International Journal of Computer Sciences and Engineering
Vol.**11**, Issue **3**, pp.**10-16**, March **2023**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Research Paper

Energy-Efficient and Secure Framework for IoMT-Based E-Healthcare Systems Using Intelligent Routing

Mohammad Sirajuddin[1*], B. Sateesh Kumar[2]

[1]Department of CSE, JNTU, Hyderabad, Telangana, India
[2]Department of CSE JNTUH-College of Engineering, Jagtial, Telangana, India

**Corresponding Author: mohdsiraj569@gmaill.com*

Received: 05/Feb/2023; **Accepted**: 15/Mar/2023; **Published**: 31/Mar/2023. **DOI**: https://doi.org/10.26438/ijcse/v11i3.1016

Abstract: The Internet of Medical Things (IoMT) is a group of internet-connected medical devices used in e-healthcare for remote patient diagnosis, medical equipment regulation, and tracking of quarantined patients. However, the IoMT faces security and privacy concerns due to the vast amounts of data handled by these devices, which can lead to sensitive personal data being exposed to various attacks. This paper proposes a secure route management strategy using the AODV protocol and a modified lightweight AES encryption approach to protect healthcare data. The approach is demonstrated to be secure against black hole attacks and requires relatively low computation and communication resources. These findings indicate that the proposed paradigm is suitable for deployment in IoMT devices with limited.

Keywords: IoMT Intelligent routing, lightweight cryptography, IoMT, E-healthcare, IoMT-Security.

1. Introduction

The Internet of Things (IoT) has brought a revolutionary change in the healthcare industry by introducing the concept of the Internet of Medical Things (IoMT). It refers to the interconnectivity of medical devices, healthcare software, and healthcare systems through the internet. The IoMT has opened doors to advanced healthcare services, remote patient monitoring, and personalised medicine. However, the IoMT also brings significant security issues that must be addressed to ensure patient safety and privacy [1].

The IoMT consists of various medical devices such as sensors, wearables, and implantable devices that collect, store, and share patient data. These devices communicate with each other, the healthcare providers and other stakeholders to provide real-time data analysis, alerts, and notifications. However, the unsecured communication channels between these devices and systems can lead to cybersecurity vulnerabilities. One of the most significant security issues related to the IoMT is data breaches. The medical devices connected to the internet can be hacked, and the sensitive patient data they store can be stolen, altered, or deleted. This data can include personal health information (PHI), medical records, and financial information. The theft of PHI can lead to identity theft, insurance fraud, and other malicious activities. Another security issue is the lack of proper authentication and authorisation mechanisms in the IoMT [1]. Most of the medical devices in the IoMT are not designed with strong security features, making them vulnerable to attacks. A hacker can gain unauthorised access to a medical device, manipulate the data, and even cause harm to the patient [2]. The use of legacy devices and outdated software is also a major security risk in the IoT. Many medical devices were not built with security in mind and lacked the necessary encryption and authentication protocols. IoMT devices are often connected to outdated software that is no longer supported by the manufacturer, making them more susceptible to security threats.

The security issues related to the IoMT are not limited to medical devices alone. The communication channels between the devices, the healthcare providers, and the patients are also vulnerable to attacks. The use of unsecured Wi-Fi networks, mobile devices, and cloud services can expose sensitive data to cybercriminals [3]. To address these security issues, healthcare organisations and device manufacturers must take proactive measures to secure the IoMT.

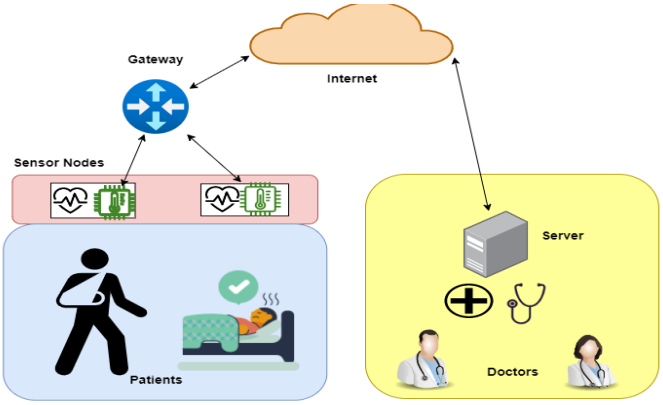

Figure 1. IoMT-based E-health care system Scenario

This includes implementing strong encryption and authentication protocols, regularly updating the software and firmware of the devices, and monitoring the network for suspicious activities. Healthcare providers must also educate their staff and patients about the importance of cybersecurity and safe internet practices [3].

The world is increasingly relying on technology to manage various aspects of life, and the Internet of Medical Things (IoMT) is no exception. IoMT is a rapidly growing area of technology that is transforming the healthcare industry, allowing doctors and patients to access vital health data in real time. However, as with any emerging technology, IoMT is not without its challenges. One such challenge is the need for strong security measures to protect the sensitive data generated and transmitted by these devices. This is where lightweight cryptography comes into play [4].

Lightweight cryptography is a set of cryptographic algorithms designed specifically for resource-constrained devices, such as those used in IoMT. These algorithms are designed to use minimal resources, such as memory and processing power, while still providing strong security. The importance of lightweight cryptography in IoMT devices cannot be overstated. In this article, we will explore the unique ways in which lightweight cryptography is essential to the security of IoMT devices. Firstly, IoMT devices are often small, low-power devices with limited processing capabilities. This makes them vulnerable to attacks from malicious actors who may attempt to exploit weaknesses in the device's security protocols [5]. Light cryptography algorithms are designed to mitigate this vulnerability by using fewer resources while still providing strong security. This means that IoMT devices can be designed to incorporate strong security measures without sacrificing performance or battery life.

Secondly, IoMT devices are often used in sensitive applications such as patient monitoring, drug delivery, and diagnostic testing. Any breach of the security of these devices could have serious consequences, including compromising patient privacy, compromising the accuracy of medical tests, and even endangering patient lives. Lightweight cryptography algorithms provide an extra layer of protection against these risks by ensuring that sensitive data is encrypted and transmitted securely [5]. Thirdly, IoMT devices are often deployed in remote or uncontrolled environments, such as in patients' homes or in the field during emergency response operations. This means that they may be subject to physical attacks, such as tampering or theft. Lightweight cryptography algorithms can provide protection against physical attacks by ensuring that data stored on the device is encrypted and that only authorised users can access the device. Fourthly, IoMT devices are often part of a larger ecosystem of connected devices, such as medical databases, patient monitoring systems, and diagnostic equipment. This interconnectedness increases the complexity of the security architecture, making it more difficult to ensure that every device in the network is secure [6]. Light cryptography algorithms can help to simplify this process by providing a standardised, lightweight set of cryptographic protocols that can be easily integrated into the security architecture of the entire system. Finally, lightweight cryptography algorithms are designed to be easily upgradable and adaptable to changing security threats. As the threat landscape evolves, it is essential that IoMT devices can be updated with the latest security measures to ensure that they remain secure. Lightweight cryptography algorithms can be easily updated to incorporate the latest security protocols, ensuring that IoMT devices remain secure even in the face of new threats.

The importance of lightweight cryptography in IoMT devices cannot be overstated. These algorithms provide an essential layer of protection against a wide range of security threats, including physical attacks, data breaches, and unauthorised access. By using minimal resources while still providing strong security, lightweight cryptography algorithms allow IoMT devices to operate in resource-constrained environments without sacrificing performance or battery life [7]. As the use of IoMT devices continues to grow, it is essential that designers and developers incorporate lightweight cryptography algorithms into their designs to ensure the security and safety of patients and healthcare professionals alike.

The structure of this article can be summarized as follows: Section 2 provides an overview of the related work. Section 3 details the methodology used to create the Secure Routing framework for an e-healthcare system enabled by the Internet of Medical Things (IoMT). Section 4 explains the secure transmission of healthcare data, which utilizes the Lightweight AES Algorithm. Sections 5 and 6, respectively present the results and conclusions of the study.

2. Related Work

The article [8] suggests a three-factor privacy-preserving strategy that is safe, secret, and lightweight to address security issues in IoMT-enabled TMIS scenarios. We demonstrated that SALS-TMIS protects users from a variety of security threats and provides essential security features, such as user secrecy, scalability, and reciprocal verification. The security of SALS-TMIS was then assessed using the ROR Oracle Model, BAN Logic, and AVISPA Execution. Additionally, we assessed how SALS-TMIS performed in contrast to similar schemes in terms of processing and transmission expenses. In comparison to similar systems, SALS-TMIS increased the security level while also ensuring minimal computation and transmission costs. SALS-TMIS is, therefore, suitable for IoMT-enabled TMIS settings because it offers greater protection and efficiency than similar methods.

In the article [9], a brand-new ASCP-IoMT, or short for ASCP-IoMT, a lightweight, secure communication strategy for an IoMT system, has been developed. There are several methods used to conduct the security assessment of ASCP-IoMT, including a casual method and a rigorous method (using the random oracle model). When contrasted to other comparable methods, ASCP-IoMT outperforms them in terms of performance and security and offers more characteristics in terms of usefulness.

The paper [10] proposed a novel data-sharing method that uses blockchain technology and permits secure profile

matching while maintaining user anonymity. It uses a bloom filter with hash algorithms to check the validity of keyword ciphertext. To accomplish safe profile matching, the key-policy attribute-based encryption algorithm and smart contracts are used. We design a reward mechanism and build a two-phase Stackelberg game to handle pricing issues for data owners and access issues for data requesters in order to motivate users who actively participate in profile matching. The optimal pricing system was created specifically to increase user participation in the exchange of health data while optimising user profit. Additionally, security analysis indicates that the proposed protocol can achieve a variety of security objectives the high scalability and viability of the proposed protocol.

To track patient bodily details and address the problems, Paper [11] suggested a three-factor enhanced protocol. The suggested procedure can guarantee both the privacy of medical professionals and their patients as well as the secrecy of transmitted data. In the Random Oracle Model (ROM) for algorithmic security, the suggested protocol's security is shown. The suggested protocol also performs effectively in terms of execution time and communication expenses when compared to other related works.

By combining fault analysis and differential power analysis, the article [12] provided a physical analysis model of Rainbow. The cloud computing platform is used to execute the suggested strategy. Based on the trial findings, we were able to effectively retrieve every secret key for the Rainbow signature, demonstrating the significance of safeguarding multivariate signatures on medical equipment.

The proposed framework [13] is safer than current frameworks and immune to a variety of security risks. The random oracle model (ROM) and two different methods are used to verify the formal security analysis of RAPCHI in the article. Using the simulation software AVISPA, the article also demonstrates that RAPCHI is resistant to man-in-the-middle and reply assaults. Furthermore, RAPCHI is shown to be comparatively light in terms of computation and communication when compared to similar systems. These results show that the suggested model can be applied to actual situations.

Artificial intelligence (AI) technology has been used to create a new secure communication system for the Internet of Medical Things (IoMT) in [14]. The ASCP-IoMT protocol describes the configurations of various network devices and the related attacks that may happen in the IoMT environment. It has been meticulously developed, taking into consideration the network and threat models of the IoMT. Extensive security analysis was carried out, proving that the ASCP-IoMT protocol is safe from a variety of potential threats. The ASCP-IoMT protocol offers more features and better protection when compared to other approaches of a comparable nature. After that, practical research was conducted to determine how ASCP-IoMT affected different factors.

A blockchain-enabled authentication and key agreement protocol is introduced in the article [15] that is created especially for the Internet of Medical Things (IoMT) environment. The BAKMP-IoMT protocol guarantees safe key management for personal computers, online servers, and implantable medical devices. Healthcare data saved on cloud servers and managed using blockchain technology is safely accessible to authorised users. To show that BAKMP-IoMT is resilient to various kinds of potential threats, a thorough formal security analysis is performed, including proof using the widely used Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. BAKMP-IoMT offers greater security and usefulness while needing less transmission and processing resources, according to a comparison with pertinent current schemes.

In [16], the exponential K-anonymity method is used to preserve secrecy. A brand-new and enhanced Elman neural network (IENN) is also suggested for examining the degree of data sensitivity. The Gaussian mutated ape optimisation method is used to update the weights in this IENN. A novel RECC-VC is suggested, which guarantees that the data is saved on the cloud server using blockchain technology to safely upload data to the cloud server. Experimental research shows that the suggested approaches outperform the current ones. The suggested IENN model, which has been verified against cutting-edge techniques, gets an accuracy of 96%.

The strategy described in [17] makes use of lattice as a defence against potential quantum attacks in the future. This scheme's lightweight design makes it especially appropriate for settings with limited resources found in the Internet of Medical Things (IoMT). The protocol has proven to be resistant to the majority of conventional and prospective quantum security threats. The suggested scheme can be applied in resource-constrained quantum settings because of its effectiveness and simplicity. The suggested protocol has additionally undertaken a thorough security analysis to guarantee its verifiable security. Efficiency analysis further supports the suggested approach's suitability for use in IoT devices.

3. Methodology

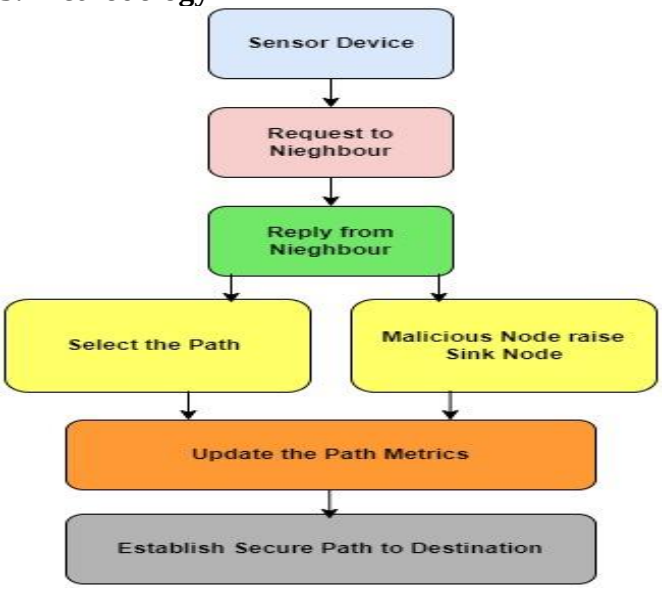

Figure 2. Architecture of Proposed Methodology

The Intelligent Routing-Based Energy-Efficient and Secure System for IoMT that is being offered The suggested method includes a variety of elements, from biosensor devices to servers, and is intended to improve the energy economy and security of patient data transfer. The framework offers an efficient, dependable, and private method of keeping track of patient's bodily well-being during emergencies by utilising WBN technology and a lightweight AODV procedure. Overall, this framework provides a strong answer for medical apps, offering numerous advantages to both patients and healthcare professionals. The sink node then transmits healthcare data to medical experts via intermediate devices after gathering patient data. It is crucial to remember that malevolent nodes have the ability to target the network's architecture, which could result in leaks.

Sending a Route Request to the closest device, the biosensor device starts the connection procedure. Following a prompt evaluation of the request, the nearby node replies to the source sensing node with a route response. The adjacent node's answer is suitable and relevant if it can raise the sequence number and provide accurate information free of malicious content. When the biosensor node receives an invalid answer, it is stopped, forcing the source node to find another nearby node with which to communicate.

The Shortest Path Routing method is used in conventional network strategies to choose the best route for transmission. To enhance the network's general security, this method has been changed to include safe and effective standards using recommended routing logic. When malicious nodes are discovered, the sink node serves as an evaluator node, determining the node's energy levels and offering the required path information to bring it back to normal and qualify it for the subsequent transfer. This guarantees that energy-efficient nodes are given priority and that the network can function even when there are energy-inefficient nodes present.

4. Secure transmission of healthcare data using Lightweight AES Algorithm

The proposed route management methodology employs a Light weight AES algorithm for transmitting confidential patient data from the sink node to remote servers. The proposed technique utilises the Light weight AES algorithm to both encrypt the data at the sender's end and decrypt it at the receiver's end, ensuring that the patient data remains secure and protected during transmission.

Lightweight cryptography is essential for ensuring the security and privacy of the Internet of Medical Things (IoMT) devices. IoMT devices, such as wearables, implantable medical devices, and health sensors, are designed to monitor and transmit sensitive medical data. As such, they are often connected to the internet, creating vulnerabilities to cyber-attacks and data breaches.

Lightweight cryptography algorithms are specifically designed to be implemented on resource-constrained devices such as IoMT devices. These devices often have limited processing power, memory, and battery life, making it challenging to implement complex security mechanisms. Lightweight cryptography algorithms, however, have been optimised for performance, ensuring that the security features do not impede the device's functionality.

The use of lightweight cryptography in IoMT devices has several benefits. Firstly, it enables the use of strong encryption algorithms that ensure the confidentiality and integrity of patient data. Secondly, it helps to reduce the energy consumption of these devices, which is essential for extending their battery life. Finally, lightweight cryptography algorithms can be implemented on devices with limited resources, providing a cost-effective security solution. Lightweight cryptography plays a critical role in ensuring the security and privacy of IoMT devices. Its optimisation for performance and resource-constrained devices makes it an ideal solution for securing medical data in IoMT devices while also ensuring the devices remain functional and energy-efficient.

The Lightweight AES Algorithm has been specifically designed as a lightweight encryption mechanism for wireless sensor devices with limited resources. The primary objective of this algorithm is to balance complexity and speed while also reducing execution and computation time. To achieve this goal, several modifications have been made to the conventional AES Algorithm.

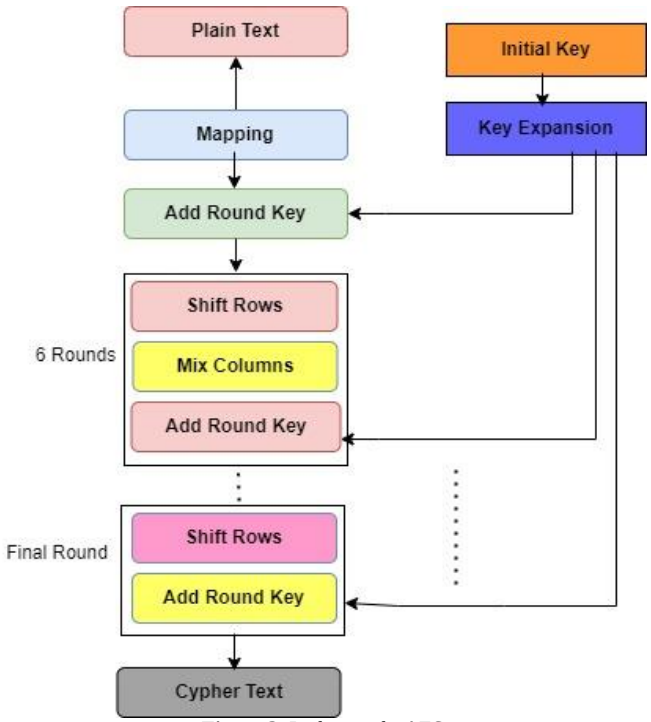

Figure 3. Light weight AES

The light weight algorithm incorporates a mapping procedure for plain text, which reduces the number of rounds to six. Each round includes three steps, namely ShiftRows, MixColumn, and AddRoundKey, except for the last round, which only includes two steps. The MixColumn function is a

crucial operation in terms of both complexity and security, but it requires significant computational time. To improve performance, the algorithm includes a mapping phase that rearranges the characters of the plain text to disrupt the analytical relationships between them. This phase is only applied once before encryption to replace the S-box round of the conventional AES algorithm.

The Light weight AES Algorithm leverages the mapping phase to increase the complexity of the encryption process and compensate for the absence of the Sub Bytes step. The mapping phase reorganises the characters in the plain text and applies a mapping.

5. Results and Discussion

In this section, we outline the suggested strategy and offer supporting data. It's a good idea to have a backup plan, just in case. To perform the simulation, we utilised Network Simulator 2 to reproduce the wireless sensor network, utilising the AODV protocol. The essential components needed for the simulation are listed in Table 1. We looked at the network's packet overhead, throughput, delay, and resource usage, among other quantitative aspects.

Table 1. Simulation Setup

Parameter	Quantity
Protocol	AODV
Simulator	NS-2
Simulation Area	500x500m
Number of Nodes	20
Packets	TCP Packets
Transmission Range	200m
Simulation Time	100 sec

Figure 4. Delay analysis

Delay is determined by the time between transmission and reception, which includes various stages such as network formation, path creation, encryption at the sender, decryption at the receiver, and more. The ICARS methodology proposed in this study successfully decreases data transmission delay to a certain extent, as demonstrated in Figure 5. The reduction achieved by ICARS is superior to that of the traditional AODV routing protocol and RAPCHI.

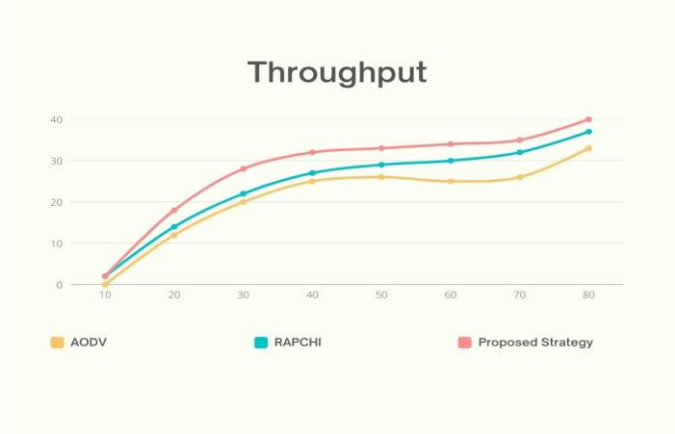

Figure 5. Throughput analysis

We assessed the throughput of the proposed scheme by measuring the ratio of received packets to transferred packets without any loss. Our analysis reveals that the proposed approach delivers a moderately higher throughput value compared to both the classical AODV Routing protocol and RAPCHI.

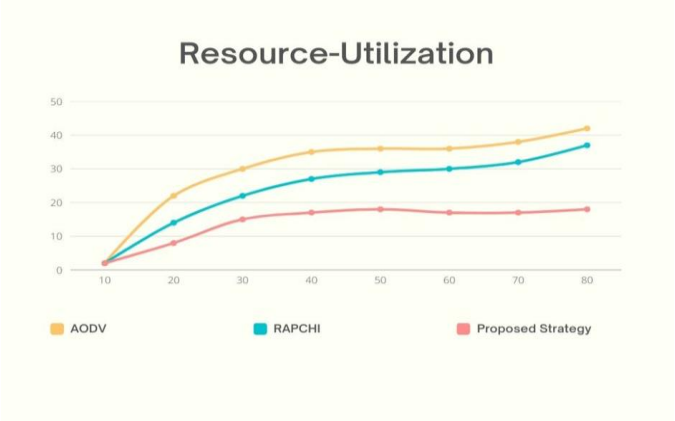

Figure 6. Resource-Utilisation analysis

We conducted a comprehensive analysis of resource utilisation during packet transmission, as illustrated in Figure 4. Since energy consumption is impacted by factors such as distance and link efficiency, the proposed scheme employs a moderate amount of energy. Our analysis confirms that the proposed approach outperforms both the classical AODV Routing protocol and RAPCHI in terms of energy usage.

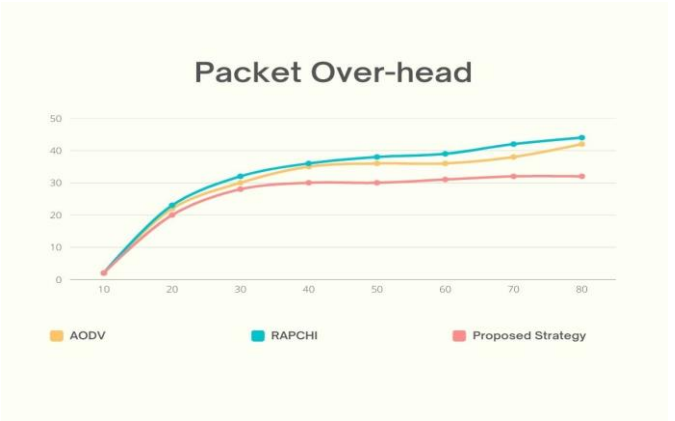

Figure 7. Packet Over-head analysis

As depicted in Figure 6, our analysis of packet overhead validates the proposed scheme and demonstrates that it surpasses both the classical AODV Routing protocol and RAPCHI.

6. Conclusion and Future Scope

IoMT has revolutionised the healthcare industry by providing advanced healthcare services and personalised medicine. However, the security issues related to the IoMT cannot be ignored. The sensitive patient data stored and shared through the IoMT must be protected from cybercriminals. It is the responsibility of healthcare organisations, device manufacturers, and other stakeholders to ensure the safety and privacy of the patients using the IoMT. E-healthcare equipment connected to the internet are called the Internet of Medical Things (IoMT). Smart electronic gadgets at the patient's location enable remote patient diagnostics, medical equipment regulation, and confined patient tracking. The exponential rise of data handled by medical devices exposes sensitive personal data to numerous susceptible assaults, posing security and privacy risks for the IoMT. This research presents an efficient and safe route management method using the AODV protocol and modified lightweight AES encryption to protect healthcare data. The article also proves the technique is black hole-proof. The research compares it to other frameworks and concludes that it uses little computation and communication. These findings suggest the suggested paradigm is suitable for resource-constrained IoMT devices.

References

[1]. F. Khan, M. A. Jan, R. Alturki, M. D. Alshehri, S. T. Shah and A. u. Rehman, "A Secure Ensemble Learning-Based Fog-Cloud Approach for Cyberattack Detection in IoMT," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2022.3231424.

[2]. B. Tahir, A. Jolfaei and M. Tariq, "A Novel Experience-Driven and Federated Intelligent Threat-Defense Framework in IoMT," in IEEE Journal of Biomedical and Health Informatics, doi: 10.1109/JBHI.2023.3236072.

[3]. Z. Xu, Y. Guo, C. Chakraborty, Q. Hua, S. Chen and K. Yu, "A Simple Federated Learning-Based Scheme for Security Enhancement Over Internet of Medical Things," in IEEE Journal of Biomedical and Health Informatics, vol.**27**, no.**2**, pp.**652-663, Feb. 2023**, doi: 10.1109/JBHI.2022.3187471.

[4]. M. Sirajuddin and B. S. Kumar, "Efficient and Secured Route Management Scheme Against Security Attacks in Wireless Sensor Networks," 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, pp.**1045-1051, 2021.** doi: 10.1109/ICESC51422.2021.9532779.

[5]. R. P. Parameswarath, P. Gope and B. Sikdar, "Privacy-Preserving User-Centric Authentication Protocol for IoT-Enabled Vehicular Charging System Using Decentralised Identity," in IEEE Internet of Things Magazine, vol.**6**, no.**1**, pp.**70-75**, March **2023.** doi: 10.1109/IOTM.001.2200041.

[6]. Sirajuddin, M., Sateesh Kumar, B. (2022). Collaborative Security Schemes for Wireless Sensor Networks. In: Kumar, A., Mozar, S. (eds) ICCCE 2021. Lecture Notes in Electrical Engineering, vol **828, 2022.** Springer, Singapore. https://doi.org/10.1007/978-981-16-7985-8_36

[7]. T. Alladi, A. Agrawal, B. Gera, V. Chamola and F. R. Yu, "Ambient Intelligence for Securing Intelligent Vehicular Networks: Edge-Enabled Intrusion and Anomaly Detection Strategies," in IEEE Internet of Things Magazine, vol.**6**, no.**1**, pp.**128-132**, March **2023**, doi: 10.1109/IOTM.001.2200197.

[8]. S. Yu and K. Park, "SALS-TMIS: Secure, Anonymous, and Lightweight Privacy-Preserving Scheme for IoMT-Enabled TMIS Environments," in IEEE Access, vol.**10**, pp.**60534-60549**, **2022**, doi: 10.1109/ACCESS.2022.3181182.

[9]. M. Wazid, J. Singh, A. K. Das, S. Shetty, M. K. Khan and J. J. P. C. Rodrigues, "ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things," in IEEE Access, vol.**10**, pp.**57990-58004**, **2022**, doi: 10.1109/ACCESS.2022.3179418.

[10]. Xueli Nie, Aiqing Zhang, Jindou Chen, Youyang Qu, Shui Yu, "Blockchain-Empowered Secure and Privacy-Preserving Health Data Sharing in Edge-Based IoMT", Security and Communication Networks, vol.**2022**, Article ID 8293716, 16 pages, **2022**. https://doi.org/10.1155/2022/8293716.

[11]. Chien-Ming Chen, Shuangshuang Liu, Xuanang Li, SK Hafizul Islam, Ashok Kumar Das, A provably-secure authenticated key agreement protocol for remote patient monitoring IoMT, Journal of Systems Architecture, Vol.**136**,2023,102831,ISSN1383-7621, https://doi.org/10.1016/j.sysarc.2023.102831.

[12]. Yi, H., Nie, Z. On the security of MQ cryptographic systems for constructing secure internet of medical things. Pers Ubiquit Comput 22, **1075–1081, 2018**. https://doi.org/10.1007/s00779-018-1149-y.

[13]. Kumar, V., Mahmoud, M.S., Alkhayyat, A. et al. RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure. J Supercomput 78, **16167–16196, 2022.** https://doi.org/10.1007/s11227-022-04513-4S.

[14]. Willium, "Biological Sciences," *International Journal of Scientific Research in Computer Science and Engineering*, Vol.**31**, Issue **4**, pp.**123-141**, **2012**.

[15]. M. Wazid, J. Singh, A. K. Das, S. Shetty, M. K. Khan and J. J. P. C. Rodrigues, "ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things," in IEEE Access, vol.**10**, pp.**57990-58004, 2022**, doi: 10.1109/ACCESS.2022.3179418.

[16]. N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues and Y. Park, "BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment," in IEEE Access, vol.**8**, pp.**95956-95977, 2020**, doi: 10.1109/ACCESS.2020.2995917.

[17]. M. Kumar, Kavita, S. Verma, A. Kumar, M. F. Ijaz and D. B. Rawat, "ANAF-IoMT: A Novel Architectural Framework for IoMT-Enabled Smart Healthcare System by Enhancing Security Based on RECC-VC," in IEEE Transactions on Industrial Informatics, vol.**18**, no.**12**, pp.**8936-8943**, Dec.**2022**, doi: 10.1109/TII.2022.3181614.

[18]. Gupta, D.S., Mazumdar, N., Nag, A. et al. Secure data authentication and access control protocol for industrial healthcare system. J Ambient Intell Human Comput, **2023**. https://doi.org/10.1007/s12652-022-04370-2

AUTHORS PROFILE

Mohammad Sirajuddin is currently pursuing a PhD in Computer Science & Engineering at Jawaharlal Technological University in Hyderabad, Telangana, India. His research interests include machine learning, Internet of Medical Things (IoMT), artificial intelligence, and wireless sensor networks. He has authored more than 15 peer-reviewed academic papers and articles in reputed journals like Springer and IEEE. Additionally, he has received advanced training in machine learning algorithms, IoT, and Mission 10X. Mohammad has also attended several conferences and presented his research work.

Dr. B. Sateesh Kumar is a Professor of Computer Science & Engineering at JNTUH College of Engineering Jagitial (JNTUHCEJ) in Telangana, India. He has received numerous national and international awards for his outstanding contributions to the field of education and services. These awards include the Vishista Seva Puraskar from JNTUHCEJ in 2011, the Bharath Jyoti Award from IIFS Delhi in 2011, and the Best Teacher Award from JBREC in 2006. He has organised several professional development programs, including a recent one on Advanced Machine Learning Algorithms at JNTUH HRDC in September 2021. He has also received training on Big Data and Cloud Analytics, as well as Data Mining and Data Warehouse techniques. He is an active member of several professional and service-oriented organisations, including the Indian Society for Technical Education (ISTE). He has served and is currently serving as a governing body member for the boards of studies of various universities, including Kakatiya University.

