalent, primarily if the IoMT devices are low-cost with little or no security hardware [132]. For example, if a software update exposes hardcoded encryption keys stored in an IoMT device's firmware, attackers can use them to decrypt all communications involving the device.

6.7. Insider Attacks

Insider attacks involve trusted individuals, such as healthcare workers or technicians, exploiting their access to IoMT devices or cryptographic keys to steal or tamper sensitive data [46]. These attacks target critical storage systems, authentication protocols, and cryptographic implementations within IoMT systems. Insiders can bypass security mechanisms to access encrypted data or keys, jeopardizing confidentiality and integrity. For example, a malicious insider could extract encryption keys from a hospital’s IoMT system, enabling unauthorized access to patient records or medical device configurations [79].

6.8. Denial-of-service (DoS) Attacks

A DoS attack overwhelms the cryptographic processing capabilities of an IoMT system, rendering it unavailable [133]. DoS attacks can disrupt encrypted communication channels, hindering authorized users from accessing critical information and impairing the overall functionality of secure systems. Attackers may exploit the computational complexity of cryptographic algorithms to exhaust resources. This attack targets cryptographic operations that require significant processing power (e.g., RSA, ECC) and IoMT devices with limited resources, such as wearable health monitors [134]. For example, an attacker floods an IoMT server with cryptographic requests, such as digital signature verifications, overwhelming the system and preventing legitimate communications from processing [45].

6.9. Phishing and Social Engineering Attacks

Phishing and social engineering attacks aim to deceive users—such as healthcare providers or patients—into disclosing cryptographic credentials, keys, or other sensitive data. These attacks might involve fake websites, emails, or phone calls that attempt to harvest login details or authentication credentials. If attackers acquire these cryptographic keys or credentials, they can impersonate legitimate users and gain unauthorized access to health data [79].

6.10. Chosen plaintext/chosen ciphertext attacks

Chosen plaintext and ciphertext attacks are significant threats to cryptographic systems, particularly those with weak encryption schemes. In a chosen plaintext attack, the attacker can deliberately select specific plaintexts for encryption and then analyze the corresponding ciphertexts. This attack allows adversaries to identify patterns or vulnerabilities in the encryption process, potentially uncovering sensitive information or deducing encryption keys [135]. Similarly, a chosen ciphertext attack allows the attacker to choose ciphertexts and obtain their decrypted outputs. By exploiting the decryption process, attackers can gather critical insights about the encryption key or plaintext data. These attacks are particularly

effective against poorly implemented cryptographic systems and can lead to severe security breaches [136]. Wireless medical devices, such as pacemakers, illustrate such attacks effectively. An attacker might generate specific medical commands for encryption and analyze the device's responses to discern encryption patterns. With this knowledge, the attacker could manipulate the pacemaker's functionality, demonstrating the real-world risks associated with these attack methods [137].

6.11. Malware Injection Attacks

Malware injection is a significant security threat in the realm of IoMT devices. Attackers can embed malicious code within these devices, enabling them to bypass security protocols or even manipulate cryptographic operations [138]. Suppose adequate protection mechanisms are not in place; malware can exploit vulnerabilities in the device's software to gain control over cryptographic keys or sensitive data, compromising the security and privacy of the system. Two common malware injection attacks are Trojan attacks and rootkits or firmware attacks. Trojan attacks involve threat actors infiltrating IoMT devices and deploying trojans to interfere with encryption processes. For example, a trojan could modify the encryption methods used by the device, rendering the resulting ciphertext vulnerable to cryptanalysis. On the other hand, rootkits embedded in the firmware present an even more insidious threat. These rootkits allow attackers persistent access to sensitive resources, such as cryptographic keys stored in the device's memory, enabling them to compromise security continuously [139].

6.12. Ransomware and Data Corruption Attacks

Ransomware attacks work by encrypting data and blocking authorized users from accessing it. This malicious tactic disrupts access to critical information, creating significant obstacles for individuals or organizations reliant on the affected systems. These attacks effectively hold the data hostage, preventing access to vital information and disrupting the IoMT and its networks. Such incidents can lead to the manipulation of sensitive data, interfering with the delivery of healthcare services, and undermining patient confidence in the reliability and security of their medical information [47]. In the context of IoMT, ransomware attackers often target patient data or medical records, either locking them within a device or making them otherwise inaccessible unless the demanded payment is made [140]. These disruptions can weaken healthcare services, delaying treatments and jeopardizing patient care. Attackers can also tamper with or poison IoMT data, leading to the contamination of patient databases or other sensitive health information. The impact of such attacks becomes even more severe when cryptographic methods fail to ensure data integrity. This vulnerability can result in catastrophic outcomes for healthcare decision-making processes, as corrupted or inaccessible data compromises the accuracy and timeliness of critical medical judgments [141]. Consequently, ransomware attacks on IoMT systems highlight the urgent need for robust cybersecurity measures in healthcare.

6.13. Firmware Tampering

Firmware tampering is a type of cyberattack where adversaries modify the firmware of IoMT devices to compromise security, and it can involve disabling encryption, introducing vulnerabilities, or installing backdoors to gain unauthorized access [142]. Such tampering undermines the integrity and security of these critical devices. A key target of firmware tampering is the cryptographic modules embedded within the firmware of IoMT devices. These modules, which include encryption algorithms and critical management systems, are essential for ensuring secure communication and data protection [44]. When compromised, they leave the devices and their communications susceptible to exploitation. For instance, an attacker might modify the firmware of an insulin pump to turn off its cryptographic functions. As a result, all subsequent communications with the device become unencrypted, exposing sensitive data to potential interception and manipulation [26]. Such breaches highlight the need for robust measures to secure IoMT firmware and safeguard patient safety.

6.14. Quantum Computing Threats

Quantum computing represents a significant future challenge to traditional cryptographic techniques such as RSA and ECC. Quantum algorithms, notably Shor's algorithm, can potentially solve the mathematical problems underpinning these cryptographic methods, rendering them ineffective, which poses a critical risk to systems relying on these encryption techniques, including the IoMT. IoMT devices commonly use traditional public-key cryptography methods like RSA and ECC for securing encryption, authentication, and key exchange processes [143]. A sufficiently advanced quantum computer could exploit vulnerabilities in these methods, breaking encryption protocols and exposing sensitive medical data. Attackers could compromise RSA encryption in IoMT devices, allowing them to decrypt confidential medical communications or remotely manipulate connected devices. This highlights the urgent need for post-quantum cryptographic solutions to secure future IoMT systems [144].

Cryptographic security is crucial for protecting sensitive data in IoMT environments. However, sophisticated attacks continue to exploit vulnerabilities in cryptographic implementations, posing significant challenges to data integrity, confidentiality, and system reliability. As a result, developing and deploying robust security solutions have become increasingly important to counter these threats. Table 4 highlights various security attacks targeting cryptographic techniques in IoMT systems and their impact on meeting critical security requirements.

TABLE IV. SUMMARY OF THE VARIOUS SECURITY ATTACKS TARGETING CRYPTOGRAPHIC TECHNIQUES IN IOMT SYSTEMS AND THEIR IMPACT ON MEETING CRITICAL SECURITY REQUIREMENTS.

S/No	Reference	Security Attacks	Brief Description	Violated Security Principle			
				C	I	A	Au
1	[48][79][121-123]	MitM attacks	Attackers intercept communication between IoMT devices and servers, potentially altering or stealing sensitive medical data.	✓	✓	×	×
2	[18][79][124][123]	Side-channel attacks	These attacks exploit cryptographic devices' physical characteristics (timing, power consumption, or electromagnetic leaks) to retrieve cryptographic keys or other sensitive information.	✓	✓	×	×
3	[79][125-127]	Replay attacks	Malicious actors capture and retransmit valid data packets to disrupt the communication between devices or servers, potentially leading to unauthorized access.	×	✓	×	×
4	[128-130]	Cryptanalysis	Attacks that target the cryptographic algorithms themselves, seeking weaknesses that could allow decryption without the key.	✓	×	×	×
5	[79][131]	Brute-force attacks	Attackers exploit computational power to guess encryption keys, primarily targeting systems that use weak cryptographic algorithms or insufficient key lengths.	✓	×	✓	×
6	[38][132]	Key management attacks	Weaknesses in generating, storing, or exchanging cryptographic keys create vulnerabilities that allow attackers to gain unauthorized access to the system.	✓	✓	×	×
7	[46][79]	Insider attacks	These occur when individuals with authorized access to IoMT devices or systems (e.g., healthcare staff or vendors) exploit their position to leak or alter sensitive data, bypass security controls, or sabotage cryptographic systems.	✓	✓	×	×
8	[45][133][134]	DoS attacks	A DoS attack floods IoMT systems or devices with excessive requests or traffic, overwhelming them and causing a loss of service. For cryptography, this could interfere with secure communication, leading to temporary shutdowns or degraded performance, making devices vulnerable to further exploits.	×	×	✓	×
9	[79]	Phishing and social engineering attacks	These attacks manipulate users into revealing sensitive information, such as cryptographic keys or passwords. Phishing uses fraudulent communication, while social engineering relies on psychological manipulation. They threaten the integrity of cryptographic protections in IoMT systems.	✓	✓	×	✓
10	[135-137]	Chosen plaintext/chosen ciphertext attacks	In these attacks, the attacker can choose a specific plaintext (message) or ciphertext (encrypted message) and analyze how the cryptographic system handles it. This helps attackers derive secret keys or break encryption schemes to protect IoMT data.	✓	×	×	×
11	[138][139]	Malware injection attacks	Malicious software is injected into IoMT devices to corrupt or hijack their operations. For cryptography, this could involve altering encryption keys or turning off cryptographic protections, allowing attackers to intercept or manipulate sensitive health data.	×	✓	✓	×
12	[47][140][141]	Ransomware and data corruption attacks	Ransomware locks or encrypts critical data in IoMT systems, demanding payment for its release. Data corruption attacks might alter or destroy sensitive healthcare data, rendering it unusable. Both threaten the integrity and confidentiality of cryptographic techniques used to secure IoMT.	×	✓	✓	×
13	[26][44][142]	Firmware tampering	Attackers gain control over the firmware in IoMT devices, modifying it to bypass security measures or weaken cryptographic functions. This can expose sensitive data or allow unauthorized access to medical systems.	✓	✓	✓	×
14	[143][144]	Quantum computing threats	Quantum computing poses a future risk to cryptographic techniques, including those used in IoMT, by potentially breaking traditional encryption algorithms. Quantum computers could efficiently solve problems that would otherwise take classical computers an impractical amount of time, threatening the security of IoMT data and communications.	✓	✓	×	×
Confidentiality (C), Integrity (I), Availability (A), Authentication (Au),							

7. MECHANISMS FOR SECURING CRYPTOGRAPHIC TECHNIQUES IN THE IOMT

Securing cryptographic techniques in the IoMT is crucial because healthcare data is sensitive, a wide range of devices is involved, and breaches can have severe consequences [18]. The following outlines the detailed mechanisms to ensure the security of cryptographic techniques within the IoMT.

7.1. Lightweight Cryptographic Algorithms

IoMT devices often have limited computational power, storage, and energy, necessitating lightweight cryptographic algorithms that provide robust security without overburdening the system [145]. A lightweight encryption scheme uses a Lattice-based proxy Homomorphic encryption method to encrypt and decrypt healthcare data quickly. This approach efficiently processes large amounts of data within a distributed network [146]. Examples include lightweight block ciphers, such as SIMON and SPECK, specifically designed for constrained devices, offering strong security with reduced resource requirements. Stream ciphers like Grain and Trivium serve scenarios that demand minimal hardware footprint and low power consumption. Additionally, ECC provides security levels equivalent to RSA but with significantly smaller key sizes, making it particularly well-suited for IoMT applications with limited memory and computational capacity [147].

7.2. Key Management Mechanisms

Effective key management is essential for ensuring secure cryptographic operations, particularly in IoMT systems, where it must address the safe distribution, generation, storage, and revocation of keys in a scalable manner [148]. Common approaches include symmetric key distribution, which involves securely sharing symmetric keys between devices using methods like Diffie-Hellman or key distribution centers. In IoMT systems, secure initial pairing of devices and periodic key refreshes are critical for maintaining security. Asymmetric key exchange, utilizing public-private key pairs, is another approach, with mechanisms such as RSA or ECC enabling secure key exchanges in devices that support public-key infrastructure. Additionally, lightweight key management schemes accommodate the resource constraints of many IoMT devices. Methods like ECC-based approaches, including Elliptic Curve Diffie-Hellman, provide efficient and secure solutions in such environments [149].

7.3. Authentication Mechanisms

Given the importance of user privacy and the resource limitations on the user side in IoMT, an enhanced lightweight anonymous authentication protocol can ensure the necessary security within the IoMT system [4][18]. It is essential to ensure that access to sensitive medical data in IoMT systems is restricted to authorized devices and users because it is a critical aspect of maintaining the security and integrity of these systems. Common authentication mechanisms include device authentication, where each device in the IoMT network is verified using digital certificates or cryptographic tokens, often employing lightweight schemes such as ECC-based certificates or the Elliptic Curve Digital Signature Algorithm. Mutual authentication is another crucial approach, enabling both the device and the server (or another device) to authenticate each other using cryptographic keys, effectively mitigating MitM. Additionally, biometric authentication combines users' unique biometric traits, such as fingerprints or retina scans, with cryptographic keys to provide robust multi-factor authentication for accessing IoMT systems [51][150].

7.4. Access Control Mechanisms

Access control mechanisms ensure data is accessible or modifiable only by authorized entities, safeguarding it from unauthorized access or alterations [151]. Cryptography significantly enhances access control by integrating with security policies [152]. One example is attribute-based encryption, which enables data encryption so only users with specific attributes, such as roles or privileges, can decrypt the data. This approach is efficient in IoMT systems for enforcing fine-grained access control policies [42]. Similarly, role-based access control systems assign roles to users, granting data access based on these roles. Cryptographic tokens or certificates often authenticate users' roles and facilitate secure access [153].

7.5. Data Integrity And Secure Hashing

Ensuring the integrity of medical data is crucial in the IoMT. Secure hashing techniques play a vital role in verifying that data remains unaltered. SHA-256 or lightweight alternatives, such as SHA-3, compute hash values for integrity checks [154]. Message Authentication Codes (MACs), such as HMACs, enhance data integrity and authenticity using a shared secret key [155]. Additionally, digital signatures offer proof of data's origin and integrity, with the Elliptic Curve Digital Signature Algorithm (ECDSA)--based signatures being particularly suitable for IoMT environments due to their lightweight nature [156].

7.6. Homomorphic Encryption

Homomorphic encryption allows computations on encrypted data without decrypting it first. This encryption technique ensures that data remains secure and private throughout the process, as the results of the computations are also encrypted. Only the party with the decryption key can decrypt the final output, maintaining confidentiality while enabling meaningful analysis and processing of sensitive data. This feature is especially advantageous in secure data processing within IoMT environments, where protecting sensitive health data while allowing valuable operations is critical [157]. Partially homomorphic encryption supports specific operations on encrypted data, such as addition or multiplication. Paillier encryption, for example, can be utilized in IoMT to perform simple aggregate calculations. In contrast, fully homomorphic encryption permits arbitrary computations on encrypted data. While computationally intensive, recent advancements make fully homomorphic encryption more viable for secure data processing in IoMT applications [158].

7.7. End-To-End Encryption

End-to-end encryption ensures that data transmitted from an IoMT device to its destination, such as a server or medical database, remains encrypted throughout communication [159]. The critical components of this encryption include using TLS/SSL protocols, which offer secure communication over IP-based networks, safeguarding the confidentiality and integrity of medical data in transit [160]. Additionally, virtual private networks and secure tunnels encrypt communication pathways, ensuring the secure transmission of sensitive medical data between IoMT devices and healthcare servers [161].

7.8. Privacy-Preserving Techniques

Ensuring privacy is crucial in the IoMT, where protecting patient data is paramount [162]. Privacy-preserving techniques such as differential privacy and zero-knowledge proofs safeguard this data. Differential privacy involves adding controlled noise to the data before analysis, ensuring that individual patient information remains protected while enabling meaningful aggregate data analysis. On the other hand, zero-knowledge proofs allow one party to demonstrate possession of specific information—such as a key or password—without revealing the information itself, thus strengthening privacy in IoMT authentication mechanisms [163].

7.9. Blockchain-Based Security For Iomt

Blockchain is an ideal security framework for IoMT due to its distributed nature and high consistency. It improves healthcare data security by preventing illegal access, as updates to the distributed ledger are irreversible. Recent cryptographic approaches leverage the blocks within the Blockchain to protect data, further strengthening security for IoMT systems [146]. Blockchain technology improves the IoMT's security by offering a decentralized, tamper-proof platform for managing device identities, ensuring data integrity, and enabling secure communication [164]. Blockchain records all transactions involving IoMT devices, such as data exchanges and interactions, which helps maintain data integrity and traceability by utilizing an immutable ledger. Smart contracts on the Blockchain can also automate enforcing access control policies and manage cryptographic key exchanges between IoMT devices and healthcare providers, further enhancing security [21][165][166].

7.10. Quantum-Resistant Cryptography

Traditional cryptographic algorithms like RSA and ECC could become vulnerable, leading to potential security risks for the IoMT. As a result, quantum-resistant cryptography has become a growing area of interest for securing IoMT systems in the future [167]. Researchers are exploring lattice-based cryptographic schemes like NTRU and Learning With Errors (LWE) for their resistance to quantum attacks. They are considered potential solutions for enhancing IoMT security [168]. Hash-based signature schemes, like Lamport signatures, offer quantum-resistant alternatives for digital signatures, making them suitable for authentication and communication in IoMT devices [169]. The NIST is actively working on standardizing quantum-resistant cryptographic algorithms to protect IoMT architectures from emerging quantum threats [54].

7.11. Intrusion Detection Systems With Cryptographic Techniques

In the context of intelligent healthcare systems, network-based intrusion detection systems (IDS) protect the system and its networks from malicious attacks. These systems actively monitor the entire network or individual devices within the IoMT framework. When the IDS detects any suspicious or harmful activity, it promptly alerts the system administrator, enabling swift action to mitigate potential threats [31][170]. Cryptographic methods like secure log analysis are integrated with IDS to enhance monitoring security, which involves cryptographically hashing and signing logs that contain sensitive information or access histories, ensuring their integrity and making them tamper-proof and verifiable. Machine learning techniques cryptographically secure data and identify unusual behavior within IoMT devices and networks. This approach helps detect anomalies by analyzing data patterns while maintaining security and integrity.

7.12. Secure Software And Firmware Updates

IoMT devices typically operate over long periods, requiring regular software and firmware updates to ensure long-term protection [171]. Secure update procedures ensure that devices can defend against emerging threats while remaining unaffected by attacks. Code signing is vital in this process, as a digital signature verifies the firmware's authenticity before installation. IoMT devices should check these signatures during updates to prevent attackers from inserting malicious code [172]. Over-the-air (OTA) updates facilitate the remote patching of IoMT devices, eliminating the need for physical transport. These updates are typically secured with encryption and authentication, ensuring only authorized updates are applied. However, attackers may initially attempt to downgrade devices to insecure firmware versions, where rollback prevention mechanisms come into play. These mechanisms ensure that IoMT devices only accept firmware updates with higher versions, helping to mitigate such attacks.

Securing cryptographic techniques in the IoMT demands a comprehensive approach that integrates lightweight cryptographic algorithms, efficient key management, robust authentication, encryption, and privacy-preserving methods. As the IoMT landscape continues to evolve, emerging advancements such as homomorphic encryption, quantum-resistant cryptography,

and Blockchain integration hold the potential to significantly improve the security and privacy of medical data within this vital sector [173].

8. FUTURE RESEARCH DIRECTIONS

Cryptographic techniques are crucial for securing communication, ensuring data integrity, and protecting sensitive information within the IoMT ecosystem. Future research should focus on the following.

- Developing lightweight cryptographic algorithms that require minimal computational resources while maintaining strong security. For example, developers can further optimize ECC and lightweight block ciphers for IoMT devices. A promising solution is hybrid models that combine symmetric and asymmetric cryptography, minimizing computational complexity without sacrificing security.
- Developing quantum-resistant cryptographic techniques: With the potential for quantum computers to break existing cryptographic systems, it is essential to explore post-quantum cryptographic algorithms, including lattice-based, hash-based, code-based, and multivariate polynomial cryptography. Post-quantum cryptography develops algorithms based on mathematical problems resistant to traditional and quantum computing [33]. Research should also focus on hybrid cryptosystems that combine classical and quantum-resistant algorithms, ensuring transitional security for IoMT applications as quantum threats emerge.
- Homomorphic encryption, which allows for computations on encrypted data, also holds promise for IoMT, but its computational efficiency remains challenging. Research should aim to optimize homomorphic encryption techniques by exploring partial or leveled encryption schemes that balance performance and security for real-time IoMT systems.
- Additionally, integrating Blockchain with cryptographic methods can enhance security by creating decentralized and trustless models for IoMT. Developing lightweight consensus mechanisms like Proof of Authority (PoA) or Delegated Proof of Stake (DPoS) could reduce the computational burden on IoMT devices while ensuring data integrity and trust.
- Efficient and secure multiparty computation protocols for IoMT applications are also a priority. These protocols would allow different parties to collaborate without exposing private medical data. Research should focus on lightweight, secure multiparty computation algorithms tailored for the limited resources of IoMT devices, ensuring scalability and efficiency in practical deployments.
- Developing lightweight and distributed key management systems will also be essential for securing key generation, storage, distribution, and revocation in IoMT environments. Approaches such as self-sovereign identity-based key management and identity-based encryption could streamline key distribution without introducing unnecessary complexity.
- Context-aware cryptographic solutions are another promising area of research. These solutions could dynamically adjust security levels based on environmental factors and risks, ensuring that IoMT devices maintain appropriate security without overburdening their resources. Integrating machine learning models into cryptographic frameworks may allow IoMT devices to predict and adapt security settings based on real-time data, such as device status or user behavior.
- Ensuring the authenticity and integrity of firmware updates is critical in the context of IoMT devices. Maintaining trust in their operations is paramount as these devices often handle sensitive health data and interact with other medical systems. Any unauthorized or tampered firmware updates could compromise device functionality or expose patients to potential security risks. Research should explore secure boot mechanisms and cryptographic signatures for verifying firmware updates before installation, safeguarding against tampering.
- Researchers must examine privacy-preserving techniques, such as differential privacy and secure enclaves, to protect sensitive medical data while enabling its analysis and sharing. By combining encryption with differential privacy, they can develop protocols that facilitate secure data sharing and analysis within IoMT systems.
- Finally, integrating fault-tolerant cryptographic mechanisms with machine learning techniques could enhance the IoMT's ability to predict and prevent emerging attacks.

The future of cryptography in the IoMT ecosystem lies in addressing these environments' unique constraints and challenges. Research into lightweight algorithms, post-quantum cryptography, adaptive security models, and the mitigation of emerging threats like quantum attacks and side-channel exploits will be crucial for developing robust, scalable cryptographic solutions for IoMT.

9. CONCLUSIONS

This comprehensive review delves into the cryptographic techniques that form the foundation for securing the IoMT. As a crucial subset of the broader IoT, IoMT presents unique security challenges due to the sensitivity of medical data, the interconnectedness of devices, and the direct impact on human health. Ensuring data confidentiality, integrity, and availability in IoMT environments is critical, and cryptographic solutions play a pivotal role in protecting against various security threats.

The review covers classical and contemporary cryptographic methods, such as symmetric encryption, asymmetric encryption, hash functions, digital signatures, and newer technologies like homomorphic encryption and quantum cryptography. Each technique provides distinct advantages in securing different aspects of IoMT systems, from data transmission to authentication and privacy preservation. While these cryptographic methods have effectively addressed many security concerns, cryptographic techniques in IoMT systems remain vulnerable to various sophisticated attacks, including MitM attacks, side-channel attacks, replay attacks, cryptanalysis, brute-force attacks, key management attacks, insider attacks, DoS attacks, phishing and social engineering attacks, chosen plaintext/chosen ciphertext attacks, malware injection attacks, ransomware and data corruption attacks, firmware tampering, and quantum computing threats. Medical devices limited computational power and energy resources further complicate the deployment of robust cryptographic systems. Additionally, the diversity of devices and the dynamic nature of medical environments introduce challenges in key management and secure data sharing between devices and stakeholders.

The review also examines mitigation mechanisms, highlighting that while many cryptographic techniques can guard against specific attacks, the ever-evolving nature of cyber threats in healthcare demands the continual refinement of these methods. Moreover, integrating IoMT into larger medical ecosystems necessitates scalable, interoperable, and adaptable solutions that maintain performance and user experience while ensuring security. The review stresses the importance of lightweight cryptographic solutions for resource-constrained IoMT devices. Such protocols are essential for balancing security and operational efficiency in medical settings.

In conclusion, this review offers essential insights into the present status of cryptographic methods used in the IoMT. It identifies the challenges and future research directions needed to secure this vital area of modern healthcare. The findings highlight the ongoing need for innovation in cryptography to protect the future of IoMT systems and support the safe and efficient delivery of healthcare services worldwide.

Conflicts of Interest

The authors declare no conflict of interest.

Funding

This research received no external funding.

Acknowledgment

The authors offer their heartfelt appreciation to the anonymous reviewers for their insightful suggestions and constructive comments. They also extend their gratitude to Muni University and Baghdad College of Economic Sciences University.

References

[1]. A. Iqbal, M. A. Jaffar, and R. Jahangir, “Enhancing Brain Tumour Multi-Classification using Efficient-Net B0-Based Intelligent Diagnosis for Internet of Medical Things (IOMT) applications,” *Information*, vol. 15, no. 8, pp. 1–15, 2024. https://doi.org/10.3390/info15080489

[2]. M. S. Arefin, M. M. Rahman, M. T. Hasan, and M. Mahmud, “A topical review on enabling technologies for the internet of medical things: sensors, devices, platforms, and applications,” *Micromachines*, vol. 15, no. 4, pp. 1–32, 2024. https://doi.org/10.3390/mi15040479

[3]. M. Fiore, A. Bianconi, G. Sicari, A. Conni, J. Lenzi, G. Tomaiuolo, F. Zito, D. Golinelli, and F. Sanmarchi, “The Use of Smart Rings in Health Monitoring—A Meta-Analysis,” *Applied Sciences*, vol. 14, no. 23, pp. 1–18, 2024. https://doi.org/10.3390/app142310778

[4]. A. Maarouf, R. Sakr and S. Elmougy, “An Offline Direct Authentication Scheme for the Internet of Medical Things based on Elliptic Curve Cryptography,” *IEEE Access*, vol. 12, pp. 134902–134925, 2024. https://doi.org/10.1109/access.2024.3458424

[5]. K. Wang, M. Song, G. Bian, B. Shao, and K. Huang, “A lightweight Identity-Based network coding scheme for internet of medical things,” *Electronics*, vol. 13, no. 7, pp. 1–23, 2024. https://doi.org/10.3390/electronics13071316

[6]. Z. Jamroz, I. Ullah, B. Hassan, N. U. Amin, M. A. Khan, P. Lorenz, and N. Innab, “An Optimal Authentication Scheme through Dual Signature for the Internet of Medical Things,” *Future Internet*, vol. 15, no. 8, pp. 1–14. https://doi.org/10.3390/fi15080258

[7]. C. Chunka, S. Banerjee and S. K. Gupta, “A secure communication using multifactor authentication and key agreement techniques in internet of medical things for COVID-19 patients,” *Concurrency and Computation Practice and Experience*, vol. 35, no. 7, pp. 1–22, 2023. https://doi.org/10.1002/cpe.7602

[8]. W. Villegas-Ch, J. García-Ortiz, and I. Urbina-Camacho, "Framework for a secure and sustainable internet of medical Things, requirements, design challenges, and future trends," *Applied Sciences*, vol. 13, no. 11, pp. 1–21, 2023. https://doi.org/10.3390/app13116634

[9]. T. Alsolami, B. Alsharif, and M. Ilyas, "Enhancing Cybersecurity in Healthcare: Evaluating ensemble learning models for intrusion detection in the Internet of Medical Things," *Sensors*, vol. 24, no. 18, pp. 1–23, 2024. https://doi.org/10.3390/s24185937

[10]. X. Zhou, S. Wang, K. Wen, B. Hu, X. Tan, and Q. Xie, "Security-Enhanced lightweight and Anonymity-Preserving user authentication scheme for IoT-Based healthcare," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 9599–9609, 2024. https://doi.org/10.1109/jiot.2023.3323614

[11]. I. A. Khatib, A. Shamayleh, and M. Ndiaye, "Healthcare and the Internet of Medical Things: applications, trends, key challenges, and proposed resolutions," *Informatics*, vol. 11, no. 3, pp. 1–24, 2024. https://doi.org/10.3390/informatics11030047

[12]. G. Balhareth, and M. Ilyas, "Optimized Intrusion Detection for IoMT Networks with Tree-Based Machine Learning and Filter-Based Feature Selection," *Sensors*, vol. 24, no. 17, pp. 1–19, 2024. https://doi.org/10.3390/s24175712

[13]. V. K. Prasad, P. Bhattacharya, D. Maru, S. Tanwar, A. Verma, A. Singh, A. K. Tiwari, R. Sharma, A. Alkhayyat, F. Turcanu, and M. S. Raboaca, "Federated Learning for the Internet-of-Medical-Things: A survey," *Mathematics*, vol. 11, no. 1, pp. 1–47, 2022. https://doi.org/10.3390/math11010151

[14]. S. Conor, "*Internet of Medical Things (IOMT) - Statistics & Facts*," Statista. https://www.statista.com/aboutus/our-research-commitment/1799/conor-stewart (accessed November 22, 2024).

[15]. X. Su, and Y. Xu, "Secure and lightweight Cluster-Based User Authentication Protocol for IoMT deployment," *Sensors*, vol. 24, no. 22, pp. 1–21, 2024. https://doi.org/10.3390/s24227119

[16]. M. M. Islam, H. R. Rifat, M. S. B. Shahid, A. Akhter, and M. A. Uddin, "Utilizing deep feature Fusion for automatic leukemia classification: an Internet of Medical Things-Enabled deep learning framework," *Sensors*, vol. 24, no. 13, pp. 1–23, 2024. https://doi.org/10.3390/s24134420

[17]. A. O. Mulani, M. P. Sardey, K. Kinage, S. S. Salunkhe, T. Fegade, and P. G. Fegade, "ML-powered Internet of Medical Things (MLIOMT) structure for heart disease prediction," *Journal of Pharmacology and Pharmacotherapeutics*, pp. 1–8, 2024. https://doi.org/10.1177/0976500x241281490

[18]. S. Liu, H. Xu, and R. Zang, "An improved anonymous authentication scheme for internet of medical things based on elliptic curve cryptography," *2022 4th International Conference on Natural Language Processing (ICNLP)*, Guangzhou, China, 24-26 March 2023, pp. 345-349. https://doi.org/10.1109/icnlp58431.2023.00069

[19]. S. Abbas, G. A. Sampedro, M. Abisado, A. Almadhor, I. Yousaf, and S. Hong, "Harris-Hawk-Optimization-Based deep recurrent neural network for securing the internet of medical things," *Electronics*, vol. 12, no. 12, pp. 1–15, 2023. https://doi.org/10.3390/electronics12122612

[20]. M. S. Alkatheiri, and A. S. Alghamdi, "Blockcha," *Electronics*, vol. 12, no. 8, pp. 1–15, 2023. https://doi.org/10.3390/electronics12081801

[21]. A. Bisht, A. K. Das, D. Niyato, and Y. Park, "Efficient Personal-Health-Records sharing in internet of medical things using searchable symmetric encryption, blockchain, and IPFS," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 2225–2244, 2023. https://doi.org/10.1109/ojcoms.2023.3316922

[22]. B. Maram, R. Majji, G. K. D. Gopisetty, A. Garg, T. Daniya, and B. Santhosh Kumar, "Lightweight Cryptography based Deep Learning Techniques for Securing IoT Based E-Healthcare System," *2nd International Conference on Automation, Computing and Renewable Systems, ICACRS 2023 – Proceedings*, Pudukkottai, India, 11-13 December 2023, pp. 1334-1341. https://doi.org/10.1109/ICACRS58579.2023.10404726

[23]. N. Garg, R. Petwal, M. Wazid, D. P. Singh, A. K. Das, and J. J. P. C. Rodrigues, "On the design of an AI-driven secure communication scheme for internet of medical things environment," *Digital Communications and Networks*, vol. 9, no. 5, pp. 1080-1089, 2023. https://doi.org/10.1016/j.dcan.2022.04.009

[24]. I. Rodríguez-Rodríguez, J. Rodríguez, and M. Campo-Valera, "Applications of the internet of medical things to type 1 diabetes mellitus," *Electronics*, vol. 12, no. 3, pp. 1–23, 2023. https://doi.org/10.3390/electronics12030756

[25]. O. C. Abikoye, E. T. Oladipupo, A. L. Imoize, J. B. Awotunde, C. Lee, and C. Li, "Securing Critical User Information over the Internet of Medical Things Platforms Using a Hybrid Cryptography Scheme," *Future Internet*, vol. 15, no. 3, pp. 1–33, 2023. https://doi.org/10.3390/fi15030099

[26]. C. M. Chen, S. Liu, X. Li, S. H. Islam, and A. K. Das, "A provably-secure authenticated key agreement protocol for remote patient monitoring IoMT," *Journal of Systems Architecture*, vol. 136, no. 12, pp. 102831, 2023. https://doi.org/10.1016/j.sysarc.2023.102831

[27]. A. K. Idrees, S. K. Idrees, T. Ali-Yahiya, and R. Couturier, "Multibiosensor Data Sampling and Transmission Reduction with Decision-Making for Remote Patient Monitoring in IoMT Networks," *IEEE Sensors Journal*, vol. 23, no. 13, pp. 15140–15152, 2023. https://doi.org/10.1109/JSEN.2023.3278497

[28]. N. Shankar, M. K. Nallakaruppan, V. Ravindranath, M. Senthilkumar, and B. P. Bhagavath, "Smart IoMT Framework for Supporting UAV Systems with AI," *Electronics*, vol. 12, no. 1, pp. 1-19, 2023. https://doi.org/10.3390/electronics12010086

[29]. M. M. Mijwil, I. Bala, G. Ali, M. Aljanabi, M. Abotaleb, R. Doshi, . . . E.-S. M. El-Kenawy, "Sensing of Type 2 Diabetes Patients Based on Internet of Things Solutions: An Extensive Survey," In K. K. Hiran, R. Doshi, and M. Patel (Eds.), Modern Technology in Healthcare and Medical Education: Blockchain, IoT, AR, and VR (pp. 34-46). *IGI Global*, 2024. doi:10.4018/979-8-3693-5493-3.ch003

[30]. C. K. M. Lo, S. F. Tan, and G. C. Chung, "Enhanced Authentication Protocol for Securing Internet of Medical Things with Lightweight Post-Quantum Cryptography," *2022 IEEE International Conference on Artificial Intelligence in*

Engineering and Technology (IICAIET), Kota Kinabalu, Malaysia, 26-28 August 2024, pp. 625-630. https://doi.org/10.1109/iicaiet62352.2024.10730752

[31]. H. Naeem, A. Alsirhani, F. M. Alserhani, F. Ullah, and O. Krejcar, "Augmenting Internet of Medical Things Security: deep ensemble integration and methodological fusion," *Computer Modeling in Engineering & Sciences*, vol. 141, no. 3, pp. 2185–2223, 2024. https://doi.org/10.32604/cmes.2024.056308

[32]. A. Daoui, H. Mao, M. Yamni, Q. Li, O. Alfarraj, and A. a. A. El-Latif, "Novel Integer Shmaliy Transform and new multiparametric piecewise Linear Chaotic Map for joint lossless compression and encryption of medical images in IOMTs," *Mathematics*, vol. 11, no. 16, pp. 1–28, 2023. https://doi.org/10.3390/math11163619

[33]. F. Sabrina, S. Sohail, and U. U. Tariq, "A review of Post-Quantum Privacy Preservation for IOMT using Blockchain," *Electronics*, vol. 13, no. 15, pp. 1–18, 2024. https://doi.org/10.3390/electronics13152962

[34]. S. F. Ahmed, M. S. B. Alam, S. Afrin, S. J. Rafa, N. Rafa, and A. H. Gandomi, "Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions," *Information Fusion*, vol. 102, pp. 1–20, 2024. https://doi.org/10.1016/j.inffus.2023.102060

[35]. A. Kaushik, L. S. S. Vadlamani, M. M. Hussain, M. Sahay, R. Singh, A. K. Singh, S. Indu, P. Goswami, and N. G. V. Kousik, "Post Quantum Public and Private Key Cryptography Optimized for IoT Security," *Wireless Personal Communications*, vol. 129, no. 2, pp. 893–909, 2023. https://doi.org/10.1007/s11277-022-10162-w

[36]. M. S. Farooq, S. Riaz, R. Tehseen, U. Farooq, and K. Saleem, "Role of Internet of things in diabetes healthcare: Network infrastructure, taxonomy, challenges, and security model," *Digital Health*, vol. 9, pp. 1-19, 2023. https://doi.org/10.1177/20552076231179056

[37]. M. U. Rehman, A. Shafique, and A. B. Usman, "Securing Medical Information Transmission Between IoT Devices: An Innovative Hybrid Encryption Scheme Based on Quantum Walk, DNA Encoding, and Chaos," *Internet of Things*, vol. 24, pp. 1-19, 2023. https://doi.org/10.1016/j.iot.2023.100891

[38]. H. A. Selmy, H. K. Mohamed, and W. Medhat, "Big data analytics deep learning techniques and applications: A survey," *Information Systems*, vol. 120, pp. 102318, 2024. https://doi.org/10.1016/j.is.2023.102318

[39]. F. J. Jaime, A. Muñoz, F. Rodríguez-Gómez, and A. Jerez-Calero, "Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare," *Sensors*, vol. 23, no. 21, pp. 1-17, 2023. https://doi.org/10.3390/s23218944

[40]. R. Ettiyan, and V. Geetha, "A hybrid logistic DNA-based encryption system for securing the Internet of Things patient monitoring systems," *Healthcare Analytics*, vol. 3, pp. 1-8, 2023. https://doi.org/10.1016/j.health.2023.100149

[41]. I. L. B. M. Paris, M. H. Habaebi, and A. M. Zyoud, "Implementation of SSL/TLS Security with MQTT Protocol in IoT Environment," *Wireless Personal Communications*, vol. 132, no. 1, pp. 163–182, 2023. https://doi.org/10.1007/s11277-023-10605-y

[42]. D. S. Gupta, N. Mazumdar, A. Nag, and J. P. Singh, "Secure data authentication and access control protocol for industrial healthcare system," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 5, pp. 4853–4864, 2023. https://doi.org/10.1007/s12652-022-04370-2

[43]. M. Jammula, V. M. Vakamulla, and S. K. Kondoju, "Secure and scalable internet of medical things using ensemble lightweight cryptographic model," *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, 124, Coimbatore, India, 14-16 June 2023, pp. 982–987. https://doi.org/10.1109/icscss57650.2023.10169857

[44]. R. Akkaoui, "Blockchain for the Management of Internet of Things Devices in the Medical Industry," *IEEE* Transactions *on Engineering Management*, vol. 70, no. 8, pp. 2707 – 2718, 2023. https://doi.org/10.1109/TEM.2021.3097117

[45]. A. A. J. Al-Abadi, M. B. Mohamed, and A. Fakhfakh, "Enhanced Random Forest Classifier with K-Means Clustering (ERF-KMC) for Detecting and Preventing Distributed-Denial-of-Service and Man-in-the-Middle Attacks in Internet-of-Medical-Things Networks," *Computers*, vol. 12, no. 12, pp. 1-16, 2023. https://doi.org/10.3390/computers12120262

[46]. A. Arafa, H. A. Sheerah, and S. Alsalamah, "Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity: A Narrative Review," *Information*, vol. 14, no. 12, pp. 1-15, 2023. https://doi.org/10.3390/info14120640

[47]. M. F. Khan, and M. Abaoud, "Blockchain-Integrated Security for Real-Time Patient Monitoring in the Internet of Medical Things Using Federated Learning," *IEEE Access*, vol. 11, pp. 117826–117850, 2023. https://doi.org/10.1109/ACCESS.2023.3326155

[48]. M. Muzammil, Bin, M. Bilal, S. Ajmal, S. C. Shongwe, and Y. Y. Ghadi, "Unveiling Vulnerabilities of Web Attacks Considering Man in the Middle Attack and Session Hijacking," *IEEE Access*, vol. 12, pp. 6365-6375, 2024. https://doi.org/10.1109/ACCESS.2024.3350444

[49]. R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks," *Information*, vol. 14, no. 1, pp. 1-21, 2023. https://doi.org/10.3390/info14010041

[50]. I. A. Jayaraj, B. Shanmugam, S. Azam, and G. N. Samy, "A Systematic Review of Radio Frequency Threats in IoMT," *Journal of Sensor and Actuator Networks*, vol. 11, no. 4, pp. 1-19, 2022. https://doi.org/10.3390/jsan11040062

[51]. X. Chen, B. C. Wang, and H. Li, "A privacy-preserving multi-factor authentication scheme for cloud-assisted IoMT with post-quantum security," *Journal of Information Security and Applications*, vol. 81, pp. 103708, 2024. https://doi.org/10.1016/j.jisa.2024.103708

[52]. O. C. Abikoye, E. T. Oladipupo, A. L. Imoize, J. B. Awotunde, C. C. Lee, and C. T. Li, "Securing Critical User Information over the Internet of Medical Things Platforms Using a Hybrid Cryptography Scheme," *Future Internet*, vol. 15, no. 3, pp. 1-33, 2023. https://doi.org/10.3390/fi15030099

[53]. M. Adil, H. Alshahrani, A. Rajab, A. Shaikh, H. Song, and A. Farouk, "QoS Review: Smart Sensing in Wake of COVID-19, Current Trends and Specifications With Future Research Directions," *IEEE Sensors Journal*, vol. 23, no. 2, pp. 865-876, 2023. https://doi.org/10.1109/JSEN.2022.3170055

[54]. V. Srivastava, and S. K. Debnath, "A Multivariate-Based Provably Secure Certificateless Signature Scheme With Applications To The Internet Of Medical Things," *Computer Journal*, vol. 66, no. 10, pp. 2499–2516, 2023. https://doi.org/10.1093/comjnl/bxac100

[55]. G. R. Pradyumna, R. B. Hegde, K. B. Bommegowda, T. Jan, and G. R. Naik, "Empowering Healthcare with IoMT: Evolution, Machine Learning Integration, Security, and Interoperability Challenges," *IEEE Access*, vol. 12, pp. 20603–20623, 2024. https://doi.org/10.1109/access.2024.3362239

[56]. R. Wang, J. Lai, Z. Zhang, X. Li, P. Vijayakumar, and M. Karuppiah, "Privacy-Preserving Federated Learning for Internet of Medical Things Under Edge Computing," *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 2, pp. 854-865, 2023. https://doi.org/10.1109/JBHI.2022.3157725

[57]. A. Vallée, "Digital twin for healthcare systems," *Frontiers in Digital Health*, vol. 5, pp. 1-6, 2023. https://doi.org/10.3389/fdgth.2023.1253050

[58]. S. Razdan, and S. Sharma, "Internet of Medical Things (IOMT): overview, emerging technologies, and case studies," *IETE Technical Review*, vol. 39, no. 4, pp. 775–788, 2022. https://doi.org/10.1080/02564602.2021.1927863

[59]. A. E. Khaled, "Internet of Medical Things (IOMT): Overview, taxonomies, and classifications. *Journal of Computer and Communications*, vol. 10, no. 08, pp. 64–89, 2022. https://doi.org/10.4236/jcc.2022.108005

[60]. Z. Ashfaq, A. Rafay, R. Mumtaz, S. M. H. Zaidi, H. Saleem, S. a. R. Zaidi, S. Mumtaz, and A. Haque, "A review of enabling technologies for Internet of Medical Things (IoMT) Ecosystem," *Ain Shams Engineering Journal*, vol. 13, no. 4, pp. 1–19, 2022. https://doi.org/10.1016/j.asej.2021.101660

[61]. C. Huang, J. Wang, S. Wang, and Y. Zhang, "Internet of medical things: A systematic review," *Neurocomputing*, vol. 557, pp. 1–18, 2023. https://doi.org/10.1016/j.neucom.2023.126719

[62]. S. Maqbool, I. S. Bajwa, S. Maqbool, S. Ramzan, and M. J. Chishty, "A Smart Sensing Technologies-Based Intelligent Healthcare System for Diabetes Patients," *Sensors*, vol. 23, no. 23, pp. 1–33, 2023. https://doi.org/10.3390/s23239558

[63]. L. He, M. Eastburn, J. Smirk, and H. Zhao, "Smart Chemical Sensor and Biosensor Networks for Healthcare 4.0," *Sensors*, vol. 23, no. 12, pp. 1–15, 2023. https://doi.org/10.3390/s23125754

[64]. P. Mishra, and G. Singh, "Internet of Medical Things Healthcare for Sustainable Smart Cities: Current Status and Future Prospects," *Applied Sciences*, vol. 13, no. 15, pp. 1–29, 2023. https://doi.org/10.3390/app13158869

[65]. H. Alasmary, "ScalableDigitalHealth (SDH): An IoT-Based Scalable Framework for Remote Patient Monitoring," *Sensors*, vol. 24, no. 4, pp. 1–14, 2024. https://doi.org/10.3390/s24041346

[66]. M. A. Salman, and M. A. Mahdi, "Multi-Strategy Fusion for Enhancing Localization in Wireless Sensor Networks (WSNs)," *Iraqi Journal for Computer Science and Mathematics*, vol. 5, no. 1, pp. 299–326, 2024. https://doi.org/10.52866/ijcsm.2024.05.01.021

[67]. G. Ali, M. M. Mijwil, B. A. Buruga, M. Abotaleb, and I. Adamopoulos, "A Survey on Artificial Intelligence in Cybersecurity for Smart Agriculture: State-of-the-Art, Cyber Threats, Artificial Intelligence Applications, and Ethical Concerns," *Mesopotamian Journal of Computer Science*, vol. 2024, pp. 71–121, 2024. https://doi.org/10.58496/MJCSC/2024/007

[68]. J. Shahid, R. Ahmad, A. K. Kiani, T. Ahmad, S. Saeed, and A. M. Almuhaideb, "Data Protection and Privacy of the Internet of Healthcare Things (IoHTs)," *Applied Sciences*, vol. 12, no. 4, pp. 1–22, 2022. https://doi.org/10.3390/app12041927

[69]. V. Aivaliotis, K. Tsantikidou, and N. Sklavos, "IoT-Based Multi-Sensor Healthcare Architectures and a Lightweight-Based Privacy Scheme," *Sensors*, vol. 22, no. 11, pp. 1–21, 2022. https://doi.org/10.3390/s22114269

[70]. A. D. Aguru, E. S. Babu, S. R. Nayak, A. Sethy, and A. Verma, "Integrated Industrial Reference Architecture for Smart Healthcare in Internet of Things: A Systematic Investigation," *Algorithms*, vol. 15, no. 9, pp. 1–38, 2022. https://doi.org/10.3390/a15090309

[71]. A. Hadjadj, and K. Halimi, "COVID-19 Patients' Health Monitoring System using Fuzzy Ontology and Internet of Things," *Iraqi Journal for Computer Science and Mathematics*, vol. 4, no. 1, pp. 191–203, 2023. https://doi.org/10.52866/ijcsm.2023.01.01.0016

[72]. I. E. Kamarudin, M. A. Ameedeen, M. F. A. Razak, and A. Zabidi, "Integrating Edge Computing and Software Defined Networking in Internet of Things: A Systematic Review," *Iraqi Journal for Computer Science and Mathematics*, vol. 4, no. 4, pp. 121–150, 2023. https://doi.org/10.52866/ijcsm.2023.04.04.011

[73]. K. Alatoun, K. Matrouk, M. A. Mohammed, J. Nedoma, R. Martínek, and P. Zmij, "A Novel Low-Latency and Energy-Efficient Task Scheduling Framework for Internet of Medical Things in an Edge Fog Cloud System," *Sensors*, vol. 22, no. 14, pp. 1–36, 2022. https://doi.org/10.3390/s22145327

[74]. P. N. Srinivasu, A. K. Bhoi, S. R. Nayak, M. R. Bhutta, and M. Woźniak, "Blockchain Technology for Secured Healthcare Data Communication among the Non-Terminal Nodes in IoT Architecture in 5G Network," *Electronics*, vol. 10, no. 12, pp. 1–26, 2021. https://doi.org/10.3390/electronics10121437

[75]. M. Humayun, A. Alsirhani, F. Alserhani, M. Shaheen, and G. Alwakid, "Transformative synergy: SSEHCET—bridging mobile edge computing and AI for enhanced eHealth security and efficiency," *Journal of Cloud Computing*, vol. 13, no. 1, pp. 1–21, 2024. https://doi.org/10.1186/s13677-024-00602-2

[76]. A. Alabdulatif, I. Khalil, and M. S. Rahman, "Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis," *Applied Sciences*, vol. 12, no. 21, pp. 1–32, 2022. https://doi.org/10.3390/app122111039

[77]. S. Chaudhary, R. Kakkar, K.N. Jadav, A. Nair, R. Gupta, S. Tanwar, S. Agrawal, D.M. Alshehri, R. Sharma, G. Sharma, and E.I. Davidson, "A Taxonomy on Smart Healthcare Technologies: Security Framework, Case Study, and Future Directions," *Journal of Sensors*, vol. 2022, pp. 1-30, 2022. https://doi.org/10.1155/2022/1863838

[78]. R. Hireche, H. Mansouri, and A. K. Pathan, "Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 640–661, 2022. https://doi.org/10.3390/jcp2030033

[79]. G. Ali, and M. M. Mijwil, "Cybersecurity for Sustainable Smart Healthcare: State of the Art, Taxonomy, Mechanisms, and Essential Roles," *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 2, pp. 20–62, 2024. https://doi.org/10.58496/MJCS/2024/006

[80]. I. A. Khatib, A. Shamayleh, and M. Ndiaye, "Healthcare and the Internet of Medical Things: applications, trends, key challenges, and proposed resolutions," *Informatics*, vol. 11, no. 3, pp. 1–24, 2024. https://doi.org/10.3390/informatics11030047

[81]. N. A. Askar, A. Habbal, A. H. Mohammed, M. S. Sajat, Z. Y. Z. Yusupov, and D. Kodirov, "Architecture, Protocols, and Applications of the Internet of Medical Things (IOMT)," *Journal of Communications*, vol. 17, no. 11, pp. 900–918, 2022. https://doi.org/10.12720/jcm.17.11.900-918

[82]. N. Garg, M. Wazid, J. Singh, D. P. Singh, and A. K. Das, "Security in IoMT-driven smart healthcare: A comprehensive review and open challenges," *Security and Privacy*, vol. 5, no. 5, pp. 1–27, 2022. https://doi.org/10.1002/spy2.235

[83]. B. Cunha, and L. Gonçalves, "An IOMT architecture for patient rehabilitation based on Low-Cost hardware and interoperability standards," In Advances in medical technologies and clinical practice book series (pp. 37–59). *IGI Global*, 2022. https://doi.org/10.4018/978-1-6684-5260-8.ch003

[84]. B. Bhushan, A. Kumar, A. K. Agarwal, A. Kumar, P. Bhattacharya, and A. Kumar, "Towards a secure and Sustainable Internet of Medical Things (IOMT): requirements, design challenges, security techniques, and future trends," *Sustainability*, vol. 15, no. 7, pp. 1–25, 2023. https://doi.org/10.3390/su15076177

[85]. G. Ali, M. M. Mijwil, B. A. Buruga, and M. Abotaleb, "A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech," *Iraqi Journal For Computer Science and Mathematics*, vol. 5, no. 3, pp. 45–91, 2024. https://doi.org/10.52866/ijcsm.2024.05.03.004

[86]. W. Stallings, and L. Brown, Computer security: Principles and practice, 3rd ed., Pearson, 2014. pp. 1-848.

[87]. S. Chhabra, and K. Lata, "Obfuscated AES cryptosystem for secure medical imaging systems in IoMT edge devices," *Health and Technology*, vol. 12, no. 5, pp. 971–986, 2022. https://doi.org/10.1007/s12553-022-00686-3

[88]. R. Tikkha, and S. Sharma, "Cryptographic Measures in IOMT: Security Threats and Measurement," *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Kharagpur, India, 03-05 October 2022, pp. 1-8. https://doi.org/10.1109/icccnt54827.2022.9984359

[89]. Z. U. I. Adil, M. I. Khan, K. Sanam, S. U. R. Malik, S. A. Moqurrab, and G. Srivastava, "LightAuth: a lightweight sensor nodes authentication framework for smart health system," *Expert Systems*, pp. 1–15, 2024. https://doi.org/10.1111/exsy.13756

[90]. B. Mudassar, S. Tahir, F. Khan, S. A. Shah, S. I. Shah, and Q. H. Abbasi, "Privacy-Preserving data analytics in internet of medical things," *Future Internet*, vol. 16, no. 11, pp. 1–30, 2024. https://doi.org/10.3390/fi16110407

[91]. B. Halak, Y. Yilmaz, and D. Shiu, "Comparative Analysis of Energy Costs of Asymmetric vs Symmetric Encryption-Based Security Applications," *IEEE Access*, vol. 10, pp. 76707-76719, 2022. https://doi.org/10.1109/ACCESS.2022.3192970

[92]. G. Ali, M. A. Dida, and A. E. Sam, "A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications," *Future Internet*, vol. 13, no. 12, pp. 1-31, 2021. https://doi.org/https://doi.org/10.3390/fi13120299

[93]. W. Alexan, A. Ashraf, E. Mamdouh, S. Mohamed, and Moustafa, M. "IOMT Security: SHA3-512, AES-256, RSA and LSB Steganography," *2021 8th NAFOSTED Conference on Information and Computer Science (NICS)*, Hanoi, Vietnam, 21-22 December 2021, pp. 177-181. https://doi.org/10.1109/nics54270.2021.9701567

[94]. M. Azeem, A. Ullah, H. Ashraf, N. Jhanjhi, M. Humayun, S. Aljahdali, and T. A. Tabbakh, "FOG-Oriented secure and lightweight data aggregation in IOMT," *IEEE Access*, vol. 9, pp. 111072–111082, 2021. https://doi.org/10.1109/access.2021.3101668

[95]. A. A. Jolfaei, S. F. Aghili, and D. Singelee, "A survey on Blockchain-Based IOMT Systems: Towards Scalability," *IEEE Access*, vol. 9, pp. 148948–148975, 2021. https://doi.org/10.1109/access.2021.3117662

[96]. C. Rupa, S. K. A. Sultana, R. P. Malleswari, C. Dedeepya, T. R. Gadekallu, H. Song, and M. J. Piran, "IOMT Privacy Preservation: A Hash-Based DCIWT approach for detecting tampering in medical data," *IEEE Access*, vol. 12, pp. 97298–97308, 2024. https://doi.org/10.1109/access.2024.3420688

[97]. A. S. Alotaibi, "Biserial miyaguchi–preneel blockchain-based ruzicka-indexed deep perceptive learning for malware detection in IoMT," *Sensors*, vol. 21, no. 21, pp. 1-17, 2021. https://doi.org/10.3390/s21217119

[98]. S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of internet of things based on cryptographic algorithms: a survey," *Wireless Networks*, vol. 27, no. 2, pp. 1515–1555, 2021. https://doi.org/10.1007/s11276-020-02535-5

[99]. P. K. Sadhu, V. P. Yanambaka, A. Abdelgawad, and K. Yelamarthi, "Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions," *Sensors*, vol. 22, no. 15, pp. 1-31, 2022. https://doi.org/10.3390/s22155517

[100]. K. Chatterjee, R. R. K. Chaudhary, and A. Singh, "A lightweight block cipher technique for IoT based E-healthcare system security," *Multimedia Tools and Applications*, vol. 81, no. 30, pp. 43551–43580, 2022. https://doi.org/10.1007/s11042-022-13106-5

[101]. S. Jain, and R. Doriya, "Security framework to healthcare robots for secure sharing of healthcare data from cloud," *International Journal of Information Technology (Singapore)*, vol. 14, no. 5, pp. 2429–2439, 2022. https://doi.org/10.1007/s41870-022-00997-8

[102]. Z. Zulkifl, F. Khan, S. Tahir, M. Afzal, W. Iqbal, A. Rehman, S. Saeed, and A. M. Almuhaideb, "FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs," *IEEE Access*, vol. 10, pp. 15644-15656, 2022. https://doi.org/10.1109/ACCESS.2022.3149046

[103]. J. Shi, X. Zeng, and R. Han, "A Blockchain-Based Decentralized Public Key Infrastructure for Information-Centric Networks," *Information*, vol. 13, no. 5, pp. 1-15, 2022. https://doi.org/10.3390/info13050264

[104]. K. Gupta, K. D. Gupta, D. Kumar, G. Srivastava, and D. K. Sharma, "BIDS: Blockchain and Intrusion Detection System Coalition for Securing Internet of Medical Things Networks," *IEEE Journal of Biomedical and Health Informatics*, pp. 1-9, 2023. https://doi.org/10.1109/JBHI.2023.3325964

[105]. H. Szczepaniuk, and E. K. Szczepaniuk, "Cryptographic evidence-based cybersecurity for smart healthcare systems," *Information Sciences*, vol. 649, pp. 1-23, 2023. https://doi.org/10.1016/j.ins.2023.119633

[106]. F. A. Almalki, and B. O. Soufiene, "EPPDA: An Efficient and Privacy-Preserving Data Aggregation Scheme with Authentication and Authorization for IoT-Based Healthcare Applications," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1-18, 2021. https://doi.org/10.1155/2021/5594159

[107]. J. Ficek, W. Wang, H. Chen, G. Dagne, and E. Daley, "Differential privacy in health research: A scoping review," *Journal of the American Medical Informatics Association* vol. 28, no. 10, pp. 2269–2276, 2021. https://doi.org/10.1093/jamia/ocab135

[108]. H. D. Zubaydi, P. Varga, and S. Molnár, "Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review," *Sensors*, vol. 23, no. 2, pp. 1-43, 2023. https://doi.org/10.3390/s23020788

[109]. V. Gugueoth, S. Safavat, S. Shetty, and D. Rawat, "A review of IoT security and privacy using decentralized blockchain techniques," *Computer Science Review*, vol. 50, pp. 1-16, 2023. https://doi.org/10.1016/j.cosrev.2023.100585

[110]. P. Kutas, and C. Petit, "Torsion point attacks on 'SIDH-like' cryptosystems. *IET Information Security*, vol. 17, no. 2, pp. 1-19, 2023. https://doi.org/10.1049/ise2.12076

[111]. Z. Yang, H. Alfauri, B. Farkiani, R. Jain, Pietro, R. Di, and A. Erbad, "A Survey and Comparison of Post-Quantum and Quantum Blockchains," *IEEE Communications Surveys and Tutorials*, vol. 26, no. 2, pp. 967-1002, 2024. https://doi.org/10.1109/COMST.2023.3325761

[112]. P. Scalise, M. Boeding, M. Hempel, H. Sharif, J. Delloiacovo, and Reed, J. "A Systematic Survey on 5G and 6G Security Considerations, Challenges, Trends, and Research Areas," *Future Internet*, vol. 16, no. 3, pp. 1-38, 2024. https://doi.org/10.3390/fi16030067

[113]. A. A. Alfa, J. K. Alhassan, O. M. Olaniyi, and M. Olalere, "Blockchain technology in IoT systems: current trends, methodology, problems, applications, and future directions," *Journal of Reliable Intelligent Environments*, vol. 7, no. 2, pp. 115–143, 2021. https://doi.org/10.1007/s40860-020-00116-z

[114]. K. Azbeg, O. Ouchetto, and S. Jai Andaloussi, "Access Control and Privacy-Preserving Blockchain-Based System for Diseases Management," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 4, pp. 1515-1527, 2023. https://doi.org/10.1109/TCSS.2022.3186945

[115]. H. B. Mahajan, A. S. Rashid, A. A. Junnarkar, N. Uke, S. D. Deshpande, P. R. Futane, A. Alkhayyat, and B. Alhayani, "Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems," *Applied Nanoscience*, vol. 13, no. 3, pp. 2329–2342, 2023. https://doi.org/10.1007/s13204-021-02164-0

[116]. A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang, "A smart-contract-based access control framework for cloud smart healthcare system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5914-5925, 2021. https://doi.org/10.1109/JIOT.2020.3032997

[117]. H. Kaur, R. Jameel, M. A. Alam, B. Alankar, and V. Chang, "Securing and managing healthcare data generated by intelligent blockchain systems on cloud networks through DNA cryptography," *Journal of Enterprise Information Management*, vol. 36, no. 4, pp. 861-878, 2023. https://doi.org/10.1108/JEIM-02-2021-0084

[118]. I. Ullah, M. A. Khan, A. M. Abdullah, F. Noor, N. Innab, and Chen, C. M. "Enabling Secure Communication in Wireless Body Area Networks with Heterogeneous Authentication Scheme," *Sensors*, vol. 23, no. 3, pp. 1-16, 2023. https://doi.org/10.3390/s23031121

[119]. M. K. Hasan, T. M. Ghazal, R. A. Saeed, B. Pandey, H. Gohel, A. A. Eshmawi, S. Abdel-Khalek, and H. M. Alkhassawneh, "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things," *IET Communications*, vol. 16, no. 5, pp. 421-432, 2022. https://doi.org/10.1049/cmu2.12301

[120]. H. B. Mahajan, and A. A. Junnarkar, "Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing," *Multimedia Tools and Applications*, vol. 82, no. 28, pp. 44335–44358, 2023. https://doi.org/10.1007/s11042-023-15204-4

[121]. I. Riadi, R. Umar, I. Busthomi, and A. W. Muhammad, "Block-hash of blockchain framework against man-in-the-middle attacks," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 8, no. 1, pp. 1-9, 2022. https://doi.org/10.26594/register.v8i1.2190

[122]. J. Jose, and D. V. Jose, "The Internet of Things Architectures and Use Cases," In *Enterprise Digital Transformation*, *Taylor & Francis*, 2022. https://doi.org/10.1201/9781003119784-4

[123]. N. I. Haque, and M. A. Rahman, "PHASE: Security Analyzer for Next-Generation Smart Personalized Smart Healthcare System," *Proceedings - 2022 IEEE International Conference on Digital Health, ICDH 2022*, Barcelona, Spain, 10-16 July 2022, pp.208-214. https://doi.org/10.1109/ICDH55609.2022.00040

[124]. M. A. Hafeez, M. M. Hazzazi, H. Tariq, A. Aljaedi, A. Javed, and A. R. Alharbi, "A low-overhead countermeasure against differential power analysis for AES block cipher," *Applied Sciences,* vol. 1, no. 21, pp. 1-16, 2021. https://doi.org/10.3390/app112110314

[125]. M. Wazid, and P. Gope, "BACKM-EHA: A Novel Blockchain-enabled Security Solution for IoMT-based E-healthcare Applications," *ACM Transactions on Internet Technology,* vol. 23, no. 3, pp. 1 – 28, 2023. https://doi.org/10.1145/3511898

[126]. I. A. Jayaraj, B. Shanmugam, S. Azam, and S. Thennadil, "Detecting and localizing wireless spoofing attacks on the internet of medical things," *Journal of Sensor and Actuator Networks,* vol. 13, no. 6, pp. 1–21, 2024. https://doi.org/10.3390/jsan13060072

[127]. M. Masud, G. S. Gaba, S. Alqahtani, G. Muhammad, B. B. Gupta, P. Kumar, and A. Ghoneim, "A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care," *IEEE Internet of Things Journal,* vol. 8, no. 21, pp. 15694 – 15703, 2021. https://doi.org/10.1109/JIOT.2020.3047662

[128]. B. Aboushosha, R. A. Ramadan, A. D. Dwivedi, A. El-Sayed, and M. M. Dessouky, "SLIM: A lightweight block cipher for internet of health things," *IEEE Access,* vol. 8, pp. 203747 – 203757, 2020. https://doi.org/10.1109/ACCESS.2020.3036589

[129]. N. F. Ibrahim, and J. I. Agbinya, "A Review of Lightweight Cryptographic Schemes and Fundamental Cryptographic Characteristics of Boolean Functions," *Advances in Internet of Things*, vol. 12, no. 01, pp. 9-17, 2022. https://doi.org/10.4236/ait.2022.121002

[130]. A. I. Sanka, M. Irfan, I. Huang, and R. C. C. Cheung, "A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research," *Computer Communications*, vol. 169, pp. 179-201, 2021. https://doi.org/10.1016/j.comcom.2020.12.028

[131]. A. F. Otoom, W. Eleisah, and E. E. Abdallah, "Deep Learning for Accurate Detection of Brute Force attacks on IoT Networks," *Procedia Computer Science*, vol. 220, pp. 291-298, 2023. https://doi.org/10.1016/j.procs.2023.03.038

[132]. W. Rafique, M. Khan, S. Khan, and J. S. Ally, "SecureMed: A Blockchain-Based Privacy-Preserving Framework for Internet of Medical Things," *Wireless Communications and Mobile Computing*, vol. 2023, pp. 1-14, 2023. https://doi.org/10.1155/2023/2558469

[133]. A. Berguiga, and A. Harchay, "An iot-based intrusion detection system approach for tcp syn attacks," *Computers, Materials and Continua,* vol. 71, no. 2, pp. 3839-3851, 2022. https://doi.org/10.32604/cmc.2022.023399

[134]. S. A. Wagan, J. Koo, I. F. Siddiqui, N. M. F. Qureshi, M. Attique, and D. R. Shin, "A Fuzzy-Based Duo-Secure Multi-Modal Framework for IoMT Anomaly Detection," *Journal of King Saud University - Computer and Information Sciences,* vol. 35, no. 1, pp. 131-144, 2023. https://doi.org/10.1016/j.jksuci.2022.11.007

[135]. N. Munir, M. Khan, A. Al Karim Haj Ismail, and I. Hussain, "Cryptanalysis and Improvement of Novel Image Encryption Technique Using Hybrid Method of Discrete Dynamical Chaotic Maps and Brownian Motion," *Multimedia Tools and Applications,* vol. 81, no. 5, pp. 6571–6584, 2022. https://doi.org/10.1007/s11042-021-11810-2

[136]. S. Ibrahim, and A. Alharbi, "Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography," *IEEE Access*, vol. 8, pp. 194289 – 194302, 2020. https://doi.org/10.1109/ACCESS.2020.3032403

[137]. M. Kihara, and S. Iriyama, "Security Verification of an Authentication Algorithm Based on Verifiable Encryption," *Information*, vol. 4, no. 2, pp. 1-13, 2023. https://doi.org/10.3390/info14020126

[138]. N. Sehatbakhsh, A. Nazari, M. Alam, F. Werner, Y. Zhu, A. Zajic, and M. Prvulovic, "REMOTE: Robust External Malware Detection Framework by Using Electromagnetic Signals," *IEEE Transactions on Computers*, vol. 69, no. 3, pp. 312-326, 2020. https://doi.org/10.1109/TC.2019.2945767

[139]. B. V. S. Rao, V. Sharma, N. Rathore, D. Prasad, H. Anandaram, and G. Soni, "A Secure Framework to Prevent Three-Tier Cloud Architecture From Malicious Malware Injection Attacks," *International Journal of Cloud Applications and Computing,* vol. 13, no. 1, pp. 1-22, 2023. https://doi.org/10.4018/IJCAC.317220

[140]. Reshmi, T. R. "Information security breaches due to ransomware attacks - a systematic literature review," *International Journal of Information Management Data Insights*, vol. 1, no. 2, pp. 1-10, 2021. https://doi.org/10.1016/j.jjimei.2021.100013

[141]. M. J. Iqbal, S. Aurangzeb, M. Aleem, G. Srivastava, and J. C. W. Lin, "RThreatDroid: A Ransomware Detection Approach to Secure IoT Based Healthcare Systems," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 2574-2583, 2023. https://doi.org/10.1109/TNSE.2022.3188597

[142]. Y. Zhang, Y. Li, and Z. Li, "Aye: A Trusted Forensic Method for Firmware Tampering Attacks," *Symmetry,* vol. 15, no. 1, pp. 1-19, 2023. https://doi.org/10.3390/sym15010145

[143]. I. Pedone, and A. Lioy, "Quantum Key Distribution in Kubernetes Clusters," *Future Internet,* vol. 14, no. 6, pp. 1-19, 2022. https://doi.org/10.3390/fi14060160

[144]. S. E. Yunakovsky, M. Kot, N. Pozhar, D. Nabokov, M. Kudinov, A. Guglya, E. O. Kiktenko, E. Kolycheva, A. Borisov, and A. K. Fedorov, "Towards security recommendations for public-key infrastructures for production environments in the post-quantum era," *EPJ Quantum Technology,* vol. 8, no. 1, pp. 1-19, 2021. https://doi.org/10.1140/epjqt/s40507-021-00104-z

[145]. C. Dhasarathan, M. K. Hasan, S. Islam, S. Abdullah, S. Khapre, D. Singh, A. A. Alsulami, and A. Alqahtani, "User privacy prevention model using supervised federated learning-based block chain approach for internet of Medical Things," *CAAI Transactions on Intelligence Technology*, pp. 1-15, 2023. https://doi.org/10.1049/cit2.12218

[146]. A. G. Chandini, and P. Basarkod, "A Robust Blockchain Architecture for Electronic Health Data using Efficient Lightweight Encryption Model with Re-Encryption Scheme," *2022 IEEE International Conference on Data Science and Information System (ICDSIS)*, Hassan, India, 29-30 July 2022, pp. 1-6. https://doi.org/10.1109/icdsis55133.2022.9915902

[147]. M. Adil, M. K. Khan, M. M. Jadoon, M. Attique, H. Song, and A. Farouk, "An AI-Enabled Hybrid Lightweight Authentication Scheme for Intelligent IoMT Based Cyber-Physical Systems," *IEEE Transactions on Network Science and Engineering,* vol. 10, no. 5, pp. 2719-2730, 2023. https://doi.org/10.1109/TNSE.2022.3159526

[148]. H. Alhakami, A. Baz, M. Al-Shareef, R. Kumar, A. Agrawal, and R. A. Khan, "A Framework for Securing Saudi Arabian Hospital Industry: Vision-2030 Perspective," *Intelligent Automation and Soft Computing,* vol. 36, no. 3, pp. 2773-2786, 2023. https://doi.org/10.32604/iasc.2023.021560

[149]. V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare," *SN Computer Science,* vol. 3, no. 5, pp. 1-19, 2022. https://doi.org/10.1007/s42979-022-01238-2

[150]. N. Alsaeed, and F. Nadeem, "Authentication in the Internet of Medical Things: Taxonomy, Review, and Open Issues," *Applied Sciences,* vol. 12, no. 15, pp. 1-30, 2022. https://doi.org/10.3390/app12157487

[151]. S. F. Aghili, M. Sedaghat, D. Singelée, and M. Gupta, "MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme," *Future Generation Computer Systems*, vol. 131, pp. 75-90, 2022. https://doi.org/10.1016/j.future.2022.01.003

[152]. Z. A. Shaikh, F. Hajjej, Y. D. Uslu, S. Yuksel, H. Dincer, R. Alroobaea, A. M. Baqasah, and U. Chinta, "A New Trend in Cryptographic Information Security for Industry 5.0: A Systematic Review," *IEEE Access,* vol. 12, pp. 7156-7169, 2024. https://doi.org/10.1109/ACCESS.2024.3351485

[153]. T. Jayasankar, R. M. Bhavadharini, N. R. Nagarajan, G. Mani, and S. Ramesh, "Securing Medical Data using Extended Role Based Access Control Model and Twofish Algorithms on Cloud Platform," *European Journal of Molecular & Clinical Medicine,* vol. 8, no. 01, pp. 1075, 2021.

[154]. S. Gadamsetty, R. Ch, A. Ch, C. Iwendi, and T. R. Gadekallu, "Hash-Based Deep Learning Approach for Remote Sensing Satellite Imagery Detection," *Water,* vol. 14, no. 5, pp. 1-15, 2022. https://doi.org/10.3390/w14050707

[155]. S. Dalimunthe, J. Reza, and A. Marzuki, "The Model for Storing Tokens in Local Storage (Cookies) using JSON Web Token (JWT) with HMAC (Hash-Based Message Authentication Code) in E-Learning Systems," *Journal of Applied Engineering and Technological Science,* vol. 3, no. 2, pp. 149-155, 2022. https://doi.org/10.37385/jaets.v3i2.662

[156]. A. Mehbodniya, J. L. Webber, R. Neware, F. Arslan, R. V. Pamba, and M. Shabaz, "Modified Lamport Merkle Digital Signature blockchain framework for authentication of internet of things healthcare data," *Expert Systems,* vol. 39, no. 10, pp. 1-10, 2022. https://doi.org/10.1111/exsy.12978

[157]. J. M. Cortes-Mendoza, G. Radchenko, A. Tchernykh, B. Pulido-Gaytan, M. Babenko, A. Avetisyan, P. Bouvry, and A. Zomaya, "LR-GD-RNS: Enhanced privacy-preserving logistic regression algorithms for secure deployment in untrusted environments," *Proceedings - 21st IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing, CCGrid 2021,* Melbourne, Australia, 10-13 May 2021, pp. 770-775. https://doi.org/10.1109/CCGrid51090.2021.00093

[158]. M. U. Shaikh, S. A. Ahmad, and W. A. W. Adnan, "Secured electrocardiograph (ECG) signal using fully homomorphic encryption technique," *Test Engineering and Management,* vol. 82, pp. 12029-12034, 2020.

[159]. T. Isobe, and R. Ito, "Security Analysis of End-to-End Encryption for Zoom Meetings," *IEEE Access,* vol. 9, pp. 90677-90677, 2021. https://doi.org/10.1109/ACCESS.2021.3091722

[160]. P. Hartel, and R. van Wegberg, "Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases," *Crime Science,* vol. 12, no. 1, pp. 1-18, 2023. https://doi.org/10.1186/s40163-023-00185-4

[161]. P. Li, J. Su, and X. Wang, "ITLS: Lightweight Transport-Layer Security Protocol for IoT with Minimal Latency and Perfect Forward Secrecy," *IEEE Internet of Things Journal,* vol. 7, no. 8, pp. 6828-6841, 2020. https://doi.org/10.1109/JIOT.2020.2988126

[162]. B. Soewito, and Y. Marcellinus, "IoT security system with modified Zero Knowledge Proof algorithm for authentication," *Egyptian Informatics Journal,* vol. 22, no. 3, pp. 269-276, 2021. https://doi.org/10.1016/j.eij.2020.10.001

[163]. J. A. Chaudhry, K. Saleem, M. Alazab, H. M. A. Zeeshan, J. Al-Muhtadi, and J. J. P. C. Rodrigues, "Data Security through Zero-Knowledge Proof and Statistical Fingerprinting in Vehicle-to-Healthcare Everything (V2HX) Communications," *IEEE Transactions on Intelligent Transportation Systems,* vol. 22, no. 6, pp. 3869-3879, 2021. https://doi.org/10.1109/TITS.2021.3066487

[164]. K. S. Kumar, J. A. Alzubi, N. Sarhan, E. M. Awwad, V. Kandasamy, and G. Ali, "A secure and efficient BlockChain and distributed Ledger technology-based optimal resource management in digital twin beyond 5G networks using hybrid energy valley and levy Flight Distributer Optimization algorithm," *IEEE Access*, vol. 12, pp. 110331–110352, 2024. https://doi.org/10.1109/access.2024.3435847

[165]. M. Warkentin, and C. Orgeron, "Using the security triad to assess blockchain technology in public sector applications," *International Journal of Information Management,* vol. 52, pp. 102090, 2020. https://doi.org/10.1016/j.ijinfomgt.2020.102090

[166]. M. Q. Alsudani, M. M. Jaber, R. Q. Malik, S. K. Abd, M. H. Ali, A., Alkhayyat, and G. A. Khalaf, "Blockchain-Based E-Medical Record and Data Security Service Management Based on IoMT Resource," *International Journal of Pattern Recognition and Artificial Intelligence,* vol. 37, no. 6, pp. 2357001, 2023. https://doi.org/10.1142/S021800142357001X

[167]. M. Kumar, "Post-quantum cryptography Algorithm's standardization and performance analysis," *Array,* vol. 15, pp. 1-27, 2022. https://doi.org/10.1016/j.array.2022.100242

[168]. J. Wang, and L. Liu, "RLWE-based Privacy-Preserving Data Sharing Scheme for Internet of Medical Things System," *Proceedings - 2022 3rd International Conference on Electronics, Communications and Information Technology, CECIT 2022,* Sanya, China, 23-25 December 2022, pp. 441-445. https://doi.org/10.1109/CECIT58139.2022.00082

[169]. W. Wang, X. Li, X. Qiu, X. Zhang, J. Zhao, and V. Brusic, "A privacy preserving framework for federated learning in smart healthcare systems," *Information Processing and Management*, vol. 60, no. 1, pp. 103167, 2023. https://doi.org/10.1016/j.ipm.2022.103167

[170]. I. Al-Turaiki, and N. Altwaijry, "A Convolutional Neural Network for Improved Anomaly-Based Network Intrusion Detection," *Big Data*, vol. 9, no. 3, pp. 233–252, 2021. https://doi.org/10.1089/big.2020.0263

[171]. S. Choi, and J. H. Lee, "Blockchain-Based Distributed Firmware Update Architecture for IoT Devices," *IEEE Access*, vol. 8, pp. 37518-37525, 2020. https://doi.org/10.1109/ACCESS.2020.2975920

[172]. L. *Verderame*, A. Ruggia, and A. Merlo, "PARIOT: Anti-repackaging for IoT firmware integrity," *Journal of Network and Computer Applications,* vol. 217, pp. 1-26, 2023. https://doi.org/10.1016/j.jnca.2023.103699

[173]. A. K. Srinivas, D. Vikram, S. Sharma, and R. Kumar Lenka, "Deployment Automation for Blockchain Enabled IoMT," *Proceedings - 2022 OITS International Conference on Information Technology, OCIT 2022*, Bhubaneswar, India, 14-16 December 2022, pp. 599-602. https://doi.org/10.1109/OCIT56763.2022.00116