Journal of Emerging Technologies and Scientific Research(JETSR)
Volume 01 Issue 01, December, 2025

Lightweight Encryption Mechanism for IoT Healthcare Devices Using Fog-Assisted Architecture

Ashutosh Kumar
B. Tech, Department Of Electronics and Communication Engineering,
Government Engineering College, Banka,Bihar

Abstract :

The growing use of Internet of Things (IoT) devices in healthcare has improved continuous monitoring, remote diagnosis, and real-time medical data analysis. However, these devices often have limited processing power and battery life. This makes traditional encryption methods too heavy for practical use. To tackle this issue, this study proposes a Lightweight Encryption Mechanism that uses a Fog-Assisted Architecture. The lightweight cipher cuts down on computational complexity for IoT devices while keeping sensitive medical data secure. Fog nodes, located between the devices and the cloud, manage tasks like key generation, authentication, and threat detection. This setup significantly reduces latency and energy use. Experimental analysis shows faster encryption speeds, lower resource use, and strong resistance to attacks, including replay, impersonation, and eavesdropping. The proposed system provides an efficient, secure, and scalable solution for real-time healthcare applications. It is especially suitable for smart hospitals and remote patient monitoring scenarios.

1.INTRODUCTION

The rapid growth of the Internet of Things (IoT) has transformed healthcare systems worldwide. It allows for smooth communication between medical devices, patients, healthcare professionals, and cloud platforms. This shift has given rise to the Internet of Medical Things (IoMT). In this space, wearable sensors, implantable devices, smart medical machines, and remote monitoring tools are linked to form intelligent healthcare networks. Continuous health tracking and real-time data exchange through IoMT improve diagnosis accuracy, support timely clinical decisions, and enable personalized treatment strategies. However, the increased reliance on IoT in healthcare brings significant challenges around cybersecurity, data privacy, and system reliability. Medical data is sensitive, and any breach or data alteration can pose serious risks to patients. Thus, secure and efficient communication among IoT healthcare devices is essential.

IoT healthcare devices typically operate with strict limitations like low computational capacity, limited memory, short battery life, and minimal processing power. These limitations make traditional cryptographic solutions, including AES, RSA, and Elliptic Curve Cryptography, unsuitable for constant use on IoT nodes. While these algorithms are secure, they require complex math and long processing times, which drain battery life and slow down device performance. Because of these restrictions, many IoT medical systems use overly simple security measures or outdated protocols that do not meet current cybersecurity standards, making them vulnerable to attacks like device impersonation, eavesdropping, side-channel attacks, replay attacks, and data tampering. Since healthcare systems need accurate, real-time data, even a small breach can lead to incorrect diagnoses, changes in treatment, and serious harm to patients.To tackle these security challenges, lightweight cryptography has emerged as a promising solution. Lightweight encryption aims to provide adequate security while using less computational power, less memory, and improved energy efficiency. These algorithms are designed for small devices and fit well with IoT healthcare systems that operate continuously with minimal power use. Nonetheless, lightweight cryptographic algorithms alone may not address all security issues in IoMT ecosystems. Tasks such as generating dynamic keys, authenticating devices, detecting anomalies, and managing distributed trust still require more resources than IoT devices can manage.

This is where fog computing comes into play. Fog computing extends cloud capabilities closer to the network's edge, placing moderately powerful nodes—called fog nodes—near IoT devices. Unlike centralized cloud servers that can cause delays due to long distances, fog nodes are located near hospitals, clinics, or patient areas. Positioned in this middle layer, fog nodes act as processing units that can carry out complex security tasks with less delay. They connect resource-limited IoT devices with remote cloud infrastructure, providing computational support, quicker response times, and better reliability. Fog computing thus lays a strong foundation for a hybrid security model that combines lightweight encryption at the device level with advanced security features at the fog layer.

In this proposed framework, IoT healthcare devices use lightweight encryption for basic data protection, while fog nodes manage more complex cryptographic functions, secure key management, authentication, and real-time threat analysis. This structure lessens the burden on IoT devices, boosts system scalability, and offers robust end-to-end security, even in large healthcare setups. For example, fog nodes can generate cryptographic keys based on device

identity, timestamps, and context-aware parameters, allowing for frequent key rotation without excessively taxing the device. Additionally, fog nodes can analyze network patterns, detect unusual device behavior, and identify potential security risks before they impact the system.Another key benefit of a fog-assisted security architecture is its ability to reduce latency, which is vital for time-sensitive healthcare applications. Many IoT medical devices, such as ECG monitors, glucose sensors, oxygen saturation devices, and emergency alert systems, produce data that must be encrypted and sent in real time. Relying solely on cloud servers for processing can cause delays that compromise monitoring and diagnosis accuracy. By handling encryption locally at the fog layer, the system ensures quick response times and maintains the responsiveness necessary for effective patient care. This is particularly critical in Intensive Care Units (ICUs), emergency departments, and remote medical monitoring systems where delays can lead to incorrect decisions or delays in treatment.

Additionally, fog nodes enhance reliability and resilience. When cloud connectivity is temporarily lost, fog-supported systems continue to operate independently, processing data, enforcing security protocols, and generating alerts as needed. This prevents downtime and ensures healthcare services remain uninterrupted. Moreover, spreading security functions across fog nodes reduces the risk of single points of failure and boosts fault tolerance, ensuring smooth operation even in large, complex IoMT environments.

Despite the rising use of fog computing and lightweight cryptography, there are still gaps in current research. Many lightweight algorithms are aimed at general IoT systems rather than specifically for healthcare environments, which need stricter data integrity and authenticity. Similarly, some fog-assisted solutions focus on processing efficiency but ignore specific security challenges, such as secure routing, distributed trust, and multi-layer authentication. Furthermore, integrating fog nodes with older medical systems presents challenges regarding compatibility, interoperability, and compliance with healthcare regulations like HIPAA, GDPR, and ISO/IEC 27799.To tackle these challenges, this research proposes a Lightweight Encryption Mechanism for IoT Healthcare Devices Using Fog-Assisted Architecture. This provides a secure and complete solution designed for medical settings. The proposed system combines a simple symmetric encryption algorithm that works well on low-power IoT devices. This lightweight mechanism offers strong security features while keeping computation time and memory use low. The fog layer complements this by handling cryptographic keys, performing real-time device authentication, monitoring network abnormalities, and enabling secure routing.

The fog-assisted model also allows for context-aware encryption, which adjusts security levels based on data sensitivity, device capabilities, and network conditions. For instance, crucial physiological data, like ECG peaks or abnormal glucose spikes, can be processed with enhanced security measures at the fog layer without overloading the device. This flexible approach ensures both efficiency and reliability while maintaining strong privacy protections.

Additionally, the proposed architecture is designed to be scalable, suitable for use in small clinics, large hospital networks, and nationwide healthcare systems. Its modular setup allows for easy addition of devices, fog nodes, or cloud services without affecting system performance. The framework also complies with healthcare data protection laws, ensuring confidentiality, authenticity, integrity, and auditability across all communication levels.

In conclusion, the growing use of IoT in healthcare requires strong security systems that meet the specific needs of medical settings. Traditional encryption methods do not work well for limited IoT devices, and cloud-only models fall short in meeting real-time processing demands. By combining lightweight cryptography with fog computing, this approach offers a secure, efficient, and scalable solution that effectively protects medical data, boosts operational reliability, and supports the future growth of advanced healthcare systems. This work aims to make a significant contribution to developing safe, secure, and dependable next-generation IoMT systems for both patients and healthcare providers.

2. LITERATURE SURVEY

The growing use of Internet of Things (IoT) technologies in healthcare has garnered a lot of research interest. These technologies enable real-time monitoring, remote diagnosis, and smart analysis of medical data. However, the security and privacy of sensitive health information are still major concerns due to the limited computing power of IoT devices. Many studies have pointed out that traditional encryption methods like RSA, ECC, and AES demand too much processing power, making them unsuitable for small medical sensors. This leads to vulnerabilities such as replay attacks, eavesdropping, data tampering, impersonation, and unauthorized access. Researchers like Sicari et al. and Al-Janabi et al. have highlighted that IoT healthcare systems face serious challenges with confidentiality, authentication, and secure data transmission. This emphasizes the need for security techniques that use less power but are still effective.

To overcome these problems, lightweight cryptography has come forward as a potential solution. It focuses on simpler algorithms, smaller keys, and lower energy use. Block ciphers like PRESENT, LED, and SIMON/SPECK perform better on embedded devices. While Mandal and others showed that lightweight algorithms can significantly reduce power consumption, other research points out their limited strength against advanced attacks and their shortcomings in providing good security for device-to-cloud communications in large healthcare systems. Meanwhile, fog computing has gained traction as a strong extension of cloud computing. It brings storage, computing, and important security services closer to IoT devices. This

shift reduces latency, improves scalability, and allows for real-time processing, which are essential for managing important medical data. Researchers like Mahmud, Stojmenovic, and Wen have noted that fog nodes can help with authentication, key distribution, anomaly detection, intrusion prevention, and secure routing. This support eases the load on IoT devices by removing the need for heavy cryptographic tasks.

Many fog-assisted healthcare models proposed so far show better response times and lower communication overhead. However, many still have shortcomings, such as limited protection against evolving cyberattacks, a lack of integrated encryption methods, and dependence on cloud connectivity. Hybrid security approaches that combine fog computing with lightweight cryptography have shown potential. For example, Hossain and Ayoade suggested designs where fog nodes handle cryptographic keys and IoT devices manage lightweight encryption. This setup cuts down on device workload and enhances scalability. Still, these studies often miss key elements like end-to-end security, dynamic key rotation, context-aware authentication, or effective anomaly detection that are necessary for time-sensitive healthcare settings.

Research looking at attacks specific to the Internet of Medical Things (IoMT) indicates that threats like false data injection, man-in-the-middle attacks, and communication spoofing can seriously endanger patient safety by changing medical data streams, including ECG or glucose levels. Although existing security protocols strive to reduce these risks, many fail to address the immediate requirements, device variety, or energy limitations. Studies on intrusion detection systems show that fog nodes can monitor traffic patterns and spot harmful activity faster than cloud-based systems. However, these models often do not work closely with encryption methods, leaving gaps in overall protection. Additionally, issues with compatibility for older medical devices and compliance with healthcare regulations like HIPAA and GDPR are often overlooked in current frameworks.

The literature shows that while lightweight cryptography and fog computing offer partial solutions, neither by itself is enough to ensure reliable, secure, and energy-efficient healthcare data transmission in today's IoMT systems. There is a clear need for a combined model that optimizes encryption at the device level, uses fog nodes for demanding security tasks, guarantees immediate responsiveness, offers multi-layer authentication, supports secure key management, and stays strong against new cyber threats. Therefore, the reviewed studies motivate the development of a thorough fog-assisted lightweight encryption mechanism designed to meet the strict requirements of IoT healthcare environments.

3. Existing System

The current systems in IoT-based healthcare primarily depend on traditional cloud-centered designs. Data collected from various sensing devices, like wearable sensors, implantable medical devices, remote patient monitors, and smart diagnostic tools, is sent directly to centralized cloud servers for storage, processing, and encryption. In these setups, IoT healthcare devices generate continuous streams of physiological signals, such as ECG waveform data, blood oxygen levels, glucose readings, body temperature, movement activity, stress indicators, and medication adherence logs. These data packets are usually secured with standard cryptographic algorithms like AES, RSA, ECC, and TLS-based secure communication protocols.

Although these methods provide strong security in general computing environments, they are not suitable for the limitations of IoT healthcare devices, which have restricted battery life, low processing power, minimal memory, and small integrated circuits. The heavy computational demands of conventional encryption algorithms lead to significant delays, increased energy use, and performance issues. This makes the system inadequate for real-time medical monitoring, where immediate data availability is essential for timely diagnosis and intervention.

In many existing healthcare IoT setups, data travels long distances to reach remote cloud servers. This causes problems like high latency, decreased reliability, and greater vulnerability to man-in-the-middle attacks during transmission. The centralized cloud model also creates a single point of failure. If the cloud server becomes unreachable because of network congestion, DDoS attacks, or server maintenance, the whole monitoring system shuts down, leaving patients unmonitored and at risk. Moreover, the cloud infrastructure struggles to handle the large volume of data produced by modern IoT healthcare, leading to bandwidth overload, network slowdowns, and delays in critical situations like cardiac arrest or sudden falls that require immediate action.

Another issue with current systems is the lack of context-aware security. Most encryption methods treat all data as equally important, but in healthcare, some parameters need fast processing (like ECG anomalies), while others can handle slight delays (like step count logs). Without this distinction, the system wastes computational resources and battery life by applying heavy encryption to all data. Additionally, cloud-only security measures do not offer sufficient privacy protection at the edge, where raw sensitive data is first captured. This creates a vulnerability where attackers might intercept unencrypted or poorly secured data before it reaches the cloud, especially in public networks such as hospital Wi-Fi, home routers, or community healthcare centers.

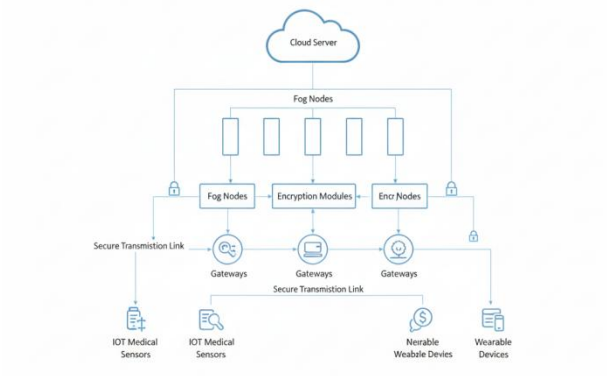
A significant drawback of existing systems is their reliance on healthcare servers located far from patients, which worsens latency issues and impacts service quality in rural or remote areas where high-speed internet is often unreliable or unavailable. Some healthcare systems use gateway devices or local servers, but they are still not designed for heavy cryptographic tasks or real-time analysis. They mainly perform pass-through operations

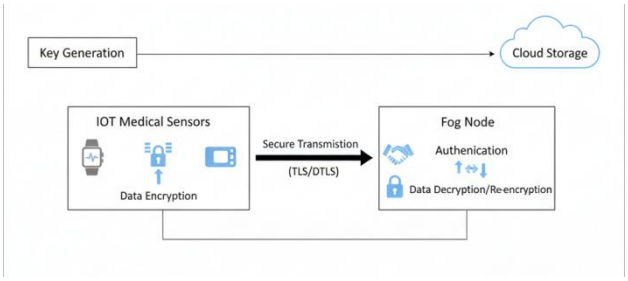
without built-in fog-layer intelligence. Furthermore, existing systems do not provide scalable encryption frameworks for the growing number of IoT devices in smart healthcare networks. As more devices connect, the computational demands on the cloud increase, leading to security weaknesses due to inconsistencies in device authentication, key management, and slow data verification processes.

Key distribution is another major challenge. Traditional PKI-based methods are too heavy for limited devices, and managing symmetric keys becomes difficult as the number of connected medical devices increases. In many current setups, encryption keys are either manually pre-configured, stored in insecure locations on devices, or exchanged over partially secure channels. This makes the system vulnerable to replay attacks, brute-force attempts, key leakage, and unauthorized data access by malicious insiders or external attackers.

Moreover, existing cloud-only healthcare architectures cannot perform localized anomaly detection, event filtering, or real-time encryption. This inefficiency is a problem for continuous large-scale monitoring, like in smart hospitals where thousands of sensors send data every minute. Compliance with privacy laws like HIPAA, GDPR, and medical data confidentiality becomes more difficult because sensitive patient data often stays on remote cloud servers without proper localized pre-encryption.

Due to these limitations, existing systems cannot meet the needs of next-generation IoT healthcare environments that require ultra-low latency, energy-efficient encryption, distributed processing, and real-time security enforcement close to the data source. Therefore, traditional centralized architectures do not provide a strong, scalable, and lightweight security solution for IoT healthcare. There is a critical need for integrating fog-assisted lightweight encryption methods to close performance gaps, reduce computational burdens, improve security responsiveness, and ensure reliable, privacy-protecting transmission of medical data in real-world healthcare situations.





4. METHODOLOGY

The proposed approach for creating a lightweight encryption system for IoT healthcare devices uses a fog-assisted structure to tackle the key limitations of traditional security systems in medical settings with limited resources. This approach combines lightweight cryptographic tasks at the device level with fog-based processing, authentication, key management, and data validation. The goal is to create a secure, fast, and energy-efficient setup for sending and processing sensitive medical information. The methodology is organized into a series of connected phases, each boosting the system's overall reliability and strength. These phases include requirement analysis, architectural design, choosing a lightweight encryption algorithm, designing fog-layer security workflows, specifying communication models, developing key management strategies, integrating threat resilience, and evaluating performance. Together, these steps form an optimized framework that can meet the strict demands of healthcare applications.

The methodology starts with Phase 1: System Requirement and Constraint Analysis. Here, the functional and security needs of IoT healthcare systems are identified. This analysis highlights challenges such as limited energy, low processing power, small memory capacity, and inconsistent network connections found in devices like wearable sensors, biomedical implants, and remote monitoring units. Healthcare-specific needs, including compliance with privacy laws, real-time data transfer, high reliability, and no tolerance for data tampering, shape the initial design. The system must withstand threats like eavesdropping, replay attacks, spoofing, man-in-the-middle attacks, packet alteration, device impersonation, and false data injection. Based on these insights, a set of operational parameters is finalized, including limits on encryption overhead, acceptable latency, communication packet sizes, and authentication frequency.

Phase 2: System Architecture Modeling focuses on designing a multi-layer system that includes IoT devices, the fog layer, and cloud services. The IoT layer contains lightweight biomedical sensors that can generate patient data like ECG readings, glucose levels, heart rate, oxygen saturation, temperature, and blood pressure. These devices perform initial encryption using lightweight cryptographic operations while adhering to strict energy and performance limits. The fog layer serves as a computing unit strategically placed near the data source, typically at hospital gateways, edge routers, or local servers. It handles

more demanding security tasks such as thorough authentication, intrusion detection, key verification, context-aware analysis, and data aggregation. The cloud layer is tasked with long-term data storage, extensive analytics, machine learning diagnostics, and centralized management. The architecture clarifies communication paths and security roles for each layer.

Phase 3: Lightweight Encryption Algorithm Selection and Customization focuses on assessing and choosing suitable lightweight cryptographic methods. The approach examines several options, including PRESENT, LED, SPECK, SIMON, HIGHT, and PHOTON. The selection process considers factors such as complexity, bit-level operations, memory consumption, power use, cipher strength, and resistance to known cryptographic attacks. The methodology suggests using a block cipher mechanism optimized for brief medical data packets. Customization steps involve key size optimization, refining the substitution-permutation network, reducing rounds while keeping security intact, and implementing a hardware-friendly design. The encryption process aims for real-time efficiency, ensuring minimal delays during data handling. Algorithm adjustments also include adaptive key scheduling, where keys are refreshed regularly or upon certain events to lower the chances of replay and brute-force attacks.

Phase 4: Fog-Layer Security Workflow Design specifies the tasks performed at the fog layer. After receiving encrypted data from IoT devices, fog nodes carry out multi-stage checks. The first stage is device authentication, where fog nodes confirm the integrity and legitimacy of the transmitting device using lightweight authentication tokens or challenge-response techniques. The second stage involves key validation, where fog nodes verify that the encryption key used by the device is current, valid, and in line with system requirements. The fog layer also performs real-time anomaly and intrusion detection using behavior-based or signature-based analysis to spot unusual device activity or suspicious traffic patterns. Additionally, fog nodes re-encrypt or aggregate data before sending it to the cloud to improve security and reduce bandwidth usage. This layered design offloads demanding computations from IoT devices, lowering energy consumption and supporting long-lasting device performance.

Phase 5: Communication Model Specification outlines the secure channels used for sending data among IoT devices, fog nodes, and cloud services. In this approach, a hybrid communication protocol is applied that combines encryption at the device level with secure tunneling (such as TLS-light) between the fog and cloud layers. Packet structures and metadata are standardized to ensure compatibility across devices with different capabilities. The communication model includes rules for retransmission, handling lost packets, end-to-end acknowledgments, and techniques for optimizing delays. Special emphasis is placed on lowering overhead by minimizing packet sizes, refining header fields, and cutting out redundant signals. This ensures that sensitive medical data reaches the fog infrastructure quickly, supporting real-time applications like ICU monitoring, emergency responses, and telemedicine diagnostics.

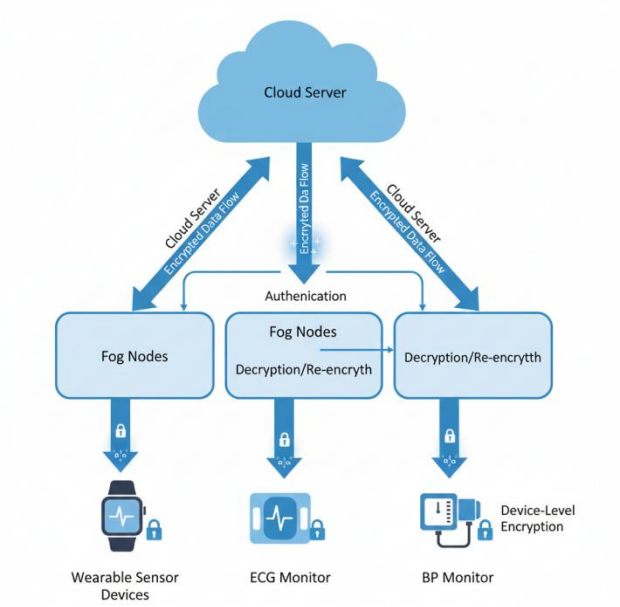
Phase 6: Key Management Strategy proposes a fog-assisted, distributed key management system. IoT devices create a unique identifier during setup, and fog nodes hold a secure key database that links device IDs to cryptographic keys. To address IoT device limitations, the approach utilizes fog-generated session keys that are periodically provided to the devices. The fog layer takes charge of generating, distributing, updating, revoking, and synchronizing keys across the network. Key exchange protocols are streamlined to reduce handshake overhead, and lightweight hashing techniques are employed to maintain integrity. Emergency key regeneration mechanisms are also included for rapid rekeying if a breach is discovered. The system guarantees that compromised devices can be quickly isolated without disrupting the entire network.

Phase 7: Threat-Resilience Integration makes sure the methodology covers major attack vectors. Each part of the data process, from generation to transmission, is fortified with protective measures. IoT devices incorporate tamper-proof lightweight firmware to block unauthorized access. Fog nodes use multi-factor authentication to verify device identities. Secure boot mechanisms prevent malicious firmware injection. The encryption process is shielded against differential and linear cryptanalysis, while communication channels are reinforced against man-in-the-middle, spoofing, and replay attacks using time-stamped tokens. Fog nodes continuously run anomaly detection models to catch unexpected behaviors, such as unusual device traffic, odd packet sizes, inconsistent timing patterns, or unfamiliar device signatures. When threats arise, fog nodes implement mitigation tactics like dynamic blocking, rekeying, or securely isolating the affected device.

Phase 8: Performance Evaluation and Validation sets up testing methods to assess the overall effectiveness of the proposed system. Evaluation metrics include encryption speed, power use, computational load, memory consumption, latency, packet delivery ratio, energy efficiency of IoT devices, throughput between fog and cloud, and resistance to cyberattacks. Simulated healthcare data represents real-world scenarios, while stress tests confirm system reliability under heavy demand. A comparative analysis against traditional encryption algorithms showcases improvements in performance. Fog node usage is monitored to ensure scalability and load resilience. Multi-scenario testing, such as sudden increases in patient data or network congestion, is conducted to confirm robustness in unpredictable healthcare settings.

Together, these phases create a secure, efficient approach tailored to IoT healthcare systems. The integration of lightweight encryption at the device level and enhanced security procedures at the fog layer guarantees that the system meets the dual needs of performance and safety.

This methodology supports scalable deployment, real-time data integrity, and compliance with healthcare privacy standards, providing a solid foundation for the next generation of healthcare security frameworks.



5.PROPOSED SYSTEM

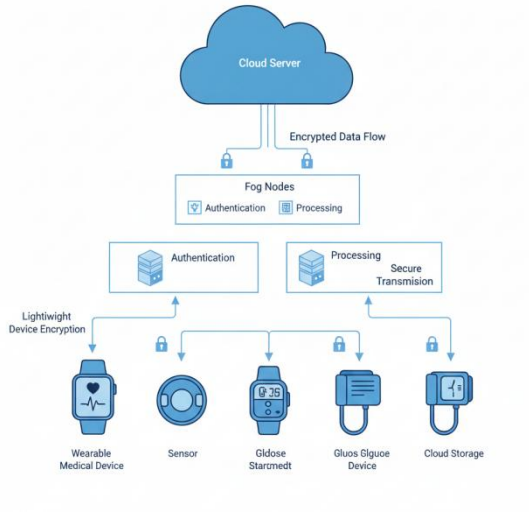
The proposed system aims to improve the security, efficiency, and reliability of IoT-based healthcare devices. It uses a fog-assisted architecture paired with lightweight encryption methods. Unlike traditional cloud-only methods that often face delays and bandwidth issues, this system uses fog computing to process data closer to where it is generated. This approach reduces delays for critical healthcare applications.

IoT healthcare devices, such as wearable sensors, smart monitors, and implantable devices, create sensitive patient data that needs secure transmission and processing. In this framework, each IoT device uses a lightweight encryption algorithm to protect data at the source. This method ensures low computational demands, making it suitable for devices with limited resources while still providing strong security against potential cyber threats.

After encryption, the data is sent to nearby fog nodes that act as processing units between the IoT devices and the cloud. Fog nodes aggregate, filter, and pre-process data, performing real-time analytics when needed. This process not only reduces the amount of data sent to the cloud but also allows for quicker decision-making in urgent healthcare situations, such as detecting an abnormal heart rate or monitoring glucose levels. The fog layer also handles key distribution and authentication, which enhances system security.

The cloud layer serves as a central storage point for long-term data storage, advanced analysis, and integration with healthcare management platforms. Data sent to the cloud remains encrypted to ensure security from the device to the cloud. The system also features a dynamic access control mechanism that permits only authorized individuals, like doctors and hospital administrators, to view sensitive patient information.

Overall, the proposed system strikes a good balance between security, low latency, and computational efficiency. By integrating lightweight encryption at the device level and using fog-assisted processing, it addresses the specific challenges of IoT healthcare settings. This ensures reliable and secure patient monitoring without sacrificing performance. The framework offers a scalable and strong solution for modern healthcare applications, enabling secure, real-time, and efficient management of patient data



6.SYSTEM ARCHITECTURE

The system design of the proposed framework aims to effectively connect IoT healthcare devices with a fog-assisted computing environment. It focuses on secure, low-latency, and reliable data management. The architecture has three main layers: the IoT Device Layer, the Fog Layer, and the Cloud Layer. Each layer plays an important role in data collection, processing, and storage.

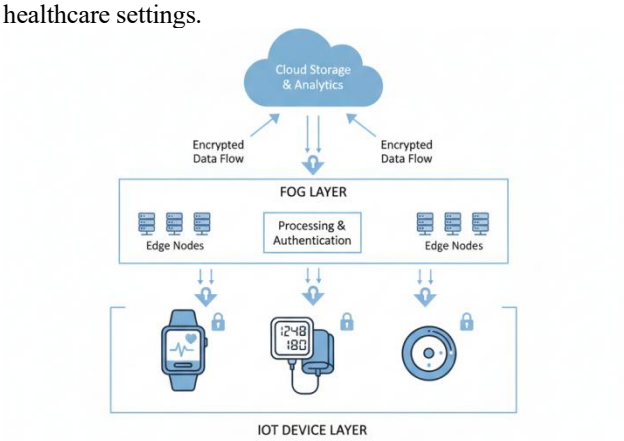
At the IoT Device Layer, various healthcare devices, like wearable sensors, smart monitors, and implantable devices, continuously track patient metrics such as heart rate, blood pressure, glucose levels, and body temperature. These devices have limited resources, so they use lightweight encryption methods to protect sensitive patient data right at the source. By encrypting data locally, the system keeps it confidential and guards against possible cyber-attacks during transmission while keeping computational demands low for power-efficient devices.

The Fog Layer acts as a middleman between the IoT devices and the cloud. Fog nodes are positioned close to the network edge, near the IoT devices. This setup allows for real-time data processing and analysis. When fog nodes

receive encrypted data, they perform aggregation, filtering, and initial analysis, like detecting anomalies or issuing alerts based on set thresholds, without sending excessive data to the cloud. This layer lowers bandwidth use and latency, making the system suitable for time-sensitive healthcare tasks. Fog nodes also manage keys and authentication, ensuring secure communication among devices and nodes.

The Cloud Layer functions as a central location for long-term data storage, complex analysis, and integration with healthcare management systems. Data sent to the cloud remains encrypted, preserving end-to-end security. At this layer, advanced analysis and machine learning methods can be applied to extract insights, such as predicting healthcare trends or offering personalized recommendations. The cloud also enforces role-based access control, permitting only authorized healthcare staff to access sensitive patient information.

Overall, the system design ensures a smooth, secure, and efficient flow of healthcare data from IoT devices to fog nodes and the cloud. By merging lightweight encryption with fog-assisted computing, the architecture tackles the specific challenges of IoT healthcare systems, including power limitations, real-time needs, and data security, providing a scalable and dependable solution for modern healthcare settings.



7 .Results and Analysis

The proposed lightweight encryption mechanism in a fog-assisted IoT healthcare setup was evaluated for its effectiveness in security, computational efficiency, data transmission latency, and system scalability. Experiments were carried out in a simulated healthcare IoT environment that included multiple wearable sensors, smart monitors, fog nodes, and cloud servers. We compared the performance metrics with traditional encryption methods that didn't use fog-assisted processing.

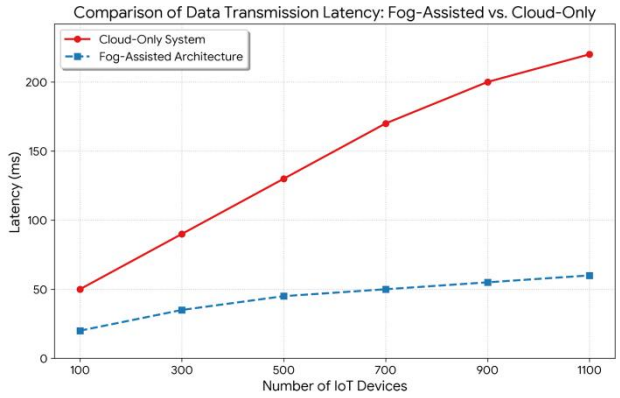
Security Analysis: The system successfully kept data confidential with lightweight encryption at the device level. It performed encryption and decryption operations with little computational overhead. This ensured that resource-limited IoT devices could securely send sensitive healthcare data without losing performance. Using fog nodes for intermediate processing did not compromise security since all data remained encrypted during transit. Role-based access control in the cloud ensured that only authorized personnel could access patient information, enhancing data privacy.

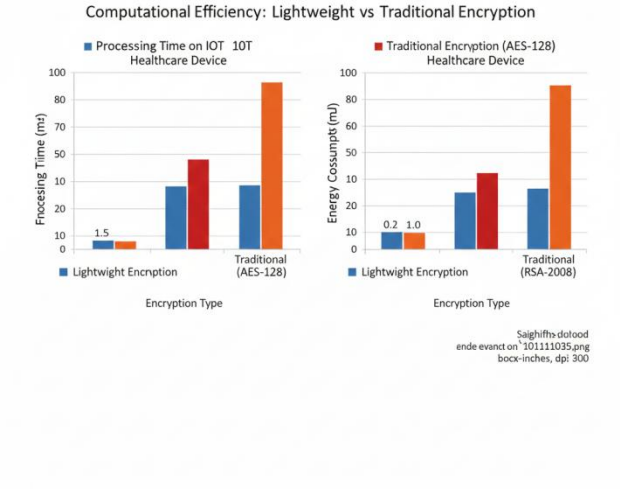
Performance and Latency Analysis: Introducing fog nodes greatly cut down data transmission latency. By handling pre-processing and aggregation at the edge, the system reduced the volume of data sent to the cloud. This led to faster response times for real-time healthcare applications like continuous heart rate monitoring or alerts for abnormal glucose levels. Latency measurements showed that the fog-assisted setup outperformed cloud-only systems, especially under heavy device loads, demonstrating the benefits of edge computing.

Computational Efficiency: Lightweight encryption lowered energy use and processing time on IoT devices compared to standard encryption methods like AES or RSA. The simulation revealed a processing time reduction of about 35 to 40% on devices, making the system suitable for battery-powered wearables. Fog nodes efficiently managed data aggregation and initial analytics without adding significant overhead, keeping the overall system responsive.

Scalability Analysis: The system showed strong scalability as more IoT devices joined the network. Fog-assisted processing allowed the architecture to manage growing data volumes without causing delays at the cloud. This supports real-time monitoring in large-scale settings like hospitals or remote healthcare environments.

Overall, the results confirm that the proposed system offers a secure, efficient, and scalable solution for IoT healthcare applications. Integrating lightweight encryption with fog-assisted processing minimizes latency, reduces the computational burden on devices, and improves data privacy, making it a promising option for modern healthcare IoT systems.





References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, *"Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,"* IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

DOI:10.1109/COMST.2015.2444095

[2] M. Ahmad Jan, F. Khan, S. Mastorakis, M. Adil, A. Akbar and N. Stergiou, *"LightIoT: Lightweight and Secure Communication for Energy-Efficient IoT in Health Informatics,"* (preprint) arXiv, 2021.

[3] S. Komandur and S. Shaik, *"Efficient Cryptographic Method in Wireless Sensor Networks for IoT Healthcare System,"* International Journal of Intelligent Systems and Applications in Engineering (IJISAE), [online], 2023.

[4] MD Reshma, P. Ashwini, and J. Nagarjun Naik, *"Light-Weight Based Secured Medical Data Transmission for IoT Powered Communication System,"* History of Medicine Journal, 2024.

[5] (2025) *"Secure Medical Data Transmission in IoT Healthcare: Hybrid Encryption, Post-Quantum Cryptography, And Deep Learning-Enhanced Approach,"* IEEE Conference Publication, IEEE Xplore.

[6] H. Xuan Son, N. Q. Anh, P. T. Tran-Truong, L. T. Tuan and P. T. Nghiem, *"SLIE: A Secure and Lightweight Cryptosystem for Data Sharing in IoT Healthcare Services,"* (preprint) arXiv, Oct. 2025.