A Secure Cloud Storage System for Iot Assisted Healthcare Environment by Employing Blockchain with Asymmetric Encryption

Aadhinarayanan. N.V[1], P.Vijayakumar[2]

[1]Research Scholar, Department of Computer Science, Government Arts and Science College (Modakurichi), Affiliated to Bharathiar University, Coimbatore, Tamil Nadu(St), India
[2]Assistant Professor, Department of Computer Science, Bharathiar University ,Coimbatore, Tamil Nadu(St), India

Received: 13.07.2024 Revised: 10.08.2024 Accepted: 15.09.2024

ABSTRACT
The emergence of new technologies like the Internet of Things (IoT) is accompanied by explosive growth in the healthcare sector. The main idea behind using IoT in healthcare facilities is to make it remotely accessible, facilitating easier communication between physicians and patients and the ability to diagnose any illness remotely in an emergency. However, when it comes to data sharing and outsourcing in the cloud, the confidentiality and integrity of medical records become crucial concerns. Hackers can breach health data without users' consent, exposing private patient information. Therefore, this article suggests using blockchain-enabled ciphertext policy-attribute-absorption (ECP-ABE) to store and access IoT healthcare data securely. Using ECP-ABE, the patient's data is encrypted before being safely transmitted to the cloud. Here, the Sine chaotic map with a Wedding dance coefficient-based Whale Optimization Algorithm (SWWOA) creates the access structure in the best possible way. The encrypted data is then securely stored in the cloud via a blockchain. Tests indicate that the strategy—which merges blockchain with encryption—can guarantee both the high throughput of medical information access and the safe storage and integrity of that data.

Keywords: Internet of things, Access Control, Secure Data Encryption, Cloud Computing, Blockchain technology.

1. INTRODUCTION

The IoT is a new technology that helps users by enabling information exchange between devices connected to the web. The International Telecommunication Union defines the IoT as a network of devices with sensors that communicate with their surroundings. The IoT has expanded to include various applications utilized in various contexts, including security, remote monitoring, controlling electrical appliances, military use, and other electronic equipment [1]. IoT device adoption in the healthcare sector is increasing. By 2025, the healthcare IoT market is anticipated to grow to 135.87 billion dollars [2]. IoT-based wearable solutions may benefit pharmaceutical companies by reducing the need for clinical screening via more efficient data collection methods. Additionally, cloud computing is extending the IoT to provide new facilities and applications for the healthcare process [3, 4]. IoT technology constantly supports the cloud to improve performance in areas like computing power, energy efficiency, storage capacity, and high resource utilization. As IoT-based solutions are introduced, people's lives increasingly rely on technology. A substantial amount of employee data, encompassing their actions and medical status, will be collected and analyzed [5]. Because IoT devices are often vulnerable to security breaches, it is crucial to ensure IoT security [6].

One of the better uses for remote electronic healthcare systems is the well-liked field of telecare medical information systems (TMIS). To help with medical diagnosis and medical record preservation, the TMIS application can be integrated with a cloud-based assistive cognitive-aware e-healthcare system. Data fabrication poses serious risks, so it should be maintained confidential to protect patient privacy and facilitate easy access. As a result, a hot topic for wireless channel access in TMIS is secure data transmission [7]. A feasible approach is to encrypt the data prior to transferring it to cloud servers. If conventional security measures fail, the only version of the data that attackers may access is an encrypted copy. All data must be secured at its origin and made available solely to authorized users to guarantee data security when sharing. Traditional symmetric and asymmetric encryption schemes are inappropriate for providing fine-grained access control; however, they may be applied in scenarios where all information readers the data owner has authorized receive the key for decryption. [8]. From now on, the suggested system encrypts IoT healthcare data using the ECP-ABE technique, which is safe since the encrypted data comprises attributes rather than actual data.

Additionally, blockchain-based cloud storage has recently been implemented to preserve and secure medical data since it is especially susceptible to vulnerabilities and attacks, including tampering forgeries and privacy breaches [9, 10]. A chain of blocks connected by a Merkle tree cryptographic hash makes up a blockchain. It is a repository for all transaction records kept on file in each block's database [11]. This aims to present a novel secure data storage solution and use the blockchain-enabled ECP-ABE technique to access IoT healthcare data. The system uses the ECP-ABE approach to encrypt patient IoT data to transmit to the cloud securely. The outcomes confirm the effectiveness of our proposed scheme over other related methods.

The remainder of the document is systematized as follows: The current works about our proposed work are listed in Section 2. A short-term summary of the suggested methodology is provided in Section 3. Additionally, the performance analysis of the suggested work using existing methods and some assessment measures is shown in Section 4. Section 5 wraps up the suggested improvements and offers some future directions.

2. RELATED WORKS

Kristtopher Kayo Coelho et al. [12] suggested a secure healthcare system for IoT environment using Low memORysymmEtric-key geNerAtion (LORENA). In assessing security performance to couple out the patient's electrical signals, the LORENA assessed the creation of each unique secret key. The findings showed that the approach worked better than the existing methods in minimizing communication costs throughout the critical agreement procedure and utilized memory by about 76%. Yaru Liu et al. [13] recommended a secure IoT healthcare system using dynamic, searchable symmetric encryption. Initially, the honest IoT gateway included the gathered data of the patients into personal health records files in a periodic manner. Subsequently, the IoT gateway built a secure index and encrypted every file's attribute value. The encrypted PHR files and the secure index were then uploaded to the cloud server. Subsequently, the cloud server executed search functions by utilizing the secure index. It then determined whether the user could access the matched files' characteristics. The system's efficiency and security were demonstrated through trials and security analysis, even with a 4.35ms access time.

An optimal security strategy for Internet of Things devices was given by Andreas Andreou et al. [14]. The owner's requirements and the regulations governing restrictions about the degree of confidentiality would determine how the data was dispersed in pieces. The distribution unit adjusts the privacy level to distribute portions to multiple servers while maintaining security. As a result, cloud storage service providers committed to establishing suitable service and confidentiality levels in the service level agreement. Following that, different cloud data stores were used to spread dataset fragments. MouradeAzrour et al. [15] proffered a hashing-based authentication scheme to authorize healthcare users in IoT. Based on the Scyther tool, experimental tests were conducted to determine that the system met security standards and could withstand known assaults. Faris A. Almalki and Ben Othman Soufiene [16] presented a secure authentication system using homomorphic encryption. The patients used wearable sensor devices, and their role was to report the sensed health data to the aggregator. In order to stop hostile nodes from entering the network, the aggregator verified the legality of any medical sensors desiring to connect with it before computing the aggregation on them. Homomorphic encryption served as the basis for the encryption procedure. According to security analysis and experimental results, the solution ensure data privacy, message authenticity, and integrity with minimal computing overhead and 0.6ms of processing time.

The works above show better outcomes and provide better security; however, they suffer from the following limitations. The problem of data security must be considered while putting this service into practice because a breach could endanger someone's life. Therefore, safe transfer of the data—that is, patient health information—to approved physicians and other healthcare professionals is necessary, as is secure data storage on a semi-trusted cloud server. Some authors used a faster symmetric algorithm, which provides less security than the asymmetric one. Attribute-based encryption (ABE) algorithm is a family of secure asymmetric algorithms. However, the processing and storage cost of decryption and encryption is associated with the number of traits in the policy in most ABE methods now in use. Therefore, lowering the overhead associated with computation and storage is crucial to increase the method's efficacy. Hence, our method uses the CP-ABE approach, which optimizes the access structure using SWWOA.

3. PROPOSED METHODOLOGY

This study recommends a blockchain-enabled ECP-ABE method for secure data monitoring for IoT-based healthcare platforms. The model initially uses ECP-ABE to encode the collected IoT data, in which the access structure is optimally created using SWWOA. Next, these encrypted data are securely transmitted and stored in the cloud using blockchain. At last, if the user wants the stored data files, the decryption process is carried out using the same ECP-ABE algorithm. The flow of the proposed methodology is shown in Fig. 1.

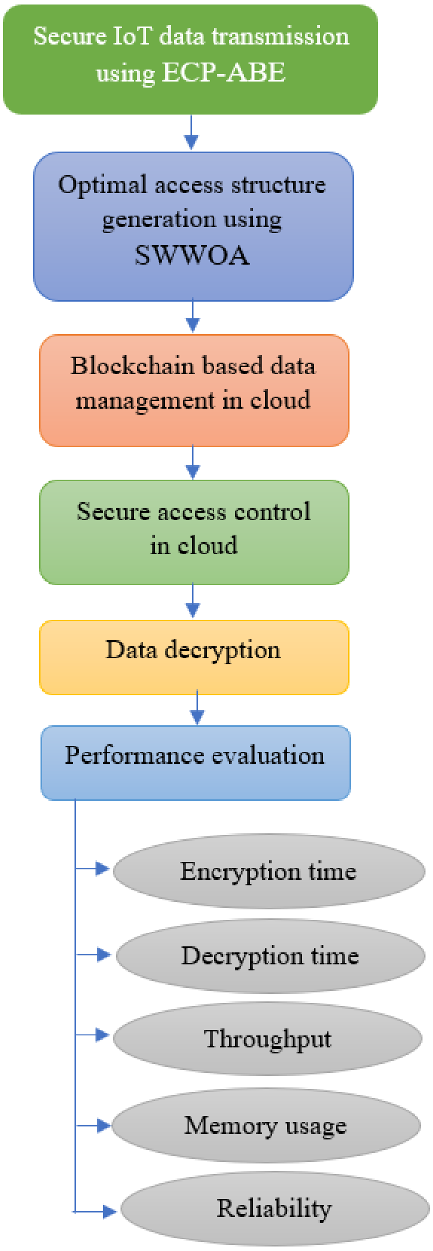

Secure IoT data transmission using ECP-ABE
Optimal access structure generation using SWWOA
Blockchain based data management in cloud
Secure access control in cloud
Data decryption
Performance evaluation
Encryption time
Decryption time
Throughput
Memory usage
Reliability

Figure 1: Proposed methodology's workflow

3.1 Secure Data Encryption

Every patient has an assortment of wearables with embedded sensors and IoT medical devices. These sensors can be used to track sleep patterns, measure physical activity, and take a variety of vital indicators. These gadgets are meant to gather and share health information with the medical staff. However, this has brought to light the severe security issue of protecting and preventing illegal access to cloud-based IoT data. The suggested solution makes use of ECP-ABE to safeguard the cloud patient data. A cryptographic system called CP-ABE can achieve safe data sharing and is appropriate for cloud storage. A user may have more than one attribute in a CP-ABE system, and numerous users may share the same attribute simultaneously. As a result, numerous users that share the property can share its decryption key. The problem is that each encryption round produces a unique access structure. Selecting these access structures at random increases processing overhead and introduces security issues. Using a SWWOA algorithm, the access structure is appropriately chosen to improve system security and reduce calculation time. Therefore, ECP-ABE refers to the improvisation in traditional CP-ABE. The four sub-basic algorithms comprise this system: key generation, encryption, set-up, and decryption.

a) Setup phase

The setup process uses A security parameter as input, which delivers a master and a public key. Both will be used as the algorithm's input for generating keys. In this setup algorithm, the public key generated by attribute authority will be created using bilinear pairing. Consider two multiplicative cyclic groups $A_1^{''}$ and $A_2^{''}$ of prime order$P^{''}$, public security parameter $C_k^{''}$ and the bilinear map $\acute{B}: A_1^{''} \times A_1^{''} \to A_2^{''}$, which includes the below two properties:

Bi-Linearity: For all $x, y \in A_1^{''} and u, v \in Z_{p^{''}}$, we have

$$\acute{B}(x^u, y^v) = \acute{B}(x, y)^{uv}$$

Non-degeneracy: $\acute{B}\left(C_k^{''}, C_k^{''}\right) \neq 1$

The public UP_{Key} and a master secret key UM_{key} are made using the security parameter$\left(C_k^{''}\right)$.

b) Access structure creation

The next step is to create the access structure, which lists all of the ciphertexts the key holder can decipher. The user registers with a trusted authority before creating an access structure to prevent unauthorized users from logging in. During the registration phase, customers provided their data center information. Initially, everything of the user's information—password, user name, user ID, and so on—is generated by the client and is regarded as a set of characteristics and it is defined as$\left(\underline{SA}_s\right)$. Next, the access structure is optimally designed using the SWWOA in the proposed system to improve system security. A new optimization technique for resolving optimization issues is the Whale Optimization Algorithm (WOA). In order to find the global optimal solution, the algorithm mimics the flight and mating behaviors of mayflies to do both local and global searches. Nevertheless, the conventional WOA exhibits premature convergence behavior because of an inadequate trade-off between the exploitation and exploration components, low convergence precision, poor stability, and a propensity to become caught in local optimality. In order to boost diversity, prevent premature convergence, and initiate the moth population, the suggested technique employs a sine chaotic map. Additionally, the Wedding Dance Coefficient (WDC) will improve the convergence accuracy by increasing the local search ability with the number of iterations to identify the global optimal solution more quickly and accurately. Therefore, SWWOA is the new moniker for these modifications to traditional WOA.

Step 1: To begin, initialize the population of whales by using a chaotic map. It is another type of chaotic map that effectively improves the initialized population, calls between [0, 1]. It is mathematically defined by,

$$\hat{Z} \leftrightarrow_w (\tau + 1) = f\left(\hat{Z} \leftrightarrow_w (\tau), \varphi\right) \left(\nu \arcsin \arcsin\sqrt{\hat{Z} \leftrightarrow_w (\tau)}\right)_{\sin} \quad (1)$$

Where, $\hat{Z} \leftrightarrow_w (\tau + 1)$ refers to the position of the w^{-th} whale at the τ^{-th} iteration, φ and $\nu$are taken 1 and 0.5.

Step 2: The whales then locate their prey's position and encircle them. The WOA algorithm assumes that the target prey is the current optimal individual position because the optimal position in the search space is unknown beforehand. Other individuals then update their positions by moving closer to the prey, resulting in the whales constantly approaching it according to equations (4) and (5).

$$\hat{Z} \leftrightarrow_w (\tau + 1) = \hat{Z} \leftrightarrow_w^* (\tau) - E.F \quad (2)$$

$$F = \left|\rho^{\leftrightarrow} .\ \hat{Z} \leftrightarrow_w^* (\tau) - \hat{Z} \leftrightarrow_w (\tau)\right| \quad (3)$$

$$E = 2.\hat{\chi}.\widetilde{R}_j - \hat{\chi} \quad (4)$$

$$\rho^{\leftrightarrow} = 2.\widetilde{R}_j \quad (5)$$

Where, $\hat{Z} \leftrightarrow_w^*$ refers to the historically best position, $\hat{Z} \leftrightarrow_w (\tau)$ denotes a whale position of w^{-th}whale at τiteration, Findicates the distance between the random and current individual of the population, $E$and $\rho^{\leftrightarrow}$ signifies the coefficients, $\hat{\chi}$ decreased linearly from 2 to 0, and $\widetilde{R}_j$ represents an arbitrary number in the range of [0, 1].

Step 3: The spiral equation that was developed between the victim's position and the whale's position is what comes next to replicate the whale's movement. It looks like this:

$$\hat{Z} \leftrightarrow_w (\tau + 1) = F^{''}.\ e^{\mu\lambda}.\ \cos\cos(2\pi\lambda) + \hat{Z} \leftrightarrow_w^* (\tau) \quad (6)$$

$$F^{''} = \left|\hat{Z} \leftrightarrow_w^* (\tau) - \hat{Z} \leftrightarrow_w (\tau)\right| \quad (7)$$

Where, F''refers to the distance between the current optimal position and w^{-th} whale, $\lambda$is an arbitrary number ranges between [− 1, 1], andα is a constant coefficient that describes the logarithmic spiral form.

Step 4: Then, to get the global optimum values updating has been done with WDC agent rather than the best agent. The agent is forced to move away from this location in the exploration phase using $1 < E < -1$. The exploration step of the model is mathematically expressed using equations (10) and (11).

$$\hat{Z} \leftrightarrow_w (\tau + 1) = \hat{Z} \leftrightarrow_{Rand} (\tau) - E.F + \underline{WD}^{\tau} \quad (8)$$

$$F = \left|\rho^{\leftrightarrow} . \hat{Z} \leftrightarrow_{Rand} (\tau) - \hat{Z} \leftrightarrow_w (\tau)\right| \quad (9)$$

Where, $\hat{Z} \leftrightarrow_{Rand}$ is whale's position vector that is selected at random, and $\underline{WD}^{\tau}$signifies the WDC at timeτthat protects the algorithm from the problem of local optima and should be increased gradually in each iteration and this can be computed as follows:

$$\underline{WD}^{\tau} = \underline{WD}^{1} * \gamma_1^{\tau}, \quad 0 < \gamma_1 < 1 \quad (10)$$

Where, $\underline{WD}^{\tau}$signifies the attenuation parameter. This process continues until to obtain the optimum solution (optimal access structure(OA_s^{**})).

c) Key generation

The private key of the model is generated by considering master key(UM_{key}), public key(UP_{Key}), and a set of attributes$(\underline{SA}_s)$. It is formulated as follows;

$$UR_{key} = \{UP_{Key}, UM_{key}, \underline{SA}_s\} \quad (11)$$

d) Encryption

Each user can encrypt their shared resources and upload them to the cloud server. The patient's data$(\underline{ID}_s)$is encrypted using the public key$(UP_{Key})$and the optimal structure$(OA_s^{**})(OA_s^{**})$ generated using SWWOA and the encrypted data or a cipher data (CT''_{text}) is stored in cloud for unauthorized access. If any user wants to access this encrypted data, they must satisfy the optimal access policy.

3.2 Blockchain based Data management

Subsequently, the encrypted data are kept in cloud settings at the data management stage, where they efficiently facilitate read-write storage operations. We should conceal the access policy from the cloud server since, in a real-world situation, it is an inquisitive yet honest cloud server. As a result, the suggested solution adds more security by securely keeping the encrypted data in the cloud using the blockchain technique. Blockchain is a distributed database with transparency, security, and decentralized features. Blockchain, a decentralized database, offers a solid answer to the issues of inadequate security, low efficacy, and poor sharing in medical data management.

It maintains an ever-expanding list of sorted records called blocks. These blocks are linked using cryptography; everyone has transactional data, a timestamp, and a cryptographic hash of the preceding block. After that, these blocks are kept on nodes resembling tiny servers. A peer-to-peer network, made up of all the nodes on a blockchain, allows the nodes to communicate constantly and share the most recent information on the network, keeping all nodes up to date. The nodes hold an entire copy of the distributed ledger and ensure the accuracy of the data they store. The network as a whole also helps to guarantee the security and dependability of the transactions.

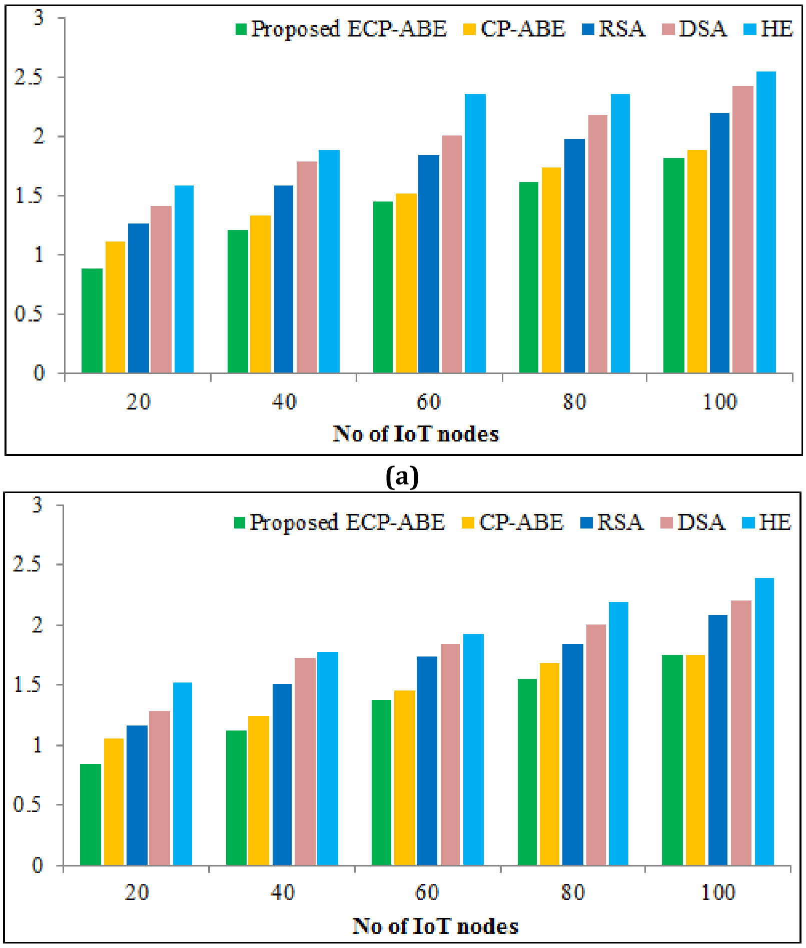
3.3 Data Decryption

The encrypted data $(CT''_{text})$is decrypted by providing optimal access structure $(OA_s^{**})$and private key(UR_{key}), which are expressed using eqn. (14).

$$(\underline{ID}_s) \rightarrow \{UR_{key}, CT''_{text}, OA_s^{**}\} \quad (12)$$

4. RESULTS AND DISCUSSION

Here, the effectiveness of the suggested study is tested and compared against some related encryption methods such as CP-ABE, Rivest Shamir Adelman (RSA), Digital Signature Algorithm (DSA), and Homomorphic Encryption (HE) regarding some indicators like encryption time, decryption time, memory usage, throughput, and reliability. The proposed system is implemented in the working platform of the NS2 network simulator. The simulation is done within the range of 500 × 500 m, and the number of IoT nodes considered is 20 to 100 respectively. Fig. 2 demonstrates the outcomes of the ECP-ABE and related existing models in terms of (a) encryption and (b) decryption time. For 20 nodes, the existing HE offers encryption and decryption time of 1.59 and 1.52, respectively, whereas the ECP-ABE provides 0.89 and 0.85 for the same encryption and decryption process.



(a)

(b)

Figure 2: (a) Encryption and (b) Decryption time analysis

Likewise, the proposed ECP-ABE provides minimal encryption and decryption time than the previous CP-ABE, RSA, and DSA. For the nodes 40 to 100, our model also illustrates the remarkable performance. Figure 3 proffers the memory utilized by the techniques for performing the cryptographic operations. For nodes 20 to 100, the proposed ECP-ABE uses the memory of 10541458, 13021124, 15231476, 18231459, and 21036452, respectively, which was lower usage than the existing methods. Thus, it concludes that the proposed one attains more performance than the existing methods.

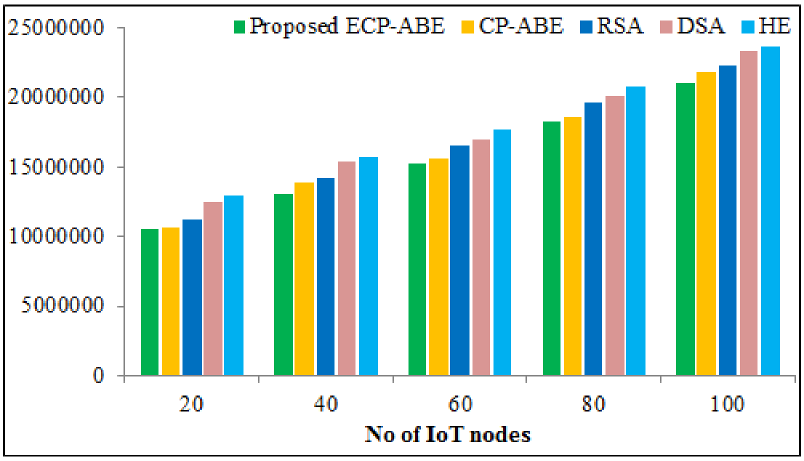


Figure 3: Memory usage analysis

Table 1 shows the throughput and reliability results of the encryption techniques. For 100 nodes, the proposed ECP-ABE gives the throughput and reliability of 81.23 kbps and 99.56%, which are higher compared to existing techniques, because the existing CP-ABE, RSA, DSA, as well as HE offers throughput of 61.41 kbps, 50.32 kbps, 41.12 kbps, and 38.65kbps and reliability of 95.22%, 94.39%, 90.78%, and 89.12%, which is comparatively lower than the existing methods. Overall, the experimental study demonstrates that the suggested strategy performs better than the current ones. The rationale is that the suggested method employs the CP-ABE encryption technique, and SWWOA is optimally used to form the CP-ABE access structure for safe cloud transmission.

Table 1: Performance analysis based on throughput and reliability

Metrics	No of IoT nodes	Proposed ECP-ABE	CP-ABE	RSA	DSA	HE
Throughput	20	74.25	51.41	39.12	31.22	25.23
	40	76.23	53.21	42.46	33.35	29.88
	60	79.21	56.86	45.52	36.71	33.54
	80	80.45	59.23	48.61	39.79	36.68
	100	81.23	61.41	50.32	41.12	38.65
Reliability	20	98.13	95.32	93.22	90.86	88.35
	40	98.66	95.41	93.33	90.25	88.12
	60	98.79	95.66	93.55	90.98	88.67
	80	99.21	95.88	93.79	90.45	88.78
	100	99.56	95.22	94.39	90.78	89.12

5. CONCLUSION

This study suggests a blockchain-enabled ECP-ABE method for providing secure access control and data storage systems for IoT-based healthcare environments. The outcomes of the suggested system are compared to the existing CP-ABE, RSA, DSA, and HE approaches concerning some evaluation measures and node variations. The proposed ECP-ABE achieves 0.89 encryption time, 0.85μs decryption time, 10541458 bits memory usage, 74.25kbps throughput, and 98.13% reliability for 20 nodes. Similarly, our method shows its significance over others for the rest of the nodes 40 to 100. Therefore, the total analysis of the experiments demonstrated that the suggested strategy is far superior to the current methods. This method is very secure because the user cannot retrieve the file without authentication verification. The suggested approach can be improved in the future to reduce memory usage in hospital computer systems by determining whether the same medical record will be uploaded repeatedly and starting a deduplication process to securely share the medical records with other consulting physicians in another hospital.

Conflict Of Interest

I, Aadhinarayanan.N.V, declares no conflicts of Interest to disclose.

Competing Interests

Not Applicable

Funding Information
Not Applicable

Author Contribution

Not Applicable

Data Availability Statement

Not Applicable

Research Involving Human And/Or Animals

This article does not contain any studies with human participants or animals performed by any of the authors.

Informed Consent

Not Applicable

REFERENCES

[1] Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., &Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). Applied Sciences, 12(4), 1927.

[2] Farid, F., Elkhodr, M., Sabrina, F., Ahamed, F., & Gide, E. (2021). A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services. Sensors, 21(2), 552.

[3] Memos, V. A., Psannis, K. E., Goudos, S. K., &Kyriazakos, S. (2021). An enhanced and secure cloud infrastructure for e-health data transmission. Wireless Personal Communications, 117, 109-127.

[4] Bharati, S., Podder, P., Mondal, M. R. H., & Paul, P. K. (2021). Applications and challenges of cloud integrated IoMT. Cognitive Internet of Medical Things for Smart Healthcare: Services and Applications, 67-85.

[5] Sadek, I., Codjo, J., Rehman, S. U., & Abdulrazak, B. (2022). Security and privacy in the Internet of Things healthcare systems: toward a robust solution in real-life deployment. Computer Methods and Programs in Biomedicine Update, 2, 100071.

[6] Ravikumar, S., & Kavitha, D. (2021). IoT based home monitoring system with secure data storage by Keccak–Chaotic sequence in cloud server. Journal of Ambient Intelligence and Humanized Computing, 12, 7475-7487.

[7] Deebak, B. D., & Al-Turjman, F. (2021). Secure-user sign-in authentication for IoT-based eHealth systems. Complex & Intelligent Systems, 1-21.

[8] Agyekum, K. O. B. O., Xia, Q., Sifah, E. B., Cobblah, C. N. A., Xia, H., & Gao, J. (2021). A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain. IEEE Systems Journal, 16(1), 1685-1696.

[9] Mustafa, M., Alshare, M., Bhargava, D., Neware, R., Singh, B., & Ngulube, P. (2022). Perceived security risk based on moderating factors for blockchain technology applications in cloud storage to achieve secure healthcare systems. Computational and mathematical methods in medicine, 2022.

[10] Gupta, B. B., Li, K. C., Leung, V. C., Psannis, K. E., & Yamaguchi, S. (2021). Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system. IEEE/CAA Journal of AutomaticaSinica, 8(12), 1877-1890.

[11] Prabha, P., & Chatterjee, K. (2022). Design and implementation of hybrid consensus mechanism for IoT based healthcare system security. International Journal of Information Technology, 14(3), 1381-1396.

[12] Coelho, K. K., Nogueira, M., Marim, M. C., Silva, E. F., Vieira, A. B., & Nacif, J. A. M. (2022). LORENA: Low memORysymmEtric-key geNerAtionmethod based on group cryptography protocol applied to the internet of healthcare things. IEEE Access, 10, 12564-12579.

[13] Liu, Y., Yu, J., Fan, J., Vijayakumar, P., & Chang, V. (2021). Achieving privacy-preserving DSSE for intelligent IoT healthcare system. IEEE Transactions on Industrial Informatics, 18(3), 2010-2020.

[14] Andreas, A., Mavromoustakis, C. X., Mastorakis, G., Do, D. T., Batalla, J. M., Pallis, E., & Markakis, E. K. (2021). Towards an optimized security approach to IoT devices with confidential healthcare data exchange. Multimedia Tools and Applications, 80, 31435-31449.

[15] Azrour, M., Mabrouki, J., & Chaganti, R. (2021). New efficient and secured authentication protocol for remote healthcare systems in cloud-iot. Security and Communication Networks, 2021, 1-12.

[16] Almalki, F. A., &Soufiene, B. O. (2021). EPPDA: an efficient and privacy-preserving data aggregation scheme with authentication and authorization for IoT-based healthcare applications. Wireless Communications and Mobile Computing, 2021, 1-18.