International Journal of Safety and Security Engineering
Vol. 15, No. 11, November, 2025, pp. 2403-2417
Journal homepage: http://iieta.org/journals/ijsse

A Comprehensive Survey on Lightweight Cryptography Algorithms to Enhance Quality of Service in Medical Internet of Things

Tanukonda Padmaja*, Misha Chandar

School of Computer Science and Engineering, VIT-AP University, Amaravati 522237, India

Corresponding Author Email: padmaja.23phd7126@vitap.ac.in

https://doi.org/10.18280/ijsse.151120

Received: 3 September 2025
Revised: 4 November 2025
Accepted: 20 November 2025
Available online: 30 November 2025

Keywords:
Internet of Medical Things, healthcare industry, security, lightweight cryptography, Quality of Service

ABSTRACT

Internet of Things (IoT) refers to the network of interconnected electronic devices and software that gather, transmit, and analyze data. Included in the healthcare category are fitness trackers and other wearable tech, as well as high-tech medical equipment used in hospitals to record patients' vital signs. The Internet of Medical Things (IoMT) enables these devices to communicate and share data, which improves the ability of healthcare providers, nurses, and family members to deliver efficient and timely care. Natural disaster prediction, information management, agriculture, healthcare monitoring, and many more disciplines could potentially benefit from it. No IoT application should ever compromise on security. Security measures to protect sensitive patient data are becoming more important as IoMT devices become more widely used. All the way from high-tech medical imaging systems to portable fitness trackers, these gadgets are constantly gathering and sending patient data in real-time. The security and privacy of sensitive medical data are becoming more important as the IoMT is being used more and more in healthcare. As the IoMT was being developed, the security of user data was given top priority. Lightweight cryptography (LWC) is one approach that might be used to enhance the security and privacy of the IoMT. Execution time, memory consumption, latency, throughput, and security resilience are some of the parameters taken into account when evaluating algorithms on IoT boards with limited processor power and capabilities. Following these steps will help users evaluate cryptographic algorithms for their suitability and make well-informed selections as they search for the best ones that strike a balance between performance and security. This research benefits academics and researchers by providing a deeper understanding of existing security models and facilitating the development of improved approaches for protecting medical IoT data.

1. INTRODUCTION

Internet of Healthcare Things (IoHT) or Internet of Medical Things (IoMT) is anticipated to bring about substantial advancements in healthcare efficiency and care quality as a result of its varied and exciting advances [1]. Recent developments in microelectronics, materials, and biosensor designs have piqued interest in a variety of smart medical devices, but notably implantable and wearable ones. The privacy and security of these healthcare systems that rely on IoMT have, however, been neglected due to the fast development of IoMT. Inadequate security in IoMT healthcare systems can lead to implications such as patients' privacy being compromised through eavesdropping and life-threatening incidents going undetected due to Denial of Service (DoS) attacks disrupting the usual functioning of IoMT devices [2]. In 2022, numerous researchers discovered that every one of the top ten smart watches sold at the time had security flaws due to things like inadequate authorization or authentication, unencrypted data transmission [3], insecure user interfaces, insecure software/firmware, and privacy problems [4]. As an example, authentication is the procedure that verifies the user's identification. Only authorized individuals or devices should be able to access any IoMT healthcare system [5].

Inadequate authentication protection leaves users' sensitive healthcare data vulnerable to attackers. It is critical to authenticate users and devices in order to ensure correct data attribution and restrict system information access to authorized parties only [6]. Data from patients who are overweight, for example, could be more reliably recorded if healthcare systems had the ability to confirm the identity of those who use medical devices [7]. Electronic medical records (EMRs) and other personally identifiable information can be better protected with authentication, as only authorized individuals can access them [8]. There are a lot of various ways to make sure that computer systems and networks are secure, and this is an established field of study. There is a wide variety of medical Internet of Things (IoT) applications, including remote health monitoring, care for the aged, and early diagnosis. With the use of the IoT, medical sensors [9], smartwatches, and fitness trackers can gather crucial health data that can illuminate patients' conditions. These devices are essential in healthcare as they enable efficient data collection and sharing. They improve patient monitoring, diagnostics, and overall treatment effectiveness [10]. Thus, the IoT exemplifies new information technology advancements in healthcare. It allows healthcare institutions to track patients' health issues remotely by continuously monitoring patients' vital signs such as temperature, blood pressure, and heart rate [11]. Medical professionals electronically access patient data for remote monitoring. This enables prompt intervention and timely medical decisions [12].

Concerns about data security have grown in response to the increased collection of data, particularly about the private and personal nature of healthcare records. Examples of this type of sensitive personal data are patient diagnoses, medical records, and genetic information [13]. Inadequate protection of sensitive information puts patients at risk of psychological injury, prejudice, and identity theft [14]. The interconnectedness of IoT devices renders them vulnerable to cyber assaults, which in turn compromises the security, privacy, and accessibility of patient information. These breaches have serious legal and financial consequences in addition to endangering patient care [15]. Traditional cryptography algorithms are effective, but many IoT devices just don't have the chip power to use them [16]. Lightweight cryptography (LWC) is a viable option since it lessens the computing burden without compromising security. Elliptic Curve Cryptography (ECC) to increase the scheme's security is proposed [17]. In addition, fresh healthcare-related data supports the idea that safeguarding sensitive medical data requires IoT technologies and lightweight encryption. The data security model for IoMT data is shown in Figure 1.

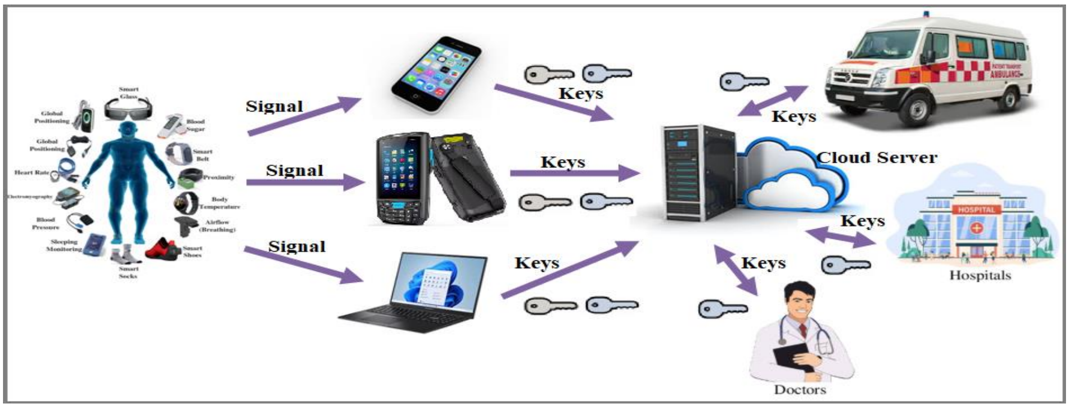

Figure 1. General Internet of Medical Things (IoMT) data security model

The IoT enables real-time data transmission through a network of connected devices. This connectivity enhances communication and data sharing across various systems. The IoT is supported by three layers: perception, network, and application. RFID tags, cameras, and sensors all contribute to the physical layer's data collection capabilities [18]. An integral part of IoT is the network layer, which relays data acquired by the physical layer. It is made up of hardware and software parts. Users' devices are linked to the IoT through the application layer. Two ways of LWC are symmetric key and asymmetric key. In contrast to asymmetric key encryption, which is too complex and computationally costly for the majority of IoT devices, symmetric encryption is useful since it is fast, secure, and has low latency. It is recommended to employ symmetric key cryptography algorithms when constructing IoT devices [19]. They are more popular than asymmetric encryption because they are simpler and need less space, computer power, bandwidth, and storage. Figure 2 depicts the encipher and decipher process using the set of keys.

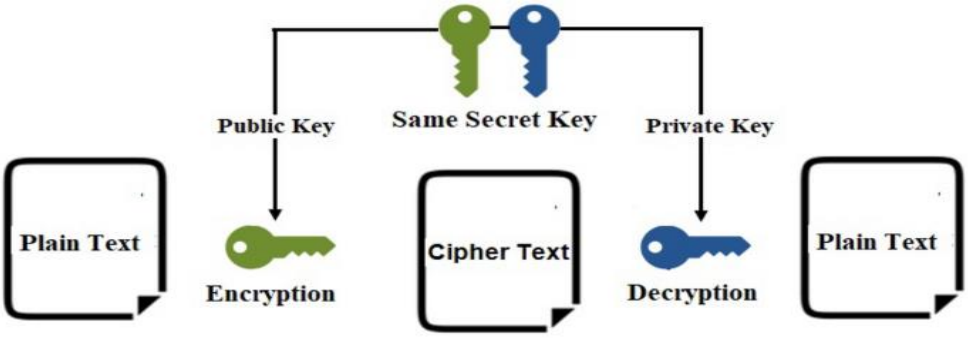

Figure 2. Encipher/decipher process

The varieties of symmetric ciphers are block and stream. When encrypting data, stream ciphers utilize keys of the same length as the data, while block ciphers use keys of a predetermined number of bits. Block ciphers are better suited for the IoT than stream ciphers due to their increased flexibility. The use of block ciphers in resource-constrained computer system design has been ubiquitous in the past decade [20]. This choice was made because of the improved error propagation and diffusion features, the simpler software and hardware implementation, and the ease of use. Fewer hardware resources are needed compared to stream ciphers. Considerations such as structure, key size, round count, and block size are crucial in determining LWC requirements. This research presents a comprehensive analysis of cutting-edge lightweight encryption algorithms that are based on IoT. The size of blocks, length of keys, encryption times, number of rounds, and throughput are some of the metrics used to compare. This research helps numerous researchers and academicians to analyze the models and to provide solutions to enhance the data security levels in medical IoT.

2. LIGHTWEIGHT CRYPTOGRAPHY ALGORITHMS IN MEDICAL INTERNET OF THINGS: OVERVIEW

Through the integration of linked medical equipment, wearable sensors, and smart healthcare systems, the IoMT promises to revolutionize healthcare delivery by enabling round-the-clock patient monitoring, instantaneous diagnosis, and tailored treatment plans. The ecosystem includes a wide variety of devices that capture sensitive health data, such as glucose sensors, implantable heart monitors, smart inhalers, fitness trackers, and remote patient monitoring systems. With early disease identification, reduced hospital readmissions, and proactive medical interventions made possible by the spread of IoMT devices, healthcare has been revolutionized. While new technology has undoubtedly improved service quality and patient safety, it has also brought about unparalleled privacy and security concerns.

The need for strong security measures in IoMT systems has been further emphasized by the rise of complex cyber attacks against healthcare infrastructure. Ransomware assaults on hospital networks and illegal access to patient monitoring devices are just two examples of the many cyberattacks that have targeted healthcare organizations. Many attack vectors, such as device manipulation, man-in-the-middle, data interception, and denial-of-service assaults, are created by the linked nature of IoMT networks. Due to the prevalence of resource-constrained devices and wireless communication channels in IoMT environments, traditional security approaches frequently overlook the specific vulnerabilities that these environments bring. Thus, security solutions that offer complete protection without sacrificing the operational efficiency and service quality necessary for medical applications are urgently needed.

One potential answer to these problems is LWC, which offers security methods developed for low-resource settings. All the while keeping appropriate levels of security in mind for medical applications, these algorithms strive to minimize computational overhead, reduce energy consumption, and optimize memory utilization. Innovative methods for algorithm design, key management, and protocol optimization are necessary for the creation of lightweight cryptographic protocols, which necessitate careful trade-offs between resource efficiency and security strength. In the IoT context, where conventional cryptographic methods are impractical, new developments in LWC have shown that strong security may be achieved with much less resource consumption.

Other restrictions on the choice of cryptographic algorithms are also enforced through regulatory compliance, specifically data privacy standards such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) in healthcare. Law requires that medical records be confidential, accessed by a few persons, readily audited, and containing minimum amount of data. Cryptography algorithms must provide accountability and traceability along with strong encryption, key management, and strong authentication processes. As an example, GDPR mandates cryptographic solutions that communicate with identity management systems, record-keeping systems, and policies, and they should not impose unnecessary computing load.

LWC has the ability to improve service quality in many ways when integrated into IoMT systems. These techniques can increase system reliability, decrease maintenance needs, and prolong device battery life by lowering computational overhead and energy usage. Lightweight cryptographic protocols' enhanced performance features allow for real-time data processing, eliminate communication latencies, and facilitate critical care-essential high-frequency monitoring applications. Along with enabling everything from basic sensor nodes to complicated medical imaging devices inside a single security framework, lightweight cryptographic architectures are scalable and flexible enough to meet the varied needs of heterogeneous IoMT networks. The LWC algorithms with layer-wise representation are shown in Figure 3.

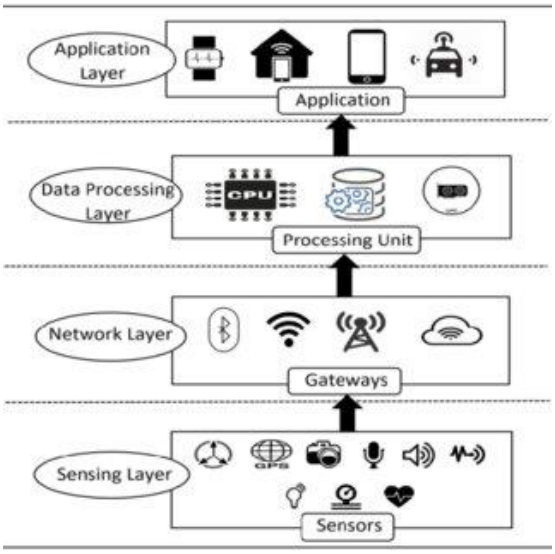

Figure 3. Layer-wise Internet of Things (IoT) model with lightweight cryptography (LWC)

The increasing regulatory demands and industry standards regarding the security of medical devices and the protection of patient data further strengthen the case for this study. Manufacturers are being pushed to show strong security measures all the way through the gadget's lifecycle as regulatory agencies around the world tighten their grip on medical device cybersecurity. Integrating suitable cryptographic protection is now a regulatory need for medical device certification and market access, rather than only a technical consideration. LWC provides a long-term solution for implementing security in environments with limited resources, allowing for compliance with these changing requirements without sacrificing the performance qualities necessary for medical applications.

3. ATTACKS IN MEDICAL INTERNET OF THINGS

3.1 Device-level attacks

Because of their extensive use in unprotected settings, including patients' homes, ambulances, and distant healthcare facilities, medical IoT devices are especially susceptible to physical manipulation assaults. Physically gaining access to insulin pumps, pacemakers, or continuous glucose monitoring enables attackers to steal critical information, alter firmware, or install malicious software. In order to physically tamper with a device, one can open its casing and access its internal components, connect it to unapproved hardware ports, or use specialized equipment to retrieve cryptographic keys from its memory. The fact that many medical equipment does not have strong tamper-detection features and keep working properly even after being hacked makes these attacks all the more worrisome.

3.2 Network-level attacks

Medical IoT networks are vulnerable to man-in-the-middle attacks because these attacks take advantage of the wireless communication channels that devices and healthcare systems typically employ to transmit data. In order to stealthily alter, reroute, or intercept medical data without the knowledge of authorized parties, attackers position themselves between communicating equipment. Impacting patient vital sign readings transmitted from patient monitors to central systems, changing drug dose instructions transmitted to infusion pumps, or intercepting sensitive patient information during transmission are all examples of the serious outcomes that can result from these types of assaults in healthcare settings. Medical IoT connections are especially vulnerable to interception attempts due to their wireless nature and the fact that encryption implementations are typically poor. In order to carry out these assaults, hackers can utilize easily accessible tools to intercept wireless traffic, take advantage of insecure authentication procedures, or even build fake access points that look like real healthcare network infrastructure.

3.3 Data-level attacks

Because they can change vital health information covertly, data manipulation assaults are among the most dangerous threats to medical IoT systems and the safety of patients. Medical monitoring data, prescription administration records, and diagnostic results are all potential targets of attackers looking to fabricate medical emergencies, conceal real health issues, or provoke unwarranted medical treatments. Threats like this can happen at any stage of the data lifecycle, from when sensors are collecting data to when it is transmitted, stored, or processed in healthcare databases or clinical decision support systems. Healthcare providers may be misdiagnosed, given the wrong therapy, or even delayed in responding to emergencies due to manipulated information that looks very valid because of the sophistication of modern data manipulation tools.

3.4 Authentication and authorization attacks

By taking advantage of loopholes in device authentication methods, identity spoofing attacks can masquerade as genuine medical devices or healthcare workers on IoT networks. In order to obtain unauthorized access to healthcare systems, attackers might counterfeit digital certificates, clone device identifiers, or take advantage of weak authentication procedures. By impersonating a trusted healthcare provider, an attacker in a healthcare setting can get access to sensitive patient information, inject malicious data into medical devices, or inject fraudulent medical data. Because they seem to come from trustworthy sources within the healthcare network, these assaults can overcome perimeter security safeguards, making them particularly deadly. To make matters worse, a lot of medical IoT devices are susceptible to easy spoofing attacks since they use basic authentication mechanisms or depend on easily replicable identities.

4. TYPES OF LIGHTWEIGHT CRYPTOGRAPHY ALGORITHMS

4.1 Symmetric key cryptography algorithms

With their quick encryption and decryption procedures and little computing overhead, lightweight symmetric encryption algorithms are the backbone of resource-constrained cryptographic systems. Because of their well-balanced security-performance properties, the Advanced Encryption Standard (AES) variations, especially AES-128, are among the most extensively used lightweight symmetric algorithms. The 128-bit key length and strong security provided by AES-128 make it an ideal choice for many IoT applications due to its minimal computational cost and memory requirements. Even AES-128 might be too demanding for very resource-constrained environments, so developers came up with ultra-lightweight alternatives like PRESENT. Compared to traditional AES implementations, it runs on 64-bit blocks with 80-bit or 128-bit keys and uses a lot fewer hardware resources. The symmetric key cryptography model is shown in Figure 4.

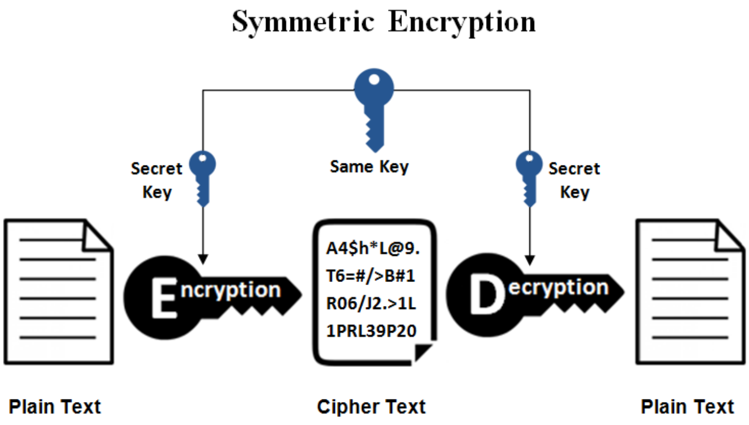

Figure 4. Symmetric cryptography model

For ASIC and FPGA implementations where power consumption and gate count are crucial, SIMON is a great choice due to its simple structure, focused solely on bitwise operations, which focuses on hardware efficiency. SPECK, in contrast, puts software efficiency ahead of hardware efficiency by making use of ARX operations (Addition, Rotation, and XOR), which are well-suited to contemporary processor designs. To accommodate varying levels of security and practical limitations, both ciphers are compatible with a wide range of block and key sizes. Use of a generalized Feistel structure with efficient diffusion and confusion qualities allows for high-speed implementations with low memory requirements; this algorithm, CLEFIA, provides an alternative method of lightweight symmetric encryption.

4.2 Block cipher algorithms

When conventional cryptographic methods aren't an option due to a device's limited resources, ultra-lightweight block ciphers are a great solution. This class of ciphers is exhibited by the PRESENT cipher, which has a substitution-permutation network architecture with a small 64-bit block size and a memory footprint of about 1,570 gate equivalents in hardware implementations. Using a simple 4-bit S-box reused throughout the encryption process, its design philosophy prioritizes hardware efficiency, allowing for cost-effective implementation in severely constrained hardware conditions. Lightweight Encryption Device (LED) cipher takes a different tack, utilizing a framework similar to AES but optimized for lightweight implementation. The block cipher model is shown in Figure 5.

4.3 Stream cipher algorithms

For applications that need continuous data encryption with minimal buffering needs and low-latency processing, lightweight stream ciphers are a great alternative to block ciphers. The Trivium cipher is a well-known example of this type of encryption. The cipher's initialization vector and 80-bit key ensure sufficient security for numerous lightweight applications while preserving the computational efficiency necessary for devices powered by batteries. The stream cipher model is shown in Figure 6.

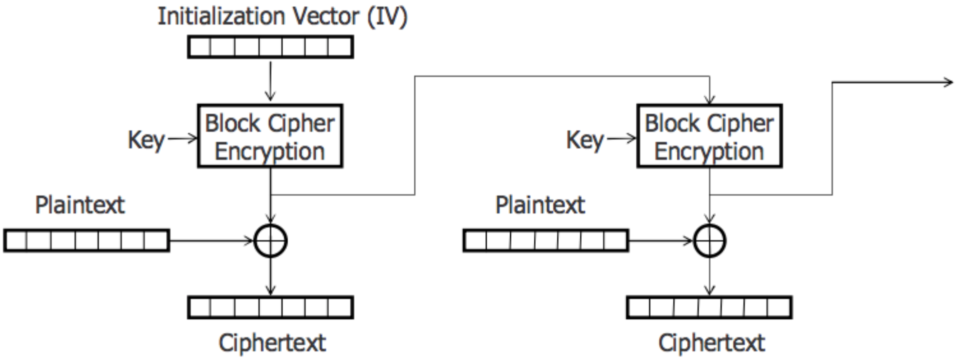

Figure 5. Block cipher model

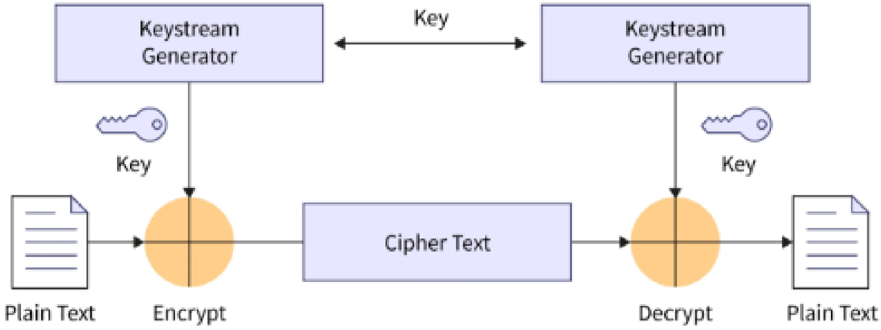

Figure 6. Stream cipher model

4.4 Hash function algorithms

In situations where conventional hash algorithms such as SHA-256 are not feasible due to resource limitations, lightweight cryptographic hash functions play an essential role in authentication, digital signatures, and key derivation applications. A series of hash functions called PHOTON uses a sponge architecture with internal variations that are optimized for both software and hardware implementation to demonstrate effective hash design in limited conditions.

Various PHOTON variations support output widths ranging from 80 bits to 256 bits, allowing for applications to make suitable security-performance trade-offs while still requiring compact implementation. Despite offering sufficient security for many IoT authentication applications, the algorithm's design prioritizes serial processing performance and minimal memory usage, making it ideal for devices with severe resource limits. The hash function model is shown in Figure 7.

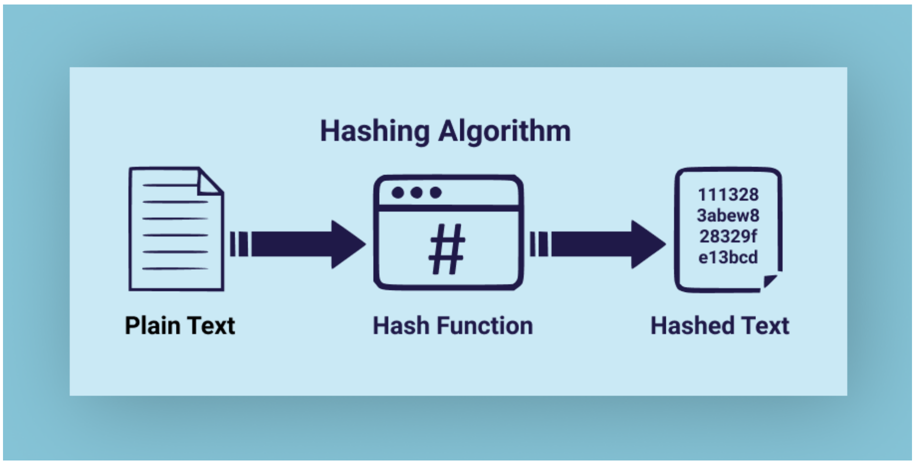

Figure 7. Hash function model

4.5 Message authentication code algorithms

When conventional HMAC implementations are too taxing on system resources, lightweight message authentication code (MAC) algorithms step in to verify the authenticity and integrity of data. Use of an ARX-based structure allows for high-performance implementation in software and hardware contexts while requiring minimal computational resources and memory, as shown by the Chaskey MAC method, which is an example of an efficient authentication architecture. Chaskey's approach is appealing for IoT applications that need authentication procedures frequently since it enables various message lengths, offers good security guarantees against forgery attacks, and is simple to implement. Implementing the algorithm efficiently is possible even on platforms with very limited resources, thanks to its compact internal state and 128-bit key size. The MAC algorithm model is shown in Figure 8.

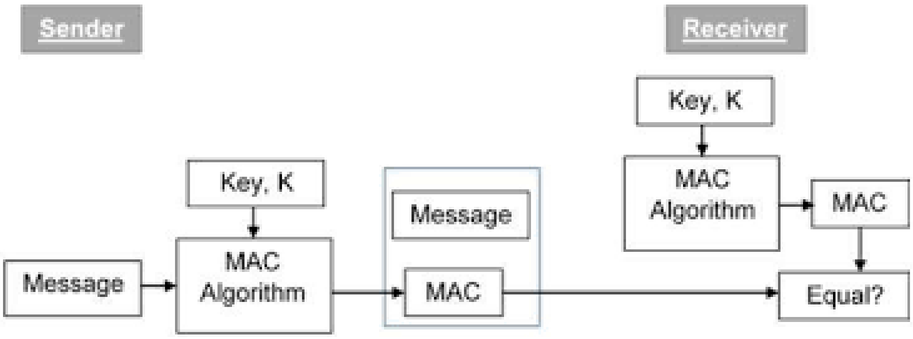

Figure 8. Message authentication code (MAC) algorithm model

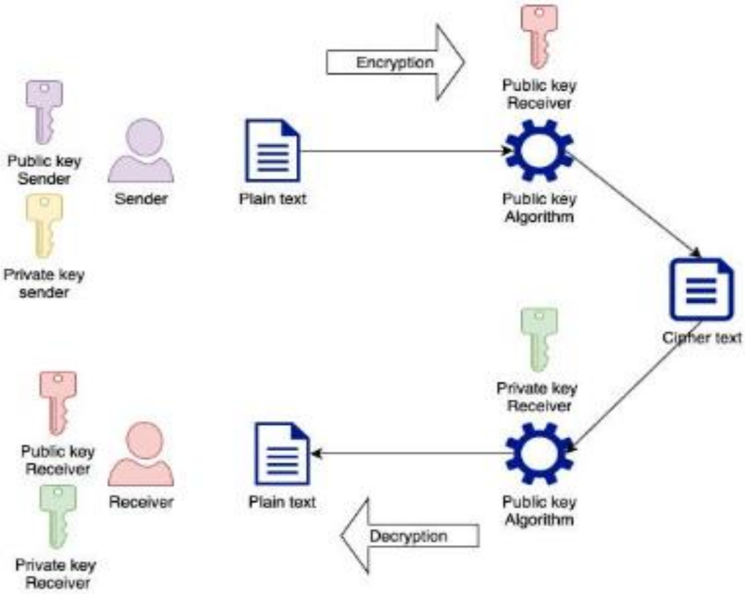

Figure 9. Public key cryptography model

4.6 Public key cryptography algorithms

With decreased processing requirements and key sizes that are comparable to RSA, ECC provides the same level of security in resource-constrained contexts. To keep processing time and memory use to a minimum, lightweight ECC solutions prioritize efficient curve arithmetic and optimized point multiplication techniques. Specialized curves, such as FourQ, give improved performance via sophisticated mathematical structures, and general-purpose curves, such as secp256r1 and Curve25519, offer robust security with reasonably efficient implementation properties. Optimizing field arithmetic operations and point representation formats can be a challenge when trying to implement lightweight ECC due to the low processing capabilities and memory limits common of IoT devices, which must be balanced with security needs. The public key cryptography model is shown in Figure 9.

4.7 Standardization progress of lightweight cryptography algorithms

Recent years have seen LWC proceed well along the road to standardization, particularly with regard to the IoMT in the medical sector. Upon observing that ordinary cryptographic algorithms have difficulties in operating with devices with limited resources, bodies such as NIST and ISO/IEC have embarked on specifying lightweight security primitives. The NIST Lightweight Cryptography Standardization Project has been a huge stride forward and has brought about the use of such algorithms as ASCON in hashing and encrypting messages authentically. Some of the critical requirements of medical sensors, implanted devices, and wearable systems are a reduction in computational latency, energy usage, and memory size. These standard primitives are aimed at providing strong security guarantees and simply doing so. When patient safety is a primary concern in the hospital environment, the availability of standardized LWC algorithms enhances confidence in their cryptographic power, simplifies the process of performing independent security reviews, and enables regulatory acceptance.

Lightweight cryptographic methods suitable for small-context applications are, in turn, characterized by ISO/IEC standards such as ISO/IEC 29192. This group of standards offers a specific guideline in acceptance of algorithms in the IoMT deployments through suggestions of embedded-system optimized block ciphers, stream ciphers, and hash functions. However, official standards of many lightweight algorithms depicted in academic literature are still missing and hinder their application in a controlled medical environment, although progress in this field has been observed. Healthcare providers and manufacturers of medical devices tend to prefer standardized and well-tested algorithms that are preferred both to ensure certification, compliance, and long-term maintenance. To build interoperable, auditable, and regulatory conformant medical IoT systems, it is important to make the connection between the IoMT security designs and future LWC standards.

It is demanded that a uniform security architecture that involves flexible integration strategies in combination with LWC specifications can be an answer to these issues. One of the possible solutions is to employ a hybrid cryptographic system. In this arrangement, devices execute standard sanctioned, lightweight symmetric algorithms, and gateways and backend systems execute more complex but interoperable protocols to exchange keys and convert protocols. End-to-end security has a medical application whereby heterogeneity in devices is supported with Quality of Service (QoS) standards, possibly through layered architectures.

5. LITERATURE SURVEY

5.1 Overview of cryptographic models

Cryptographic models ensure data security, authentication, privacy, and secure communication across various domains. Authentication Models verify user or device identities through techniques such as password-based authentication, biometric authentication, multi-factor authentication (MFA), and digital signatures, ensuring only systems and data have authorized access. LWC Models are optimized for “resource-constrained devices like IoT, RFID, and embedded systems” using efficient encryption techniques such as lightweight block ciphers (SIMON, PRESENT, SPECK) and hash functions (PHOTON, SPONGENT) to balance security with low computational cost. Privacy Preservation Models focus on protecting sensitive information through methods like Homomorphic Encryption, Differential Privacy, Zero-Knowledge Proofs (ZKP), and Secure Multi-Party Computation (SMPC), enabling secure data processing in untrusted environments. Communication Security Models safeguard data transmission over networks through protocols like Transport Layer Security (TLS/SSL), End-to-End Encryption (E2EE), and Internet Protocol Security (IPSec), emerging technologies like Quantum Cryptography, preventing unauthorized interception and tampering in applications such as messaging, VPNs, and online banking. Together, these cryptographic models provide a comprehensive security framework, ensuring confidentiality, integrity, and authentication in digital systems. The cryptography model for IoMT data is shown in Figure 10.

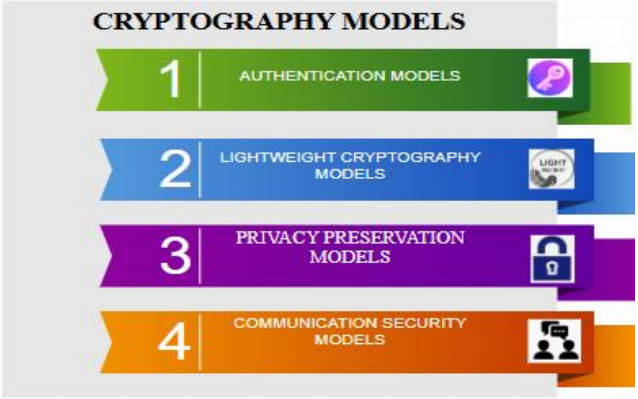
CRYPTOGRAPHY MODELS
1
AUTHENTICATION MODELS
2
LIGHTWEIGHT CRYPTOGRAPHY MODELS
3
PRIVACY PRESERVATION MODELS
4
COMMUNICATION SECURITY MODELS

Figure 10. Cryptographic model for Internet of Medical Things (IoMT)

5.1.1 Authentication models

A wide range of readily and commercially available components can be used to construct consumer electronics devices that are capable of communicating with one another. The security of the system and the environment are put at risk since thieves have more chances to take advantage of security holes and conduct a full-scale attack on the network. Since intruding hostile devices can corrupt servers and transmit dangerous data to the cloud or the server itself, they constitute a threat to the entire network. To get around this, Yanambaka et al. [1] designed a Physical Unclonable Function (PUF)–based device authentication approach that is interoperable with the IoMT.

Threats, such as man-in-the-middle attacks, modification assaults, and DoS, compromise the security and confidentiality of IoT networks. These attacks mostly utilize wireless channels for communication. A lightweight user authentication technique that safeguards users' anonymity in response to these security concerns is presented by Masud et al. [2]. Using the method that is given, legitimate users can set up secure sessions, and the IoT sensor nodes can be protected from unauthorized users. To safeguard real-time patient data, a lightweight anonymous user authentication solution was introduced. Since this protocol relies solely on hash functions rather than public-key cryptography, many researchers considered it suitable for sensor node deployment. This protocol desynchronizes in response to message jamming or blocking, and as demonstrated by Shihab and AlTawy [3], it is susceptible to session key leaks and hence cannot guarantee forward secrecy in all circumstances. A lightweight mutual authentication protocol called LAPRD was proposed by the author as a remedy for these issues; it provides resilience against desynchronization attacks.

To ensure secure communication between doctors, gateways, and IoT sensor nodes in healthcare, protecting patients' physiological data is essential. A lightweight and anonymous user authentication mechanism is being studied for this purpose. Still, in this piece, Wang et al. [4] examined their plan once again. Attacks like session key disclosure, offline password guessing, and tracing can compromise it, as the author pointed out. These vulnerabilities imply that the attacker has access to the doctor's smartphone and the sensor nodes. Furthermore, the author provided answers to each of these security issues. Authentication is a critical step in securing physiological data by verifying user identity and preventing unauthorized access. Some proposed authentication systems for WBANs have had their weaknesses and resource requirements pointed out. Two-Party Lightweight Authentication Protocol (TLAP) was proposed by Lara et al. [5] for use with WBANs. Verified by both official and informal assessments, TLAP safeguards WBANs from potential attacks and enables two-way authentication.

Zhou et al. [6] implemented various security measures to uphold the integrity of traditional protocols. To validate the effectiveness of the enhanced protocol, the author applied comprehensive formal and heuristic security analyses. Comparative evaluations with similar protocols confirmed that the proposed approach delivers efficient performance in resource-limited IoMT environments. The potential for modern WBANs to revolutionize the way the IoT networks is used to enhance human health and well-being is enormous. Using mobile-edge computing as an example, Yang et al. [7] suggest a very lightweight authentication method for WBANs. Sensor nodes and Edge nodes (ENs) use the modular square roots technique for intra-BAN authentication, and application providers and ENs use it for inter-BAN authentication. On top of that, two separate authentication phases are planned. When evaluating performance, we also take into account the costs of computation, networking, and storage.

Lightweight hybrid authentication, data privacy, and preservation were proposed by Adil et al. [8] as a solution to these security challenges. The proposed model integrates a supervised machine learning (SML) algorithm with a cryptographic parameter-based encryption and decryption (CPBE&D) mechanism. This approach verifies the authenticity of IoMT-based cyber-physical systems (CPS) before allowing encrypted data transmission over wireless networks. The authentication models are shown in Table 1.

Table 1. Authentication models

Author Name	Year of Publication	Proposed Model	Scope of the Paper	Limitations	Results
Yanambaka et al. [1]	2020	An IoMT-compatible device authentication mechanism that makes use of Physical Unclonable Functions (PUFs).	PMsec is an authentication technique resistant to device forgery and hacking.	PUF-generated outputs can vary with environmental variables like temperature, voltage fluctuations, and aging effects, which can lead to authentication failures.	PMsec achieved 99.7% authentication; it requires only 3.2 KB of ROM and 1.8 KB of RAM.
Masud et al. [2]	2022	A user authentication mechanism was introduced for providing lightweight and protecting users' anonymity.	Medical IoT devices with limited resources can benefit from efficient, safe, and privacy-enhancing authentication processes.	It can be challenging to ensure strong authentication while retaining a lightweight footprint, which might lead to trade-offs in security strength.	This approach reduced computational overhead by 43%, requiring only 0.85 seconds for complete authentication on resource-constrained devices.
Shihab and AlTawy [3]	2023	LAPRD is a streamlined authentication protocol developed to withstand desynchronization attacks.	It offers quick and safe authentication for healthcare IoT (H-IoT) devices while reducing the danger of desynchronization attacks.	The measures used to prevent desynchronization attacks could increase communication or computing costs.	The results show a 0.5% false acceptance rate (FAR) and a 0.7% false rejection rate (FRR), ensuring security and reliability.
Wang et al. [4]	2023	An improved user authentication scheme is proposed for IoT-based healthcare, resolving vulnerabilities in	This tool assists in finding and fixing security gaps in the authentication system before it's even deployed. Finding and fixing	Need for thorough testing, specialized knowledge, and specialized tools to detect any vulnerabilities.	It records an average authentication time of 1.8 ms. The scheme effectively detects desynchronization attacks with a 97.2%

		Masud et al.'s [2] design.	vulnerabilities like man-in-the-middle and replay.		success rate.
Lara et al. [5]	2021	Two-Party Lightweight Authentication Protocol (TLAP) used, ECCto lower the protocol's computational cost.	This technique is lightweight and used for WBANs in healthcare applications.	The process of creating self-certified public keys can reveal flaws if not planned well, which could make devices vulnerable to forging or key-reuse attacks.	TLAP significantly decreases energy consumption in WBANs.
Zhou et al. [6]	2024	The author used a wide variety of heuristic and formal security analysis techniques to verify that this enhanced protocol is effective.	It offers strong privacy protection for users by preserving their anonymity, which guarantees that patient data stays private and cannot be linked to specific persons.	The need for additional training for healthcare personnel and the need for meticulous integration with current healthcare systems, the implementation complexity can be significant.	The paper ensures user anonymity while mitigating security threats. The results demonstrate the scheme's effectiveness in providing secure authentication.
Yang et al. [7]	2022	An exceptionally lightweight authentication technique for WBANs enabled by mobile-edge computing is proposed in this article.	By integrating WBAN devices with mobile-edge computing, real-time health monitoring capabilities are enhanced, and processing times and latency are lowered.	Because different kinds of WBAN devices have differing hardware capabilities and resource limitations, it can be difficult to keep security standards consistent among them.	The scheme achieved an average authentication time of just 38ms on resource-constrained wearable devices, with energy consumption reduced by 72%
Adil et al. [8]	2023	The model combines SML with cryptographic parameter-based encryption and decryption (CPBE&D).	Enhanced efficiency, security in certifying devices, and safeguarding data transfer are two benefits of AI-enabled hybrid lightweight authentication techniques.	A key challenge in IIoT is ensuring privacy-preserving data transactions and adaptive security to distinguish benign from malicious activities.	The scheme authenticated IoMT requests in 23ms and reduced energy consumption by 83%, enhancing attack detection.

Table 2. Lightweight cryptography (LWC) models

Author Name	Year of Publication	Proposed Model	Scope of the Paper	Limitations	Results
Ning et al. [9]	2020	The author proposed a framework to evaluate and select the best lightweight cryptographic ciphers.	Due to the integration of different MCDM techniques like AHP, TOPSIS, or VIKOR, the evaluation of cryptographic algorithms is balanced.	Implementation is difficult due to the complexity of integrating different MCDM methodologies.	PRESENT-80 emerged as the optimal lightweight cipher for Internet of Healthcare Things (IoHT) applications.
Yavuz and Ozmen [10]	2022	Embedded devices with limited resources are well-suited for initial implementation. The SEMECS framework enables efficient digital signatures using Elliptic Curve Cryptography (ECC).	Ultra-lightweight multiple-time digital signature techniques are given more flexible for IoT devices, especially in settings with limited resources.	Because of the simpler cryptographic structures, one important problem is that they may be vulnerable to cryptanalysis.	The Signature generation time averaged 245 milliseconds on the 8-bit platform and just 28 milliseconds on the ARM device
Guo et al. [11]	2024	The author suggested Error-Correcting Lightweight Block Cipher (ECLBC), a lightweight block cipher that includes techniques for error detection and correction, it transitions modes within AND-rotation-XOR (AND-RX)	ECLBC is an excellent choice since it provides efficient and safe encryption with built-in error detection and correction algorithms.	The inclusion of error detection and repair systems may cause significant computational overhead, which could impact real-time applications that demand ultra-fast processing.	The cipher's novel error correction mechanism successfully detected 99.7% of single-bit errors and corrected 94.2% of them without additional hardware support.

5.1.2 Lightweight cryptography models

The decision-making process is further complicated by the fact that healthcare IoT devices have intrinsic limitations such as low computing power, memory, and bandwidth. To be more precise, Ning et al. [9] provided a methodology for evaluating lightweight cryptographic ciphers that consider the most important aspects. The proposed framework factors in the recommendations of internationally recognized standards, such as ISO/IEC 29192 for building evaluation criteria and NIST for performance, physical, and security. In this study, Yavuz and Ozmen [10] make two contributions: Signer Efficient Multiple-time Elliptic Curve Signature (SEMECS) is a digital signature framework designed for resource-limited embedded systems. It enables the creation of elliptic curve (EC)-based signatures even when the signer has limited familiarity with EC operations by optimizing private key and signature sizes.

The development of a secure, lightweight block cipher presents a significant obstacle in such situations. As a result, the Error-Correcting Lightweight Block Cipher (ECLBC), proposed by Guo et al. [11], is a lightweight block cipher that incorporates error repair and detection algorithms. ECLBC enhances security with fewer rounds by serving a dual purpose as it switches modes within AND-rotation-XOR (AND-RX) lightweight block ciphers. The models of LWC are shown in Table 2.

5.1.3 Privacy preservation models

The expansion of the IoT has given rise to a new paradigm in healthcare, dubbed smart health. It can reliably predict the onset of some diseases and also improve the quality of healthcare. Data security and consumer privacy issues, however, remain unresolved. Despite their many drawbacks, such as a lack of privacy for user attributes and excessive overhead, cipher text policy attribute-based encryption (CP-ABE) systems provide a potential solution to the challenge of securing s-health applications that are targeted toward the IoT. Sun et al. [14] proposed an ideal vector transformation approach to reduce the length and remove redundancy from the list of user attributes and access regulations, which is an important step in addressing these issues.

Table 3. Privacy preservation models

Author Name	Year of Publication	Proposed Model	Scope of the Paper	Limitations	Results
Sun et al. [14]	2020	An optimal vector transformation method that efficiently converts the set of user attributes and access policies into shorter vectors, eliminating redundancy and reducing their overall length.	Healthcare professionals can access only the patient data they need because of the fine-grained access control mechanism.	An increase in administrative burden may result from the need to manage and maintain comprehensive access policies.	The proposed scheme lowers the 8% computational overhead in key generation, encryption, and decryption. This enhances efficiency for resource-constrained IoT devices.
Yang et al. [15]	2020	LiBAC, a lightweight break-glass access control system, allows for both attribute-based and break-glass access to encrypted medical files.	This is well-suited to situations involving emergency healthcare.	It introduces security holes that could be exploited by bad actors to obtain vital medical data.	The LiBAC system allows authorized personnel timely data retrieval with 97% accuracy. LiBAC is designed to be lightweight, minimizing 5% computational demands on healthcare IoT devices.
Li et al. [16]	2023	Used distributed storage to address the issue of centralized management. A lightweight (t,n) -threshold secret sharingis developed to enhance the efficiency and security of medical data sharing.	Integration of Blockchain and Lightweight Secret Sharing into the Internet of Medical Things (IoMT) is well-suited for IoMT devices.	With blockchain integration comes the possibility of growing storage needs as the chain expands, which could put a burden on system resources.	The performance evaluation of the proposed scheme demonstrates its effectiveness in maintaining data privacy while ensuring efficient communication among IoMT devices with 95% accuracy and efficiency.
Fugkeaw et al. [17]	2023	LightMED, which makes use of fog computing, CP-ABE, and blockchain technology.	The distributed, immutable, and transparent ledger known as blockchain technology has the potential to revolutionize the IT industry by solving many problems.	Given the sensitive nature of healthcare data and the need to prevent any unlawful access or publication, safeguarding patient identities is an important consideration.	Performance testing showed the access control mechanism processed authorization requests in an average of 85 ms, with end-to-end transaction latency averaging 215 ms even under high load conditions of 750 concurrent users.

In healthcare, the capacity to swiftly retrieve patient records during an emergency is crucial. A lightweight break-glass access control system called LiBAC was developed by Yang et al. [15]. It enables both attribute-based and break-glass access to encrypted medical data. The access policy associated with a medical file dictate whether a healthcare professional can decrypt and retrieve the stored information. In emergencies, the break-glass access mechanism overrides the file's access policy, allowing rapid data retrieval for urgent medical care or rescue operations. To solve the problem of centralized management, Li et al. [16] used distributed storage to lay the groundwork for hidden reconstruction and retrieval. After that, a plan to improve the safety and efficacy of medical data sharing is devised for lightweight (t,n) -threshold secret sharing (t/n -SS). Using the interleaving encoding technique, it partitions the original message into smaller pieces.

Delegating the generation of encrypted EMRs, which integrate health data from IoT devices with medical applications, enhances accessibility, facilitates efficient collaboration, and eliminates computational overhead. This approach aligns with advancements in healthcare-related IoT and cloud computing. Fugkeaw et al. [17] suggested LightMED, an access control method that utilizes fog computing, CP-ABE, and blockchain technology, for secure, granular, and scalable EMR sharing in the cloud. The author laid out a safe method for sending and aggregating IoT data using lightweight encryption and digital signing. At its core, the product is a blockchain-enabled encryption and decryption technique that is outsourced. Additionally, it has a privacy-protecting access policy framework. The author introduced a novel approach to further aid EMR data owners in securely and efficiently administering their rules. Table 3 shows the models for privacy preservation.

5.1.4 Communication security models

Quite a few of these solutions put users' anonymity and privacy at risk. In view of the problems with existing protocols, Chen et al. [18] proposed a safe and effective protocol based on extremely lightweight symmetric key operations. The author provided formal and informal assessments to bolster the safety of the protocol. Furthermore, a real-time experiment was conducted by the author to evaluate the protocol's efficiency. However, there are a lot of challenges to secure data transfer caused by the nanoscale aspect of this technology. For data transmission to be secure, authentication is a must. Regarding this, a novel IoNT authentication method based on elliptic curve encryption was presented by Rana et al. [19]. Considering the limited processing power of nanoscale devices, this approach ensures lightweight yet robust authentication using a secure hash function and XOR operations. A subfield of healthcare IT, Telecare Medical Information Systems (TMIS) allows for the remote provision of medical treatment thanks to the expansion and enhancement of ICT. Mobile healthcare apps (MHA), smartphones, the IoT, and hospital servers form the backbone of TMIS. Ahamad et al. [20] presented the Secure and Resilient Scheme for Telecare Medical Information Systems (SRSTMIS), protected by white-box cryptography (WBC) are keys utilized in healthcare applications, SE, UICC, and TPM.

6. DISCUSSIONS

Lightweight symmetric block ciphers are widely used in pervasive figuring. Two types of symmetric ciphers are block and stream ciphers [21]. There are no hard and fast rules for how they can be categorized as lightweight, and they are purposefully used with devices [22]. There are three important aspects that every LWC architect must address: security, cost [23], and performance [24]. Simplifying optimization for just one of the three main design objectives, cost and performance, security and cost, or both, is far easier than optimizing for all three simultaneously. Symmetric ciphers include features like message integrity checks, encryption, entity authentication, etc., whereas asymmetric ciphers include features like non-repudiation and key management [25].

Table 4. Standard and lightweight cryptographic algorithms for secure IoT communication

Algorithm	Type	Key Size (bits)	Plaintext Size (bits)	Rounds	Security Analysis	IoT Use Case	Category
AES	Block Cipher	128, 192, 256	128	10, 12, 14	Differential cryptanalysis/Side-channel Differential fault attacks	General IoT Security	Standard
PRESENT	Block Cipher	80, 128	64	31	Differential crypta analysis, Related key attack	RFID, Sensor Networks	Lightweight
GIFT	Block Cipher	128	64	40	MITM/Biclique	IoT Devices	Lightweight
SKINNY	Block Cipher	64, 128	64, 128	32, 56	Side-channel/Differential fault attacks	Smart Cards	Lightweight
RECTANGLE	Block Cipher	80, 128	64	25	Side-channel/Differential fault attacks	IoT Communications	Lightweight
MIDORI	Block Cipher	64, 128	64, 128	16	Differential and Linear crypta analysis	Low-power IoT	Lightweight
mCrypton	Block Cipher	64, 96, 128	64	12	Related key attack	Embedded Systems	Lightweight
NOEKEON	Block Cipher	128	128	16	Related key attack	Secure Communications	Lightweight
ICEBERG	Block Cipher	128	64	16	Differential crypta analysis	Secure IoT Data	Lightweight
PUFFIN-2	Block Cipher	128	64	24	Differential crypta analysis	IoT Authentication	Lightweight
PRINCE	Block Cipher	128	64	12	Differential crypta analysis	RFID, Wearables	Lightweight
PRINT	Block Cipher	48, 96	64	48	Related key attack	RFID Tags	Lightweight
Klein	Block Cipher	64, 80, 96	64	12, 16, 20	Side-channel/Differential fault attacks	IoT Encryption	Lightweight
LED	Block Cipher	64, 128	64	32, 48	Differential crypta analysis	IoT Embedded Systems	Lightweight
EPCBC	Block Cipher	80, 128	32	32	Related Key attack	RFID Tags	Lightweight
TEA	Block Cipher	128	64	64	Related Key attack	Secure IoT Communications	Standard
XTEA	Block	128	64	64	Related Key attack	IoT Devices	Standard

	Cipher						
Camellia	Block Cipher	128, 192, 256	128	18, 24	Side-channel/Differential fault attacks	Secure IoT Storage	Standard
SIMON	Block Cipher	32-128	32-128	Variable	Differential crypta analysis	Embedded IoT Security	Lightweight
MIBS	Block Cipher	64, 128	64	32	Differential and Linear crypta analysis	IoT Authentication	Lightweight
LBlock	Block Cipher	80	64	32	Differential, MITM/Biclique	Low-Power IoT	Lightweight
ITUbee	Block Cipher	80	64	10	Related key attacks	IoT Applications	Lightweight
CLEFIA	Block Cipher	128, 192, 256	128	18, 22	Side-channel/Differential fault attacks	Secure IoT Applications	Standard
PICCOLO	Block Cipher	80, 128	64	25	Differential, MITM/Biclique	Low-power IoT	Lightweight
TWIS	Block Cipher	128	64	10	Differential crypta analysis	IoT Data Encryption	Lightweight
TWINE	Block Cipher	80, 128	64	36	MITM/Biclique	IoT Embedded Security	Lightweight
HIGHT	Block Cipher	128	64	32	Differential, MITM/Biclique	IoT Communications	Lightweight
LEA	Block Cipher	128, 192, 256	128	24, 28, 32	Side-channel/Differential fault attacks	IoT Security	Standard
KeeLoq	Block Cipher	64	32	Variable	Linear/Side-channel/Differential fault attacks	Remote Keyless Entry	Proprietary
KATAN	Block Cipher	80	32, 48, 64	48	MITM/Biclique	Sensor Networks	Lightweight
KTANTAN	Block Cipher	80	32, 48, 64	48	Related key attacks	RFID, IoT Security	Lightweight
Hummingbird-2	Stream Cipher	128	16	-	Related key attacks	RFID and IoT Authentication	Lightweight
Hummingbird	Stream Cipher	256	16	-	Several attacks	RFID and IoT Security	Lightweight

Concerns about cybercrime have dominated studies of IoT. Finding a clear solution that works for all types of IoMT is challenging. An IoMT infrastructure connects several types of systems [26]. The majority of IoT devices have limited resources, unlike some equipment that can afford to be big and safe. Their ideal network security solution would be one that responds rapidly. The same goes for how easy it is to use and modify. The issue of trustworthy security comes up last but not least [27]. Lightweight cryptographic methods, taking into account the limitations of IoT devices, were the starting point of this research. There was an investigation into both symmetric and asymmetric key cryptography. It is found that a lightweight Asymmetric Cryptographic solution satisfied the requirements for an IoT solution, which are to be both faster and easier [28]. One of the most recent developments in the field of technology, electronic healthcare systems have numerous potential uses, including remote health monitoring [29], evidence-based treatment, disease prediction, modeling, and many more. Many IoT gadgets and bodily sensors are part of these data-gathering systems. Ensuring safe data transmission becomes extremely challenging in this situation due to the low memory and power of the devices [30]. Focusing on a lightweight ciphering technology, this research aims to secure an electronic healthcare system. Conventional encryption methods are unsuitable due to the operational complexity. The overall algorithms are discussed briefly in Table 4.

6.1 Reliable basis for algorithm selection

To address the issue of irregular reviewing of performance, this paper proposes a methodological way of systematically reviewing medical IoT algorithms. The proposed structure standardizes the testing conditions, reporting schemes, and measure thresholds, whereas in earlier studies, the performance time, memory consumption, latency, or throughput are analyzed separately and in different test conditions. This ensures that comparative tests on the efficiency of various lightweight cryptographic and security mechanisms can be reproducibly done and applied in real-life scenarios in the application of medical IoT devices.

The initial stage of the proposed system is categorizing medical IoT devices into very specific functional categories, such as implanted devices, wearable sensors, bedside monitoring units, and gateway or edge nodes. Each class has some hardware requirements, which are the likes of processor architecture, clock speed, the size of available RAM and ROM, power supply, and the type of communication technology. To prevent coming out with results that are too generic or abstract, we consider the performance of the algorithm in these specific classes.

6.2 Quantitative analysis

This paper recommends the use of normalized multidimensional performance and security metrics of cryptographic algorithms to compare them quantitatively. Security metrics are the level of resistance to particular classes of attacks, key length, cryptographic strength equivalence, and protocol resilience, whereas performance metrics are the execution time, latency, memory footprint, and energy usage per safeguarded transaction. Objective evaluation of trade-offs can be made relative to determining them subjectively by measuring the outcome in normalized units such as cycles per bit, energy per message, and strength against the cost of security resources.

Each potential medical IoT application situation should have a different point of security-performance balance. Two applications of emergency monitoring that must have very low latency and high availability are the detection of cardiac arrest or the transmission of critical alarms. Cryptographic algorithms adopted in such scenarios need to minimize computing overhead and handshake delays to ensure high levels of authentication and integrity. To enable designers to select algorithms that operate within real-time constraints without compromising patient safety, quantitative upper bounds on acceptable latency and energy use can be developed.

Fitness bracelets and health trackers used to monitor chronic illnesses, in turn, are intended to be used over a day or longer and prioritize energy efficiency and lifespan of the gadgets over real-time reactiveness. In these situations, algorithms may be capable of tolerating a tiny amount of latency when they reduce power consumption by a huge percentage. Quantitative analysis can be used to discover cryptographic algorithms that are the most energy-efficient on a message-by-message basis yet remain with an adequate level of confidentiality and integrity even when running over lengthy periods.

These disparities can be operationalized by applying a multi-criteria decision framework that gives security and performance measures weights based on the criticality of the application. In emergency applications, latency and availability are weighted higher; in daily monitoring, energy economy is weighted higher, compliance and strength of security are weighted higher in intra-hospital systems. Algorithms are rated based on weighted aggregate scores, instead of being assessed subjectively, providing guidelines on how to choose them. The Mapping of Medical IoT Application Scenarios to Security-Performance Priorities are indicated in Table 5.

Table 5. Mapping of medical IoT application scenarios to security-performance priorities

Medical IoT Application Scenario	Latency Requirement	Energy Efficiency	Security Strength	Availability and Reliability	Memory / Resource Constraint	Regulatory Compliance Priority
Emergency Medical Monitoring (e.g., cardiac monitoring, insulin pumps, critical alarms)	Very High	Medium	High	Very High	Medium	High
Daily / Long-Term Health Monitoring (e.g., wearables, remote patient monitoring)	Medium	Very High	Medium	High	High	Medium
Intra-Hospital Device Communication (e.g., gateways, imaging systems, EHR integration)	Medium	Low	Very High	High	Low	Very High

7. FUTURE PROSPECTS

7.1 Unique identification of nodes and Tri Token Secret Key set for authentication

Each IoMT node must be individually analyzed to overcome the limitations of traditional models. The node's information should be processed to assign a Digital Unique Identity, ensuring precise identification in future transmissions. Additionally, a Tri Token Secret Key Set must be generated to enable authentication and access control. This approach enhances security by verifying nodes before permitting data exchanges. Implementing these measures reduces unauthorized access and strengthens the overall integrity of the IoMT system. Proper identification and authentication establish a strong foundation for secure communication, ensuring that only authorized nodes participate in network activities.

7.2 Lightweight cryptographic algorithms for encryption and decryption

Besides authentication, integrating lightweight cryptographic algorithms is essential for ensuring secure medical data transmission. Algorithms such as Advanced Encryption Standard with a 128-bit key (AES-128), Elliptic Curve Cryptography (ECC), and PRESENT cipher offer effective encryption and decryption while maintaining low computational complexity. These cryptographic techniques help protect sensitive patient data from unauthorized access without overburdening IoMT devices. Since IoMT devices have limited resources, lightweight encryption models ensure secure communication while optimizing performance. Implementing efficient cryptographic methods guarantees data confidentiality and integrity, making medical data transmission more secure and reliable in healthcare applications.

7.3 Detection of security threats and comparative analysis

Monitoring node behavior and analyzing traffic patterns is necessary to detect security threats within the IoMT network. Lightweight cryptographic techniques such as Speck, Simon, and High-speed Lightweight Cryptography (HIGHT) can further enhance security by providing fast and efficient encryption. These algorithms ensure data protection while minimizing power consumption and processing delays. Additionally, a comparative analysis between the proposed model and traditional approaches must be conducted to evaluate security improvements. The results will demonstrate that the proposed model offers enhanced protection against cyber threats. By integrating authentication, encryption, and attack detection, the model ensures a secure and efficient IoMT network.

To overcome the limitations of the traditional models that are analyzed in this research, it is necessary to analyze each IoMT node, process the node information, and allocate a Digital Unique Identity for accurate identification of nodes in future transmissions and to generate a Tri Token Secret Key Set for performing node authentication and access control for initiating secure data transmission in the IoT network. It is also required to design an LWC model to perform encryption and decryption for securing the medical data, and then to analyze the node behaviour and patterns, and to perform attack detection in the IoMT network to improve the QoS levels in the network. Finally, it is required to perform a comparative analysis of the proposed model with the traditional models and to demonstrate that the proposed model's security levels are high.

8. CONCLUSIONS

Recent studies on the use of cryptography for the IoT looked at design, mixture-column, substitution-box, and hazards. It is observed that most constrained IoT devices have low resources; using a lightweight method is a great security solution for them. The data presented in this research provides sufficient information to select an algorithm that is suitable for the selected applications and to design an enhanced version of the cryptography algorithms for enhancing the QoS levels. All algorithms rely on hardware in some way; even devices with severe constraints will work fine with them. Results of all the algorithms mentioned may differ depending on the adjustments in hardware/software and the application; however, just because an algorithm is software-dependent does not imply it will not function effectively on hardware. No algorithm has proven results in terms of speed, cycles, or throughput. For IoT uses, only a few of the algorithms are competent and safe. Lots of algorithms are resilient to various types of attacks, such as the Man-in-the-Middle assault, Differential attacks, key-IV attacks, and many more. This research addressed solutions for lightweight IoT security. In conclusion, this research provides useful information for selecting an appropriate algorithm and software/hardware combination for a given task. Researchers in the future will be able to analyze many lightweight algorithms on diverse hardware and software platforms and then evaluate them according to metrics like clock cycles, speed, memory, frequency, latency, etc., to find out how well they function and how to improve them, and then design efficient LWC solutions for providing security to IoMT.

REFERENCES

[1] Yanambaka, V.P., Mohanty, S.P., Kougianos, E., Puthal, D. (2019). PMsec: Physical unclonable function-based robust and lightweight authentication in the Internet of Medical Things. IEEE Transactions on Consumer Electronics, 65(3): 388-397. https://doi.org/10.1109/TCE.2019.2926192

[2] Masud, M., Gaba, G.S., Choudhary, K., Hossain, M.S., Alhamid, M.F., Muhammad, G. (2022). Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. IEEE Internet of Things Journal, 9(4): 2649-2656. https://doi.org/10.1109/JIOT.2021.3080461

[3] Shihab, S., AlTawy, R. (2023). Lightweight authentication scheme for healthcare with robustness to desynchronization attacks. IEEE Internet of Things Journal, 10(20): 18140-18153. https://doi.org/10.1109/JIOT.2023.3279035

[4] Wang, S.B., Zhou, X., Wen, K., Weng, B.S., Zeng, P. (2023). Security analysis of a user authentication scheme for IoT-based healthcare. IEEE Internet of Things Journal, 10(7): 6527-6530. https://doi.org/10.1109/JIOT.2022.3228921

[5] Lara, E., Aguilar, L., García, J.A. (2021). Lightweight authentication protocol using self-certified public keys for wireless body area networks in health-care applications. IEEE Access, 9: 79196-79213. https://doi.org/10.1109/ACCESS.2021.3084135

[6] Zhou, X., Wang, S.B., Wen, K., Hu, B., Tan, X., Xie, Q. (2024). Security-enhanced lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. IEEE Internet of Things Journal, 11(6): 9599-9609. https://doi.org/10.1109/JIOT.2023.3323614

[7] Yang, X., Yi, X., Khalil, I., Luo, J.W., Bertino, E., Nepal, S. (2022). Secure and lightweight authentication for mobile-edge computing-enabled WBANs. IEEE Internet of Things Journal, 9(14): 12563-12572. https://doi.org/10.1109/JIOT.2021.3138989

[8] Adil, M., Khan, M.K., Jadoon, M.M., Attique, M., Song, H., Farouk, A. (2023). An AI-enabled hybrid lightweight authentication scheme for intelligent IoMT based cyber-physical systems. IEEE Transactions on Network Science and Engineering, 10(5): 2719-2730. https://doi.org/10.1109/TNSE.2022.3159526

[9] Ning, L., Ali, Y., Ke, H., Nazir, S., Zhao, H.L. (2020). A hybrid MCDM approach of selecting lightweight cryptographic cipher based on ISO and NIST lightweight cryptography security requirements for Internet of Health Things. IEEE Access, 8: 220165-220187. https://doi.org/10.1109/ACCESS.2020.3041327

[10] Yavuz, A.A., Ozmen, M.O. (2022). Ultra lightweight multiple-time digital signature for the Internet of Things devices. IEEE Transactions on Services Computing, 15(1): 215-227. https://doi.org/10.1109/TSC.2019.2928303

[11] Guo, Y., Liu, W.F., Chen, W., Yan, Q.W., Lu, Y.C. (2024). ECLBC: A lightweight block cipher with error detection and correction mechanisms. IEEE Internet of Things Journal, 11(12): 21727-21740. https://doi.org/10.1109/JIOT.2024.3376527

[12] Zhang, J.H., Dong, C.H. (2023). Secure and lightweight data aggregation scheme for anonymous multi-receivers in WBAN. IEEE Transactions on Network Science and Engineering, 10(1): 81-91. https://doi.org/10.1109/TNSE.2022.3205044

[13] Bao, Y.Y., Qiu, W.D., Tang, P., Cheng, X.C. (2022). Efficient, revocable, and privacy-preserving fine-grained data sharing with keyword search for the cloud-assisted medical IoT system. IEEE Journal of Biomedical and Health Informatics, 26(5): 2041-2051. https://doi.org/10.1109/JBHI.2021.3100871

[14] Sun, J.F, Xiong, H., Liu, X.M., Zhang, Y.H., Nie, X.Y., Deng, R.H. (2020). Lightweight and privacy-aware fine-grained access control for IoT-oriented smart health. IEEE Internet of Things Journal, 7(7): 6566-6575. https://doi.org/10.1109/JIOT.2020.2974257

[15] Yang, Y., Liu, X.M., Deng, R.H. (2018). Lightweight

break-glass access control system for healthcare Internet-of-Things. IEEE Transactions on Industrial Informatics, 14(8): 3610-3617. https://doi.org/10.1109/TII.2017.2751640

[16] Li, C.Y., Dong, M.X., Xin, X.J., Li, J., Chen, X.B., Ota, K. (2023). Efficient privacy preserving in IoMT with blockchain and lightweight secret sharing. IEEE Internet of Things Journal, 10(24): 22051-22064. https://doi.org/10.1109/JIOT.2023.3296595

[17] Fugkeaw, S., Wirz, L., Hak, L. (2023). Secure and lightweight blockchain-enabled access control for fog-assisted IoT cloud based electronic medical records sharing. IEEE Access, 11: 62998-63012. https://doi.org/10.1109/ACCESS.2023.3288332

[18] Chen, C.M., Chen, Z.T., Das, A.K., Chaudhry, S.A. (2024). A security-enhanced and ultralightweight communication protocol for Internet of Medical Things. IEEE Internet of Things Journal, 11(6): 10168-10182. https://doi.org/10.1109/JIOT.2023.3327322

[19] Rana, A., Prajapat, S., Kumar, P., Gautam, D., Chen, C.M. (2024). Designing a security framework based on hybrid communication in Internet of Nano Things. IEEE Internet of Things Journal, 11(4): 7265-7284. https://doi.org/10.1109/JIOT.2023.3315712

[20] Ahamad, S.S., Al-Shehri, M., Keshta, I. (2022). A secure and resilient scheme for telecare medical information systems with threat modeling and formal verification. IEEE Access, 10: 120227-120244. https://doi.org/10.1109/ACCESS.2022.3217230

[21] Bao, Y.Y., Qiu, W.D., Cheng, X.C. (2022). Secure and lightweight fine-grained searchable data sharing for IoT-oriented and cloud-assisted smart healthcare system. IEEE Internet of Things Journal, 9(4): 2513-2526. https://doi.org/10.1109/JIOT.2021.3063846

[22] Jiang, Z.L., Liu, W., Ma, R.J., Shirazi, S.H., Xie, Y. (2021). Lightweight healthcare wireless body area network scheme with amplified security. IEEE Access, 9: 125739-125752. https://doi.org/10.1109/ACCESS.2021.3111292

[23] Liu, D.X., Ni, J.B., Huang, C., Lin, X.D., Shen, X.S. (2020). Secure and efficient distributed network provenance for IoT: A blockchain-based approach. IEEE Internet of Things Journal, 7(8): 7564-7574. https://doi.org/10.1109/JIOT.2020.2988481

[24] Tseng, L., Wong, L., Otoum, S., Aloqaily, M., Othman, J.B. (2020). Blockchain for managing heterogeneous Internet of Things: A perspective architecture. IEEE Network, 34(1): 16-23. https://doi.org/10.1109/MNET.001.1900103

[25] Ridhawi, I.A., Kotb, Y., Aloqaily, M., Jararweh, Y., Baker, T. (2020). A profitable and energy-efficient cooperative fog solution for IoT services. IEEE Transactions on Industrial Informatics, 16(5): 3578-3586. https://doi.org/10.1109/TII.2019.2922699

[26] Lakshman Narayana, V., Rao, G.S., Gopi, A.P., Lakshmi Patibandla, R.S.M. (2022). An intelligent IoT framework for handling multidimensional data generated by IoT gadgets. In Machine Learning for Critical Internet of Medical Things, pp. 199-228. https://doi.org/10.1007/978-3-030-80928-7_9

[27] Al-Turjman, F., Abujubbeh, M., Malekloo, A., Mostarda, L. (2020). UAVs assessment in software-defined IoT networks: An overview. Computer Communications, 150: 519-536. https://doi.org/10.1016/j.comcom.2019.12.004

[28] Rao, B.T., Patibandla, R.S.M.L., Narayana, V.L., Gopi, A.P. (2021). Medical data supervised learning ontologies for accurate data analysis. In Semantic Web for Effective Healthcare Systems, pp. 249-267. https://doi.org/10.1002/9781119764175.ch11

[29] Narayana, V.L., Gopi, A.P., Radhika, P., Sandeep, K.S. (2020). Secure data uploading and accessing sensitive data using time level locked encryption to provide an efficient cloud framework. Ingénierie des Systèmes d'Information, 25(4): 515-519. https://doi.org/10.18280/isi.250415

[30] Bharathi, C.R., Narayana, V.L., Ramesh, L.V. (2020). Secure data communication using Internet of Things. International Journal of Scientific & Technology Research, 9(4): 3516-3520. https://www.ijstr.org/final-print/apr2020/Secure-Data-Communication-Using-Internet-Of-Things.pdf.