A Secure Framework for Internet of Medical Things Security Based System using Lightweight Cryptography enabled Blockchain

Joseph Bamidele AWOTUNDE[1*][0000-0002-1020-4432], Sanjay MISRA[2][0000-0002-3556-9331],

[1]Department of Computer Science, Faculty of Communication and Information Sciences, University of Ilorin, Ilorin, Nigeria
[2]Department of Computer Science and Communication, Østfold University College, Halden, Norway

awotunde.jb@unilorin.edu.ng[1], Sanjay.misra@hiof.no[2],

Abstract. The Internet of Medical Things (IoMT) is a growing paradigm that offers several efficient and productive solutions for the treatment of various ailments for both patients and medical professionals. The IoMT has many advantages, but security remains a problem that must be overcome. The inexperienced IoMT users' lack of security and privacy consciousness and the possibility of multiple middleman attacks for getting the healthcare information, seriously puts the use of IoMT in jeopardy. Therefore, this paper proposes a lightweight cryptography enabled with blockchain for enhancing IoMT-based security and privacy. The study utilize lightweight cryptography to securely uploading the data to the cloud database for privacy preservation, and the Blockchain technology is use to securely store the data in the cloud server. The experimental results of the proposed model revealed a better results with compare with prevailing methods. The proposed system achieves an accuracy of 98% of security level.

Keywords: Internet of Medical of Things, Blockchain technology, Lightweight cryptography, Security and privacy, Cloud computing.

1 Introduction

All technological breakthroughs have been centered on data. The use of technologies that enable interconnectedness to establish communications with multiple services has been advocated among various organizations and vendors [1]. Healthcare is one of several industries where blockchain and Internet of Medical Things (IoMT) are being used extensively for applications like secure storage, interactions, and automation technologies [2-3]. IoMT devices lack security and self-protection capabilities, are resource restricted, and is extremely vulnerable to compromise [4]. Blockchain is one of the innovative aspects that has aided this development. Blockchain technology has been used to decentralize communication between many clients while preserving confidentiality and unlinkability in a fully decentralized setting without a central authority. Blockchain has been suggested for a variety of services and solutions by blockchain proponents.

One of the suggested methods for implementing blockchain functionalities is the IoMT paradigm [5]. Despite the robustness and tamper-proof nature of blockchain, but due to its transparency, significant privacy and trustworthiness issues have been brought up. When it comes to patient history information, the primary and most important cryptographic method is to encrypt sensitive information [6]. The platform for sending and receiving patient health records is thought to be the digital healthcare system [7]. The majority of the current healthcare systems, however, lack adequate access control and encryption technologies, therefore they lack security measures. The key component of effective healthcare is the dissemination of medical data to authenticate users. Blockchain offers a peer-to-peer and decentralized network system, which is more crucial [8]. It is a blockchain that is consortium- and permission-managed, which indicates that every peer is known to the network. All concerned parties benefit from the confidence and safety it offers [9].

There are a number of lightweight cryptography techniques available to address the issues raised above, but they are less effective in terms of adaptability and confidentiality [10]. The field of cryptography is developing, and new methods of attack, design, and deployment are being thoroughly researched [11]. The state-of-the-art method known as "Lightweight Cryptography (LWC)" is one of them [12]. A cryptographic technique or protocol designed for deployment in limited settings is known as lightweight cryptography. The LWC can be implemented in various environments like contactless smart cards, RFID tags, sensors, healthcare device among others. Secure is one of the most promising and reliable solutions to these problems. The LWC, which enables users to encrypt data on their own without a third party's assistance. Additionally, LWC offers sufficient security, and not necessarily take advantage of the efficiency-security trade-offs [10].

The LWC was employed for two major reasons namely:

a. End-to-end communication effectiveness end nodes must implement a symmetric key method in order to achieve end-to-end security. The cryptographic operation with a restricted quantity of energy consumption is crucial for resource - constrained devices, such as rechargeable batteries appliances. End devices can use less energy when the lightweight symmetric key method is used.
b. Application to devices with less resources: The LWC primitives have a smaller physical footprint than the traditional cryptographic ones. The use of additional network connections with less resource-intensive devices is made possible by the LWC primitives.

Some end nodes could be able to integrate general-purpose microprocessors, and in such systems, software characteristics are significant. However, because to their restricted cost and energy consumption, the cheapest devices can only integrate application-specific ICs, where hardware characteristics are of utmost importance. Because it is effective and has a less environmental impact, LWC helps to secure networks of smart items. We think that while designing networks, lightweight primitives should be taken into account. It is now viable to employ lightweight block ciphers in particular [13-14].

Additionally, blockchain is a new platform with immutability qualities that offer secure administration, authentication, and financial transactions, and secure access management for IoMT devices [15]. IoMT is a cloud-based internet connection in which

user data is processed and collected centrally. The institution must also be able to diagnose patients who are located remotely in order to deliver smart healthcare. Significant challenges with the IoMT-based framework include data security, prices, memory, sustainability, trustworthiness, and transparency between many ecosystems. Since the user's legitimacy is in doubt owing to an open internet setting, it is crucial to manage information confidentiality and authenticity. There are a number of strategies that are mostly concerned with addressing security difficulties, include attacks using stolen smartcards, timing, denial of service, and forgeries, among others. To identify the people involved in transactions, blockchain technology adheres to the principles of complete privacy. Immutability, better data sharing, increased security, and the elimination of a centralized third party are the driving forces for the usage of blockchain in IoMT-based systems [16], and for distributed applications with lower overhead expenses [17]. In addition to extra legal standards, IoMT-based platforms have several special security and privacy issues.

Therefore, this study explores the use of lightweight cryptography and blockchain to solve the security and privacy issues in IoMT-based system. Specifically, this paper use LWC to secure the patient data on the IoMT platform [18] to address the concerns about the confidentiality of transactions between blockchain nodes, and serious security risks to critical IoMT environments [1]. The paper provide the following key contributions:

(i) to guarantee the confidentiality and integrity of user data, a LWC authentication and authorisation architecture was developed for the Blockchain-enabled IoMT environments.

(ii) Make a suggestion for an enhanced multi-user enhanced secure LWC that assigned roles to safely enquire across specified search queries in the distributed ledger.

(iii) the patient initially encrypts the data before uploading it to the blockchain.

Once the data owner has finished the encryption, the proposed model offers the data owner a facility that will not allow access until they require policy revocation or deletion, through other procedures. The rest of the article is summarized as below: Section 2 presents the related work, section explain and give the full description of the proposed model. The results and discussion with experimental investigations was presented in Section 4. Finally, the conclusion and future scope was presented Section 5.

2 Related work

Blockchain is a tamper-proof, decentralized data warehouse. Consequently, blockchain technology may be utilized to maintain patient medical records, and can be extremely important for maintaining and effectively sharing healthcare data in the domain of healthcare. IoMT consists of a vast number of interconnected items, including sensors, computers, embedded systems, actuators, cellphones, and more [20-22]. Traditional communication protocols including HTTP, TCP, and IP are ineffective at supporting M2M communication, according to studies conducted by authors in [23-24]. The authors in [25] also put forth a three-layered design with artifacts, linguistic, and internet-oriented layers. In [26-27], the authors discussed the security issues and solutions of the three-layer architecture are covered in depth, and following is a summary: (a) perception layer: timing attack, man in the middle (MITM) attack, node capture,

DoS attack, and malicious node assaults can all happen in this layer; (b) Network layer: The key issues with this layer are identity authentication issues, privacy exposure to prevent various attacks within the layer, such attack are DoS attack, MITM attack, replay attacks, eavesdropping attack, and so on; (c) Application layer: This attack includes pricay protection, identity authentication, and difficulties with data and information exposure.

The majority of IoMT devices used in healthcare settings are susceptible to several cyber threats and assaults. Due to the fact that patient data is housed on the hospital's cloud server, data security is essential [28]. The most difficult challenge in the IoMT framework has been security, and choosing an algorithm that solves all issues with lightweight confidentiality is difficult. The LWC technique has been utilized for IoT in a number of disciplines, including cluster head selection, resource management, supply chain management, and crime prevention. The authors in [29] have provided a brief overview of the function of multi-criteria making decisions assessment in healthcare. For the goal of selection in IoMT, many LWC methodologies have been used. For example, the authors in [30] established a multi-criteria decision support system for dementia patients. Similar to that, multicriteria decision making analysis may be applied to contract decision-making, and tendering procedures in the healthcare industry [31].

One of the most important problems that has to be solved is authentication. The authentication model to secure IoT may be satisfied by a number of authentication mechanisms, including untraceability, perfect forward secrecy, mutual authentication, anonymity, and both cryptosystems and non-cryptosystems are employed by the authentication protocols [32]. These methods are divided into four groups: flat, hierarchical, distributed, and centralized. The following criteria and traits, such as the enrollment phase, two-way identification, offline phase, extra hardware, numerous identities, and several authentication tokens, are used to categorize these approaches. For an IoT context focused on the cloud, certain authentication mechanisms are suggested, and devices with limited resources, which are the two fundamental elements of IoMT and will be described further [33-34].

Authentication in an IoMT context focused on the cloud, and to use this cryptographic techniques, a user's device must be verified on an authorization server. Each user has their own individual secret code. Using a two-tier authentication process and the updated Diffie-Hellman mechanism, SaaS-agent handles unregistered devices. The login and password are validated at the first layer. By inputting a predetermined series of actions on a phony server interface, the user gets validated in the second layer if they are successful. The authors suggested the appropriate authentication procedures in light of the aforementioned facts. Using the three functions of user, destination server, and ID-based authentication using a server provided by an ID is demonstrated. For mutual authentication, two hash values are computed by the ID provider and sent to the user and the destination server. Elliptic Curve Cryptography is presented as a further ID-based strategy (ECC). The suggested inter-cloud authentication mechanism links all cloud servers together, and the user just needs to use one account to access them. You may find a thorough analysis of these methods in [35].

Security and privacy in the IoMT are further challenged by identity management and authentication. Identity management entails identifying the distinctive things, and authentication confirms the parties' identification relationships after that. With the Internet of Things, authentication is essential for maintaining privacy, and accessibility can be

hampered without it. If an enemy could establish their legitimacy, they would have access to all data, jeopardizing its integrity, availability, and confidentiality [36]. In the IoMT, user identification and authentication is a major problem. The most popular types of identification are password and username combinations, and parties in electronic systems authentication. The contemporary internet would face more security vulnerabilities as a result of the high rate of heterogeneity and the enormous scale of IoMT systems. Network and protocol intelligence services used for IoMT are significantly impacted by heterogeneity [37]. Security solutions must accommodate varied hardware requirements, and must provide IoT systems with authorisation and authentication. Physical constraints on communications and devices are another security concern. IoMT devices include low-power, small-area CPUs, and even the tiniest devices must adhere to Internet Protocols. IoMT device restrictions prevent information from being processed at faster than light speeds [38]. This indicates that the available memory, CPU, and energy are constrained. To reconcile the conflicting demands of robust performance and modest resource usage, difficult security forms are required. Power and size limitations have an impact on the attempts to uphold honesty, and privacy in IoMT systems [39].

An active daily living (ADL) identification framework that employs sensor data, such as that from mobile phones, and directs time-series sensor fusion processing was given by the authors of [40]. The ADL Recorder Application used patient smartphone with various intelligent sensors to capture real-time data. The location of indoor Wi-Fi, speech processing, and proximity sensor localization are the main technologies in this research, and the merging of time-series sensor data. Using the combined data from various sensors, The ADL Recognition System can accurately characterize a person's ADL and identify recurring trends in their life. Different settings have been used to improve network traffic and battery life in order to satisfy long-term requirements. The authors of [41] have created a cloud exchange and retrieval solution for medical data that is Blockchain-enabled. Each record is given a hash value, which is used to keep it safely. However, this platform does not check a participant's legitimacy, thus someone might register as a patient or doctor and continually store false information. As the system creates hash values and saves them, it also does not distinguish between diverse data forms, such as images, text, or numbers.

A Blockchain-based repository was created by the authors of [42] to share medical information with increased protection. However, there is always possibility of malfunction, which results in system inefficiency. Data latency may occur, for example, if the patient is referred to a different hospital and sees a new doctor. Individuals who aggregate the data into ledgers are not compensated in any other way. A Blockchain-based reliance on the protection for storing healthcare data has been presented in a research study [43], and mining is done using Proof of Work (PoW) methods. Data security and integrity are achieved through the use of encryption and hashing. This technique, however, does not allow for data exchange and necessitates a lot of computing power and extra time for mining. The authors of [44] described a framework for storing and transmitting healthcare data that consists of two Blockchain systems. The research demonstrates that it is superior in terms of security and record-sharing. However, it is extremely costly and impractical owing to the use of two distinct Blockchain applications.

Furthermore, there is no method for data verification in the proposed technique. A thorough analysis of the function of Blockchain in healthcare systems has also been published in [45].

Hence, it is concluded that any approaches should not sacrifice security in order to achieve high performance. Therefore, this study propose a LWC for authorization and authentication achitectureal system for Blockchain-enabled IoMT platform in accordance with joint likelihood function. When data is distributed, it creates and assigns random numbers in order to provide a secure link for data collecting. In-depth simulations are used to evaluate the proposed architecture. The suggested system supports reciprocal authentication and offers information privacy, according to results analysis.

3 Material and methods

The suggested authentication system employs a LWC mechanism for the challenge transmission and answer verification phases. The system characteristics and security level determine how many rounds are used. Then a secure connection is established after authentication. Multiple messages are sent across two nodes (that is, a sensor, a server, or an end user). The process is initiated by sending a message along with a set of encrypted identification data from one node to another. If the receiving node possesses the appropriate cipher identity information, subsequently sends the 'end' message attached with the received identity suit, agreeing to mutual authentication or concluding the contact in another manner. Authorization communications are transferred between two nodes to carry out verification in a satisfactory authentication procedure, and create a safe route. Applying the permission guidelines specified in the smart contract, this connection is then utilized to acquire additional data. Some presumptions are taken into account when conducting the trials. The following are the assumption: (i) One or more IoT devices may be owned by a user; (ii) The secret key is secured; (iii) user has an account on Ethereum; (iv) IoMT sensor, device and user are both linked to the blockchain; and (v) The user's own smart contract will be carried out. A decentralized Blockchain will be used to create a distributed smart contract framework, and to gain full system management, all users activate unique smart contracts. The proposed model framework is depicted in figure 1.

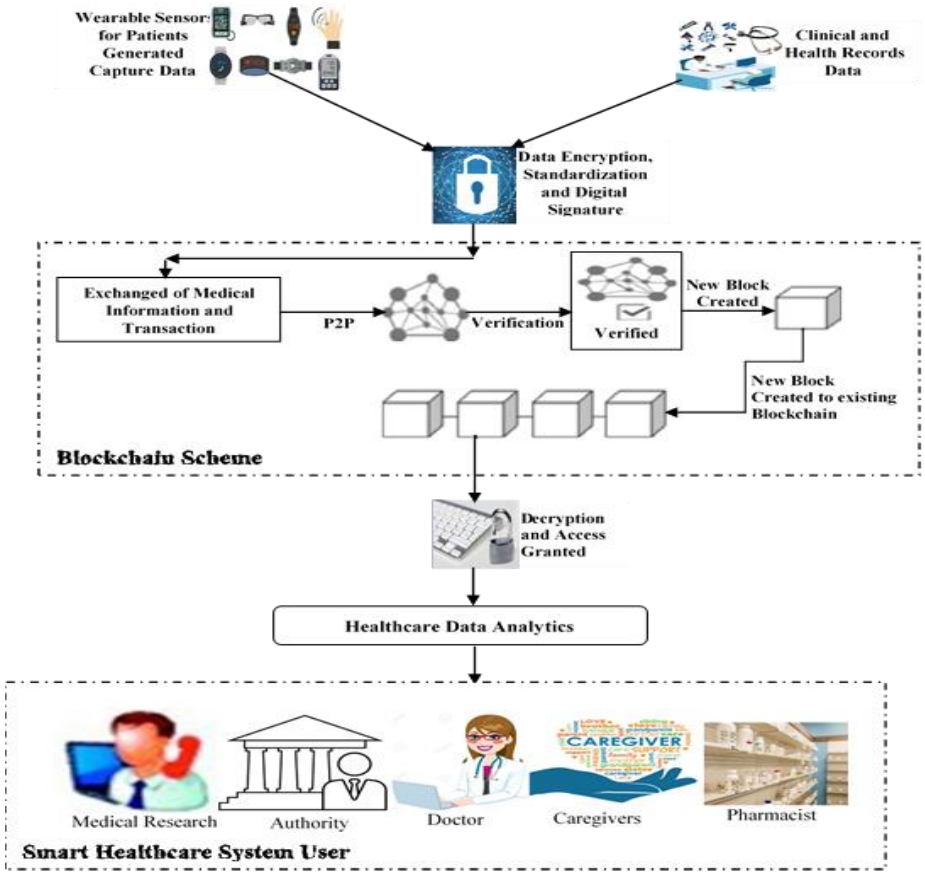

Fig. 1. The proposed Lightweight Cryptography with Blockchain-enabled IoMT-based system architecture.

3.1 Proposed Encryption and Decryption Autentication Architecture

It is anticipated that each user in the IoMT-based infrastructure with Blockchain capabilities will receive their own set of keys. Additionally, it is presumable that the authenticated user has saved data on the devices. Mutual authentication is carried out by two IoMT-based devices, X and Y. A number R_{nx} is chosen at random by X from a pool of numbers with the bounds $0 \leq R_{nx,1} \leq \log\left(id_{max/2}\right)$ where $id_{max}$the maximum length of an identification number in bits is. Following the steps outlined below, the message is encrypted with the help of Y's public key and transmitted to Y along with the selected number.

$$\textbf{Step 1}: X \rightarrow Y: \vartheta_a = E\left(PuK_y(X, R_{nx}, 1)\right)$$

ϑ_a gets the message at Y and decrypts it to determine what it is intended to say.

$$\textbf{Step 2}: \epsilon_{a,1,} R_{nx,1} \leftarrow DE_{prKy}(\vartheta_a)$$

The validation was carried out in this instance for consensual authentication. When equality is achieved, Y selects a random number R_{ny} within the range of $0 \leq R_{ny,1} \leq \log(id_{max/2})$ and answers as

$$\textbf{Step3}: \vartheta_b = E\left(PuK_x(R_{ny,1}, Y \text{ x } R_{nx})\right)$$

When X gets Y's reply, it decrypts it as

$$\textbf{Step 4}: R_{ny,} \epsilon_y \leftarrow DE_{prKx}(\vartheta_b)$$

The acceptance is contingent on ϵ_y and Y x R_{nx} being equal. X calculates the response and transmits it to Y if it is approved.

$$\textbf{Step 5}: \vartheta_c = E\left(PuK_y(X, R_{ny,1}, R_{nx,2})\right)$$

where $R_{nx,2}$ is constrained to be within the range $0 \leq R_{ny,1} \leq \log(id_{max/2})$. Up to the $(n-1)th$ message transmission, X and Y interact through challenge and answer exchanges. When X gets the $(n+1)th$ message, it decrypts the message and gathers the following information.

$$\textbf{Step 6}: \left(R_{ny,z,} \epsilon_{y,z}\right) \leftarrow DE_{prKx}(\vartheta(n-1))$$

In this case, if $\epsilon_{y,z} = Y$ x $R_{ny,z}$, X calculates the answer ϑ_b and transmits it to Y as follows:

$$\textbf{Step 7}: \vartheta_n = E\left(PuK_y(X, R_{nx}, z, 0)\right)$$

Y decrypts the message and receives the following:

$$\textbf{Step 8}: \left(\epsilon_{y,z+1}\right) \leftarrow DE_{prKy}(\vartheta_n)$$

Next looks for

$$\textbf{Step 9}: \left(\epsilon_{y,z+1}\right) = \left(X, R_{ny,z}\right) \,\&\, \tau = 0$$

If the aforementioned requirements are met, the related devices have successfully verified one another or have failed in some other way. The reciprocal authentication mechanism in the suggested framework uses n-passes. The system characteristics and encryption algorithm's security level both affect the value of n. Notably, the suggested framework is preferred to have a 64-bit security level. Then, X and Y choose two numbers from $R_{nx}\ and\ R_{ny}$ at random that are associated by the formula $\log R_{nx}\ and\ \log R_{ny} = 64$. Three passes through these steps are required for mutual device authentication.

4 Results and Discussion

The proposed system make used of Hyperledger Calliper as a tool for the blockchain network. It is compatible with a variety of Hyperledger architectures, including Fabric, Composer, Sawtooth, Iroha, and others. Moreover, the proposed model implemented WLC for encryption and decryption to provide a secure, lightweight encryption mechanism. The Calliper tool is crucial to this presented study's verification and implementation of the framework and numerous parameters. The parameters in Calliper tool includes encryption and decryption times, Latency, throughput, and computational cost are some of the parameters. The configuration parameters in the experimental setup are

changed in accordance with evaluation, including update, add, delete, and revoke policies, as well as block size, block time, endorsement policy, channel, and keyword search.

The amount of time needed to retrieve outcomes and reflect them on the interactive platform is known as read latency. 100 transactions' initial read latency is recorded for analysis, then, 500 transactions were used fot the performance of the proposed system to get results. The read throughput and read latency statistics for 500 transactions are shown in Figures 2 and 3, accordingly. The graph's trend indicates that there are more transactions per second as time goes on. The time needed to read data from each block increases as the number of transactions rises, and as a result, the linear curve is produced. The volume of transactions affects the throughput of the proposed Blockchain model. When the results were analyzed, it has been found that the system's throughput grows as the number of transactions does.

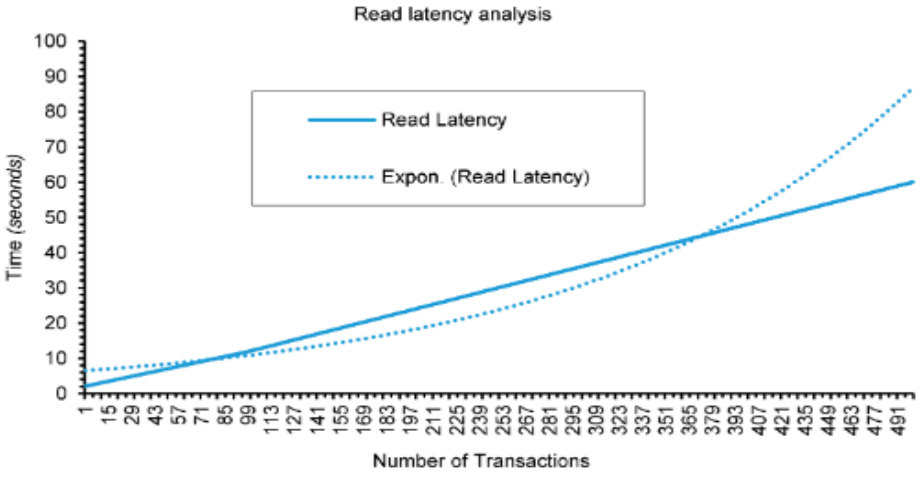

Fig. 2. Latency analysis for 500 transactions.

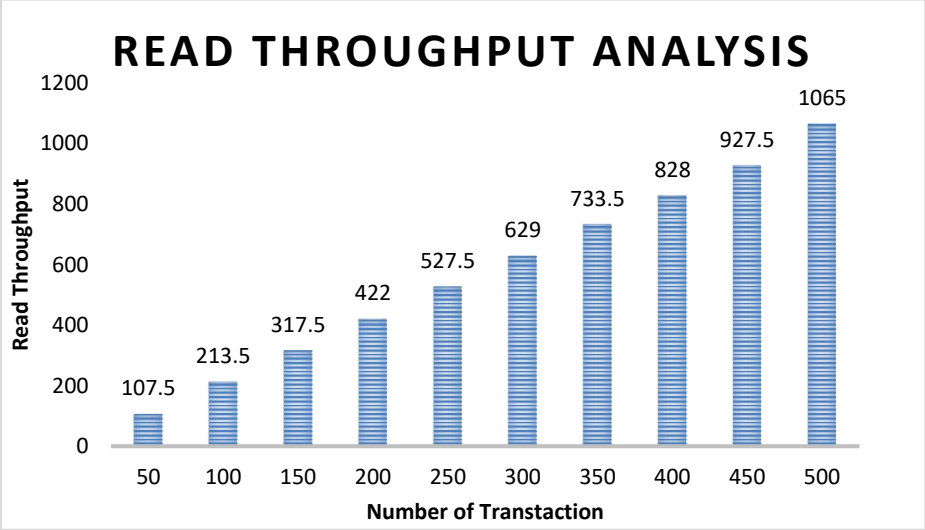

Fig. 3. Throughput for 500 transactions in the Blockchain.

The duration needed to confirm a transaction is known as transaction latency. It may be estimated by taking the confirmation time out of the submission time. The size of a transaction affects transaction delay. Additionally, a larger transaction requires more resources to process, which adds to the latency. The size of the transaction affects transaction delay. Figure 4 clearly shows that the system's throughput grows with time, this indicates that the volume and frequency of transactions affect the throughput of the proposed Blockchain technology.

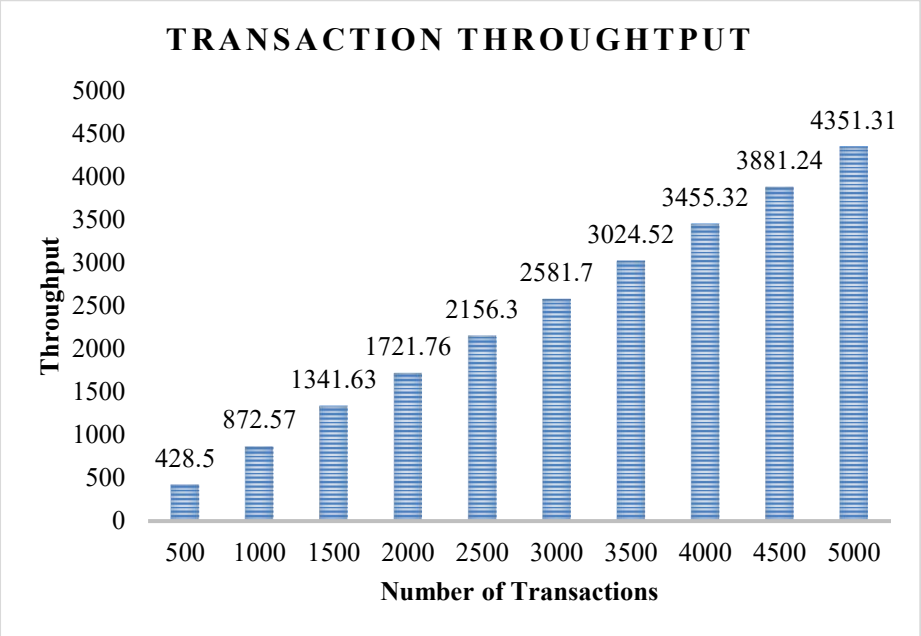

Fig. 4. Throughput for 500 transactions.

4.1 The comparison of both encryption and decryption performance

Table 1 show the results of IoMT-based patients data LWC encryption performance, the performance metrics are computing time, computing memory, processor consumption and power consumption respectively. The same size of patient data plaintext was encrypted (500kb), the patient data plaintext comprises age, blood group, sickness, diseases diagnosed, medical laboratory reports and so on.

Table 1. Cryptography encryption performance

Data Size	Cryptography	Computation time (s)	Computing memory (kb)	Processor Consumption (%)	Battery Consumption (w)	Accuracy (%)
500kb	AES	0.025	2.37	0	1.56E-05	94%
	RSA	5.487	2.08	0.7	0.004141	73%
	AESRSA	5.502	4.17	0.7	0.005091	70%
	Lightweight	0.261	1.35	0.3	1.29E-07	98%

Table 2 show the results of IoMT-based patients data LWC decryption performance, the performance metrics are computing time, computing memory, processor consumption and power consumption respectively. The same size of patient data plaintext was encrypted (500kb). The results show that the proposed LWC lgorithms perform better across the performance metrics used.

Table 2. Cryptography decryption performance

Data Size	Cryptography	Computation time (s)	Computing memory (kb)	Processor Consumption (%)	Battery Consumption (w)	Accuracy (%)
500kb	AES	0.022	2.32	0	1.50E-05	93%
	RSA	5.48	2.03	0.6	0.00411	75%
	AESRSA	5.480	4.03	0.6	0.00502	73%
	Lightweight	0.269	1.27	0.3	1.25E-07	97.5%

4.2 Resiliency of Authentication and authorization

The associated keys and matching mote IDs are believed to be reliably pre-configured. Assume that R_n, the chosen random number, has m bits. The level of security is therefore $(R_n - 1)m/2$ bits. The encryption strategy is a foundational component of the proposed mutual authentication framework. Random numbers are used for mutual authentication between devices, as was previously mentioned. So, in order to fake a legitimate device, an eavesdropper needs to produce legitimate messages. The eavesdropper, however, is unable to produce legitimate signals since they lack knowledge of random numbers. The results of the investigation demonstrate how secure the suggested encryption method is in comparison to others. Additionally, it defends against MITM and impersonator threats.

5 Conclusion and future Scope

Recently, exciting research is being conducted in a number of domains, including healthcare, using LWC and Blockchain technologies. One of the most dynamic areas of Blockchain research is the integration of healthcare with IoT. The health sector manages a vast volume of data that must be analyzed systematically. The digitalization of clinical records is a developing trend. The smart contract has the potential to be used in many Blockchain applications in the future to obtain the best performance. Blockchain-based technologies for maintaining the ledger have been the subject of substantial research, particularly in the field of healthcare systems. Very few of these use cases, however, addressed vital infrastructures that contained delicate data and systems as assets. While blockchains like Ethereum offer their users significant levels of privacy, integrity, and greater transparency, there still significant privacy and security hazards associated with their use in critical areas like IoMT-based systems. Several blockchains do have these privacy problems because one of their key design tenets is the distribution of ledgers. Consequently, with all the extra security and privacy capabilities, thus, any blockchain framework's performance should be thoroughly examined before being used in latency-sensitive settings. Therefore, this paper proposed a hybrid model using LWC enabled Blockchain technology for IoMT-based platforms to protect the patients' medical data. The suggested approach deals with the issue of reciprocal authenticity and permission and offers a creative solution. The findings of the measuring performance and data analysis show that the suggested approach boosts security while processing data more quickly and with less communication overhead. Future work will consider using a better security algorithm like scalable encryption, intrusion detection model with blockchain to further secure the IoMT-based systems. Future work will attempt to assess the proposed system's hardware in a practical environment.

References

1. Tahir, M., Sardaraz, M., Muhammad, S., & Saud Khan, M. (2020). A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics. *Sustainability*, *12*(17), 6960.
2. Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network. *Sensors*, *22*(2), 572.
3. Awotunde, J. B., Misra, S., Ayoade, O. B., Ogundokun, R. O., & Abiodun, M. K. (2022). Blockchain-Based Framework for Secure Medical Information in Internet of Things System. *EAI/Springer Innovations in Communication and Computing*, 2022, pp. 147–169. Springer, Cham.
4. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure ehrs sharing of mobile cloud based e-health systems. *IEEE access*, *7*, 66792-66806.
5. Vaiyapuri, T., Binbusayyis, A., & Varadarajan, V. (2021). Security, privacy and trust in IoMT enabled smart healthcare system: a systematic review of current and future trends. *International Journal of Advanced Computer Science and Applications*, *12*(2).
6. Egala, B. S., Pradhan, A. K., Badarla, V., & Mohanty, S. P. (2021). Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet of Things Journal*, *8*(14), 11717-11731.

7. Kim, S. K., & Huh, J. H. (2020). Artificial neural network blockchain techniques for healthcare system: Focusing on the personal health records. *Electronics*, *9*(5), 763.
8. Ogundokun, R. O., Arowolo, M. O., Misra, S., & Awotunde, J. B. (2022). Machine Learning, IoT, and Blockchain Integration for Improving Process Management Application Security. EAI/Springer Innovations in Communication and Computing, 2022, pp. 237–252. Springer, Cham.
9. Awotunde, J. B., Chakraborty, C., & Folorunso, S. O. (2022). A Secured Smart Healthcare Monitoring Systems Using Blockchain Technology. In *Intelligent Internet of Things for Healthcare and Industry* (pp. 127-143). Springer, Cham.
10. Katagi, M., & Moriai, S. (2008). Lightweight cryptography for the internet of things. *sony corporation*, *2008*, 7-10.
11. Hassan, A. (2020, November). Lightweight Cryptography for the Internet of Things. In *Proceedings of the Future Technologies Conference* (pp. 780-795). Springer, Cham.
12. AbdulRaheem, M., Balogun, G. B., Abiodun, M. K., Taofeek-Ibrahim, F. A., Tomori, A. R., Oladipo, I. D., & Awotunde, J. B. (2021, October). An enhanced lightweight speck system for cloud-based smart healthcare. In *International Conference on Applied Informatics* (pp. 363-376). Springer, Cham.
13. Ning, L., Ali, Y., Ke, H., Nazir, S., & Huanli, Z. (2020). A hybrid MCDM approach of selecting lightweight cryptographic cipher based on ISO and NIST lightweight cryptography security requirements for internet of health things. *IEEE Access*, *8*, 220165-220187.
14. Ogundokun, R. O., Awotunde, J. B., Adeniyi, E. A., & Ayo, F. E. (2021). Crypto-Stegno based model for securing medical information on IOMT platform. *Multimedia tools and applications*, *80*(21), 31705-31727.
15. Jan, M. A., Cai, J., Gao, X. C., Khan, F., Mastorakis, S., Usman, M., ... & Watters, P. (2021). Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions. *Journal of Network and Computer Applications*, *175*, 102918.
16. Rahmani, M. K. I., Shuaib, M., Alam, S., Siddiqui, S. T., Ahmad, S., Bhatia, S., & Mashat, A. (2022). Blockchain-Based Trust Management Framework for Cloud Computing-Based Internet of Medical Things (IoMT): A Systematic Review. *Computational Intelligence and Neuroscience*, *2022*.
17. Adeniyi, E. A., Ogundokun, R. O., Misra, S., Awotunde, J. B., & Abiodun, K. M. (2022). Enhanced Security and Privacy Issue in Multi-Tenant Environment of Green Computing Using Blockchain Technology. In *Blockchain Applications in the Smart Era* (pp. 65-83). Springer, Cham.
18. Abdulraheem, M., Awotunde, J. B., Jimoh, R. G., & Oladipo, I. D. (2020, November). An efficient lightweight cryptographic algorithm for IoT security. *Communications in Computer and Information Science*, 2021, 1350, pp. 444–456. Springer, Cham.
19. Shah, A. A., Piro, G., Grieco, L. A., & Boggia, G. (2019, June). A qualitative cross-comparison of emerging technologies for software-defined systems. In *2019 Sixth International Conference on Software Defined Systems (SDS)* (pp. 138-145). IEEE.
20. Mukherjee, A., Ghosh, S., Behere, A., Ghosh, S. K., & Buyya, R. (2021). Internet of Health Things (IoHT) for personalized health care using integrated edge-fog-cloud network. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1), 943-959.
21. Ferrag, M. A., Maglaras, L., & Derhab, A. (2019). Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends. *Security and Communication Networks*, *2019*.

22. Awotunde, J. B., Ayoade, O. B., Ajamu, G. J., AbdulRaheem, M., & Oladipo, I. D. (2022). Internet of Things and Cloud Activity Monitoring Systems for Elderly Healthcare. In *Internet of Things for Human-Centered Design* (pp. 181-207). Springer, Singapore.
23. Li, S., Xu, L. D., & Zhao, S. (2015). The internet of things: a survey. *Information systems frontiers*, *17*(2), 243-259.
24. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, *17*(3), 1294-1312.
25. Gou, Q., Yan, L., Liu, Y., & Li, Y. (2013, August). Construction and strategies in IoT security system. In *2013 IEEE international conference on green computing and communications and IEEE internet of things and IEEE cyber, physical and social computing* (pp. 1129-1132). IEEE.
26. Ma, Z., Shang, X., Fu, X., & Luo, F. (2013, November). The architecture and key technologies of Internet of Things in logistics. In *International conference on cyberspace technology (CCT 2013)* (pp. 464-468). IET.
27. Awotunde, J. B., Jimoh, R. G., Folorunso, S. O., Adeniyi, E. A., Abiodun, K. M., & Banjo, O. O. (2021). Privacy and security concerns in IoT-based healthcare systems. Internet of Things, 2021, pp. 105–134. Springer, Cham.
28. Rani, S. S., Alzubi, J. A., Lakshmanaprabu, S. K., Gupta, D., & Manikandan, R. (2020). Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers. *Multimedia Tools and Applications*, *79*(47), 35405-35424.
29. Frazão, T. D., Camilo, D. G., Cabral, E. L., & Souza, R. P. (2018). Multicriteria decision analysis (MCDA) in health care: a systematic review of the main characteristics and methodological steps. *BMC medical informatics and decision making*, *18*(1), 1-16.
30. Dimitrioglou, N., Kardaras, D., & Barbounaki, S. (2017, July). Multicriteria evaluation of the Internet of Things potential in health care: The case of dementia care. In *2017 IEEE 19th Conference on Business Informatics (CBI)* (Vol. 1, pp. 454-462). IEEE.
31. Drake, J. I., de Hart, J. C. T., Monleón, C., Toro, W., & Valentim, J. (2017). Utilization of multiple-criteria decision analysis (MCDA) to support healthcare decision-making FIFARMA, 2016. *Journal of market access & health policy*, *5*(1), 1360545.
32. Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2017). Authentication protocols for internet of things: a comprehensive survey. *Security and Communication Networks*, *2017*.
33. Ma, Z., Shang, X., Fu, X., & Luo, F. (2013, November). The architecture and key technologies of Internet of Things in logistics. In *International conference on cyberspace technology (CCT 2013)* (pp. 464-468). IET.
34. Castellani, A. P., Bui, N., Casari, P., Rossi, M., Shelby, Z., & Zorzi, M. (2010, March). Architecture and protocols for the internet of things: A case study. In *2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)* (pp. 678-683). IEEE.
35. Saadeh, M., Sleit, A., Qatawneh, M., & Almobaideen, W. (2016, August). Authentication techniques for the internet of things: A survey. In *2016 cybersecurity and cyberforensics conference (CCC)* (pp. 28-34). IEEE.
36. Awotunde, J. B., Folorunso, S. O., Bhoi, A. K., Adebayo, P. O., & Ijaz, M. F. (2021). Disease diagnosis system for IoT-based wearable body sensors with machine learning algorithm. In *Hybrid Artificial Intelligence and IoT in Healthcare* (pp. 201-222). Springer, Singapore.

37. Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A. (2018). Secure medical data transmission model for IoT-based healthcare systems. *Ieee Access*, *6*, 20596-20608.
38. Shackelford, S. J., Mattioli, M., Myers, S., Brady, A., Wang, Y., & Wong, S. (2018). Securing the Internet of healthcare. *Minn. JL Sci. & Tech.*, *19*, 405.
39. Abiodun, M. K., Awotunde, J. B., Ogundokun, R. O., Adeniyi, E. A., & Arowolo, M. O. (2021). Security and information assurance for IoT-based big data. *Studies in Computational Intelligence*, 2021, 972, pp. 189–211. Springer, Cham.
40. Wu, J., Feng, Y., & Sun, P. (2018). Sensor fusion for recognition of activities of daily living. *Sensors*, *18*(11), 4029.
41. Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. *Journal of medical systems*, *43*(1), 1-9.
42. Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). Medblock: Efficient and secure medical data sharing via blockchain. *Journal of medical systems*, *42*(8), 1-11.
43. Li, H., Zhu, L., Shen, M., Gao, F., Tao, X., & Liu, S. (2018). Blockchain-based data preservation system for medical data. *Journal of medical systems*, *42*(8), 1-13.
44. Zhang, A., & Lin, X. (2018). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of medical systems*, *42*(8), 1-18.
45. Zubaydi, H. D., Chong, Y. W., Ko, K., Hanshi, S. M., & Karuppayah, S. (2019). A review on the role of blockchain technology in the healthcare domain. *Electronics*, *8*(6), 679.