IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Secure and Efficient Key Management Scheme for Internet of Medical Things (IOMT)

[1]Harsha Patil,[2]Dr. Vikas Mahandule, [3]Shivanjali Shinde, [4]Shraddha Phulsundar,[5]Priti Aivale,
[1]Assistant Professor, [2]HOD,[3]Student,[4]Student, [5]Student
[1]Computer Application Department
[1]MAEER'S MIT Arts, Commerce, and Science College Alandi(D) Pune, India

Abstract: In the Internet of Medical Things (IoMT), securing cryptographic keys is critical for ensuring data privacy, integrity, and authentication in healthcare applications. Given the medical data's delicate nature and the constraints of IoMT devices, which often have limited computational and energy resources, designing an efficient key management system poses significant challenges. This paper proposes a novel, lightweight key management scheme tailored to the unique requirements of IoMT networks. Our approach optimizes the striking a balance between resource and security, ensuring robust protection against common threats such as unauthorized access, data tampering, and interception. Through security analysis and performance evaluations, we demonstrate that the proposed scheme offers enhanced protection while minimizing overhead, making it ideal for practical deployment in healthcare environments.

INTRODUCTION

Healthcare is undergoing a revolution thanks to the Internet of Medical Things (IoMT). interconnecting medical devices, sensors, and applications to facilitate real-time monitoring and data exchange. This network of devices improves the quality of healthcare services, enhances patient outcomes, and enables remote diagnosis and treatment. However, the delicate character of medical data poses significant security and privacy challenges, making it essential to ensure robust and secure communication between devices. Key management is pivotal in securing IoMT systems, as it governs the generation, distribution, and storage of cryptographic keys used to protect data. An efficient key management scheme is crucial to safeguard patient information and minimize resource consumption, such as energy and computational power, in resource-constrained IoMT devices. The challenge lies in developing a scheme that can offer resolute security assurances while being scalable, lightweight, and adaptable to the heterogeneous and dynamic environment of IoMT networks that operate securely without compromising performance or patient privacy.

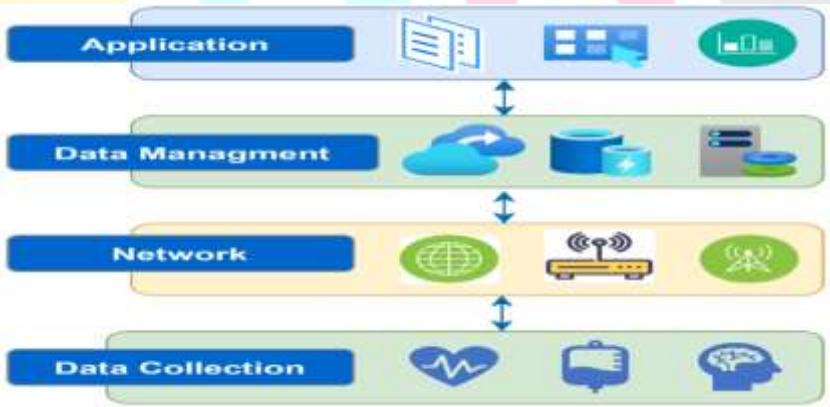

Figure 1. IoMT system architecture

Figure 1. explains that the tasks of data sensing and gathering are carried out by the data collection layer. Through the use of data sensing acquisition procedures, it gathers patient medical parameters from sensors, actuators, edge servers, handheld devices, and medical sensors. The network layer sends the medical data that has been gathered from the data collecting layer to the third tier (the data management layer) over a wired or wireless network. This layer exchanges data and links everything medical in the network.

The interoperability of the heterogeneous entities being used is ensured in the data management layer by utilizing the middleware apps and services required by IoMT applications and users. This layer offers additional crucial functions including processing, storing, and interpreting the medical data that has been gathered. The IoMT system and a user can intelligently communicate thanks to the application layer. This interface makes it simple for the user to connect, manage, and view medical data.

LITERATURE SURVEY

IoMT, or the Internet of Medical Things, is an integration of medical devices and healthcare systems with the Internet, enabling real-time monitoring and remote healthcare services. This increasing connectivity has resulted in enhanced patient care but also exposed sensitive medical data to various security threats. To address these challenges, key management schemes have been proposed as a crucial component for ensuring the confidentiality, integrity, and authenticity of medical data. Several key management strategies have been explored in IoMT, focusing on lightweight and secure methods due to the resource constraints of medical devices. Traditional cryptographic approaches such as symmetric key algorithms (e.g., AES) and asymmetric cryptography (e.g., RSA, ECC) have been widely used but are often computationally expensive, impacting the performance of IoMT devices with limited processing power and battery life. Recent studies propose lightweight encryption and key distribution techniques optimized for IoMT environments. For instance, With the rise due to its lower key of the elliptic curve cryptosystem (ECC), focus size, and reduced computational overhead, making it suitable for low-power devices. Other methods explore hybrid approaches that combine symmetric and asymmetric algorithms to balance security with efficiency. Another emerging area in IoMT key management involves the use of blockchain technology to provide a decentralized and tamper-proof framework for secure key exchange and storage. Blockchain offers enhanced transparency and trustworthiness, reducing the risk of central point failures or attacks. Authentication protocols also play a critical role in IoMT, with biometric-based key generation and secure multi-party computation (SMPC) being studied to enhance device authentication and secure data sharing. In summary, the literature indicates a growing focus on developing secure, efficient, and scalable key management schemes for IoMT, particularly emphasizing lightweight cryptographic algorithms, blockchain integration, and advanced authentication mechanisms tailored to the unique constraints of medical devices.

METHODOLOGY

The proposed key management scheme for IoMT focuses on ensuring security and efficiency through a hybrid cryptographic approach. The methodology involves the following steps: System Architecture Design: The IoMT network is structured into three layers—sensing, network, and application layers. Each layer is responsible for specific tasks like data collection, communication, and processing. Devices in the sensing layer generate and collect medical data. Key Generation and Distribution: A hybrid cryptographic mechanism is employed, combining asymmetric and symmetric key algorithms. Asymmetric cryptography (e.g., Elliptic Curve Cryptography, ECC) is used for initial key exchanges between devices, while symmetric keys (e.g., AES) are used for fast encryption and decryption during data transmission.

Lightweight Authentication Protocol A lightweight authentication mechanism is designed for IoMT devices with limited computational power. This protocol ensures mutual authentication between devices and the central server using hash functions and lightweight encryption. Session Key Establishment: Once the devices authenticate, an instance of a session key is generated using a Diffie-Hellman key exchange, ensuring secure communication. The session key is frequently refreshed to minimize the risk of key compromise. Key Revocation and Update Mechanism: A key revocation mechanism is integrated to revoke compromised keys, ensuring only authorized devices can access the network. Additionally, a periodic key update process ensures forward and backward security.

Performance Evaluation The scheme is evaluated based on computational overhead, communication latency, and energy efficiency. Simulations are conducted to measure the impact of the scheme on resource-constrained devices and to validate the security against potential threats such as man-in-the-middle and replay attacks.

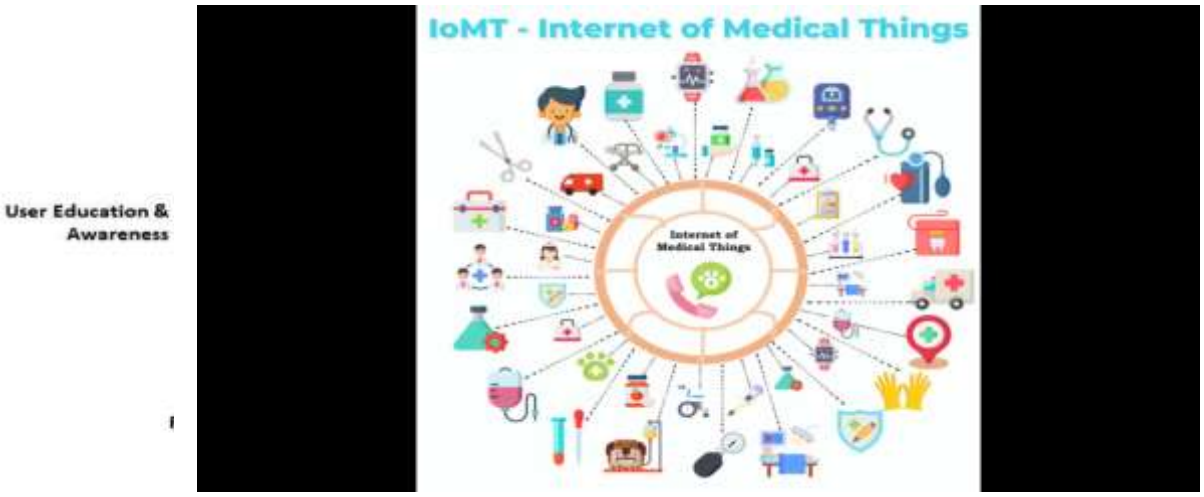

Figure 2. Security areas in IoMT

Figure 2. explains to stop the improper use of IoMT, a number of security and privacy solutions have been created within the past ten years. In fact, cyberattacks are becoming more frequent on IoT devices and applications, like IoMT, which emphasizes the necessity of implementing some crucial procedures to address these issues. Due to server attacks and DOS attacks, these IoMT apps are particularly vulnerable to security problems.

IoMT technology offers security issues because it is still in its infancy and has not fully developed. These risks can be attributed to low user awareness, inadequate maintenance, and insufficient standards. IoMT devices with lax security can be readily taken over by adversaries and hackers through ransomware.

IoMT device control has a negative impact on wearable technology, smart homes, and health-related applications. To make IoMT devices more secure against this kind of attack, research in this area is still required. In order to stay competitive, businesses release goods quickly and neglect to update software, leaving IoMT devices open to hacker attacks. During an update, the user's IoMT device's connection to the cloud may be lost. Through unencrypted transmission, hackers can gain access to unencrypted IoMT equipment. In the event that the cloud connection fails, the company must instantly limit access and ports, and IoMT devices must be updated as needed to maintain security.

OVERVIEW

A research paper on a "Secure and Efficient Key Management Scheme for the Internet of Medical Things (IoMT)" typically explores strategies to enhance security in IoMT environments, which connect medical devices to networks for data exchange. The paper likely outlines the importance of protecting sensitive health information from cyber threats while ensuring efficient data transmission in resource-constrained IoMT devices.

Key aspects of the research may include:

Security challenges IoMT devices are vulnerable to attacks due to their limited computational capacity and the critical nature of the data they handle.

Key management solution the proposed scheme often focuses on lightweight encryption methods or hierarchical key management to reduce computational overhead while ensuring data integrity and confidentiality.

Authentication and privacy Ensuring that only authorized devices and users can access sensitive data, through methods like mutual authentication or zero-knowledge protocols.

Efficiency The scheme needs to balance between security robustness and the energy or processing constraints of IoMT devices, ensuring scalability for large-scale healthcare networks.

Figure 3. Functions of IoMT Layer

IoMT nodes are included in this layer as Sensor Nodes (SNs), which are used to sense, act, and interact in various situations (smart homes and healthcare networks later on). To finish the task, SNs or IoMT nodes from other systems frequently need to communicate and share data. If one or both of the devices/nodes turn malevolent, a Sybil attack can be initiated to stop further communication. IoMT network lifespan and performance are adversely affected by attack scenarios. When the victim and intermediary nodes resend the missing packets, they may produce overheads for messages and energy. Safe communications also require a trustworthy and credible setting. Safe communications also require a trustworthy and credible setting. Prior to collecting data and communicating intermediate data, an IoMT node's additionally, confidence needs to take into account. The recipient can make appropriate use of the data rather than altering it, for example. The suggested blockchain-enabled trust framework prevents single-point loss. On the addition and evaluation of trust as well as the capacity to grow to the decentralized but developing infrastructures of the Internet of Things, there is a decentralized consensus. This layer performs a variety of tasks, including accumulating trust parameters, putting in place Cluster Heads (CHs) on the blockchain, organizing logical IoMT node clusters, and determining topology.

CHALLENGES

A secure and efficient key management scheme 1for the Internet of Medical Things (IoMT) faces several challenges:

Resource Constraints IoMT devices often have limited computational power, memory, and battery life, making traditional cryptographic techniques unsuitable.

Data Privacy and Security Protecting sensitive medical data during transmission and storage is critical, and key management must ensure secure encryption and decryption processes.

Scalability The growing number of IoMT devices requires a key management system that can handle large-scale networks without performance degradation.

Interoperability Devices from different manufacturers must communicate securely, requiring a standardized approach to key management.

Authentication Ensuring the identity of devices and users in a medical environment is crucial in order to stop unwanted access.

Real-time Performance Medical data often needs to be processed in real-time, so key management schemes must be fast and efficient without causing delays.

Resilience to Attacks The system should be robust against various attacks, including eavesdropping, man-in-the-middle, and denial-of-service attacks.

BENEFITS

A research paper on an Internet of Medical Things (IoMT) Secure and Effective Key Management System would likely highlight several key benefits:

Enhanced Security The scheme would ensure that sensitive medical data transmitted between IoMT devices is secure preserving patient confidentiality and safeguarding against cyber threats.

Efficient Key Distribution The proposed system would streamline the process of distributing and managing encryption keys, reducing computational overhead and energy consumption, which is crucial for IoMT gadgets with constrained power.

Scalability It would offer scalability to support a growing number of IoMT devices, ensuring seamless communication in large-scale healthcare environments.

Interoperability The system could facilitate secure communication between different types of IoMT devices, enhancing collaboration between medical devices, hospitals, and healthcare providers.

Reduced Latency By optimizing the encryption process, the scheme would help reduce the time taken to authenticate devices, ensuring timely medical interventions without delays.

User Authentication Stronger and more secure user authentication mechanisms would prevent unauthorized access to medical data, ensuring that only authorized personnel can access sensitive information.

RESULT

The research paper on a "Secure and Efficient Key Management Scheme for the Internet of Medical Things (IoMT)" typically presents a framework addressing the challenges of securing sensitive healthcare data transmitted between IoMT devices. The proposed scheme focuses on ensuring confidentiality, integrity, and authentication while optimizing resource usage, which is critical for IoMT devices with limited computational power and energy resources.

Key features often discussed include:
Lightweight Cryptographic Algorithms The scheme incorporates lightweight encryption techniques tailored for low-power IoMT devices, ensuring security without overwhelming the system's capabilities.
Efficient Key Distribution It suggests mechanisms for secure key generation and distribution among devices, minimizing communication overhead and ensuring seamless updates or rotations of keys.
Mutual Authentication Devices are mutually authenticated to prevent unauthorized access or tampering, typically using a combination of asymmetric and symmetric encryption.
Scalability The scheme supports scalability to accommodate the growing number of devices in IoMT networks without compromising security or efficiency.
Energy Efficiency Special attention is given to reducing computational and communication costs to extend the battery life of IoMT devices, making the solution practical for real-world healthcare environments.

DISCUSSION

Internet of Medical Things (IoMT) typically focuses on addressing the challenges of securing medical data transmitted across connected devices in healthcare environments. The Internet of Medical Things (IoMT) involves interconnected medical devices that collect, process, and share sensitive health data, making security a critical concern.
The paper likely suggests a critical management plan designed to enhance both security and efficiency in IoMT networks, where key management is crucial for protecting data confidentiality, integrity, and authentication. The research may discuss existing challenges, such as the limited computational resources of IoMT devices, the need for low-latency communication, and the risks posed by potential cyberattacks.
The proposed scheme may involve techniques like lightweight cryptographic protocols, dynamic key generation, or hierarchical key management to minimize computational overhead. It might also ensure secure communication between devices by encrypting data, periodically updating keys, and implementing secure key distribution mechanisms. Efficiency would be demonstrated through reduced energy consumption and fast data transmission, while still maintaining robust security standards.

FUTURE SCOPE

The future scope of a research paper on "Secure and Efficient Key Management Scheme for the Internet of Medical Things (IoMT)" can explore several areas:
Scalability in Large-Scale IoMT Networks Investigating how key management schemes can scale efficiently in vast IoMT ecosystems while maintaining performance and security.
Lightweight Cryptographic Solutions Further research on developing lightweight cryptographic algorithms tailored to the resource-constrained nature of IoMT devices, balancing security and power consumption.
Post-Quantum Cryptography Exploring the integration of post-quantum cryptographic techniques into IoMT systems to future-proof key management schemes against potential quantum computing threats.
AI-Driven Security Examining the use of machine learning and artificial intelligence to predict, detect, and mitigate security threats in key management protocols dynamically.
Interoperability and Standardization Investigating how secure key management can be standardized across different IoMT devices and platforms, ensuring seamless integration and operation across diverse systems.
Blockchain for Decentralization Researching blockchain technology as a means to provide decentralized, transparent, and tamper-proof key management for IoMT systems.
User Privacy and Data Integrity Exploring ways to enhance privacy-preserving mechanisms and ensure data integrity in key management protocols without compromising efficiency.

CONCLUSION

In conclusion, an effective key management scheme is crucial for ensuring the Internet of Medical Things' (IoMT) data security and privacy. It is feasible to preserve system performance and scalability while safeguarding private medical data from illegal access by putting in place a safe and effective solution. Lightweight cryptographic methods that are appropriate for IoMT devices with constrained computational resources should be the main emphasis of the suggested plan. To combat changing security risks, it must also guarantee safe key distribution, storage, and upgrades. This will boost confidence in IoMT networks and guarantee the integrity of patient data.

REFERENCE

1. Image link for fig1: - https://www.mdpi.com/2076-3417/12/15/7487
2. Image link for fig2: - https://www.mdpi.com/2071-1050/15/4/3317
3. Image link for fig3: - https://www.mdpi.com/1424-8220/23/9/4265

4. IOMT design of blockchain enabled authenticated key management protocol for internet of medical things deployment.
https://ieeexplore.ieee.org/abstract/document/9097179/

5. Internet of medical things based secure and energy efficient framework for health care
https://www.liebertpub.com/doi/abs/10.1089/big.2021.0202