Received: March 10, 2021. Revised: July 15, 2021.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Blockchain Management System with Three Layer of Security for E-Health Record using Improved 16-bit XOR Cryptography

Manikandan Ramamurthy[1]* **Shankar Pushpa[1]**

[1]*Department of Computer Science and Engineering,*
St. Peter's Institute of Higher Education and Research, Tamilnadu, India
* Corresponding author's Email: manikandanaya3@gmail.com

Abstract: Blockchain system has various advantages in transaction data storage. Due to the distributed nature of blockchain, security becomes a concern to store private data. In literature, many techniques to maintain security in the blockchain is proposed. But the conventional data security schemes are not alone sufficient to incorporate complete security in blockchain. Hence in this paper, a blockchain management system with three layers of security is proposed. The proposed blockchain system is suggested for E-health record (EHR). The proposed system includes three layers, and the first layer contains a user authentication wall, which is used to verify the user based on unique user id, password and usage pattern. A tri-factor mechanism is used to verify the usage pattern of the user. In the second layer, the EHR manager is used to verify the query based on policy. The policy contains 48 rules, which is used to analyse the query to grand or denied access. The final layer consists of lightweight 16-bit XOR cryptography used to store the data as cybertext. The proposed system is evaluated using three medical datasets, and its performances are evaluated based on turnaround time, tardiness, actual time delay and average actual time delay. The simulation performance of the proposed technique, that turnaround time is 55ms, tardiness is 150ms, and actual-time delay is 160ms. The encryption time of Data 1, Data 2 and Data 3 is 550ms, 50ms, and 1150ms, respectively. On the other hand, the proposed technique consumed time for decryption of Data 1, Data 2 and Data 3 is 1750ms, 65ms, and 1450ms, respectively. The performance analysis proves the effectiveness of the proposed system. Ultimately, the proposed blockchain management system is more suitable for enhancing the security for handling health records.

Keywords: Blockchain, E-health record, XOR cryptography, Blockchain data security, User authentication, EHR manager.

1. Introduction

Blockchain is the process of storing information in which cheating, hacking, and changes are avoided in the system [1]. It is the digital ledger of the transaction and the ledger-based damage proof methodology [2]. In blockchain technology, the transactions are registered in the public ledger [3]. To provide security, information stored in the blockchain is distributed across the overall computer network platform. It is defined as the data structure in which the records of transactions were stored. In the blockchain approach, transparency, decentralisation, and security are guaranteed. The blockchain information was stored in the form of blocks [4]. These blocks are controlled by the entire nodes present in the blockchain. Hence the central point of failure is avoided [5]. Nowadays, security in blockchain technology is one of the possible issues. Due to blockchain technology in most industries, the business thought of people will be changed. The recent behind the blockchain usage in industries is the reliability and the service providing capability. But some of the security issues present behind this blockchain technology [6].

In blockchain technology, the decision-making process is mostly done by considering the entire node in the network [7]. To provide security in blockchain technology, the bitcoin cryptocurrency

scheme is used. This scheme contains the signature so that these networks are protected from the attacks of computer hackers [8]. The key-encryption technique was used in the blockchain for promoting security. So the illegal access to information was not possible. By using the public key for encryption, security issues arise. In decryption, the private key is used at the receiver side [9]. The double encryption technique such as ARX cypher encryption and the public key encryption was used for achieving security. For ensuring the secure exchange of public key, the Diffie-Hellman approach was used. This approach secures those public key by only accessing those keys between the sender and the receiver and preventing those keys from the intruders [10].

The smart contract was used in the blockchain methodology for security enhancement. These codes are simple and easy to understand [11]. But some security issues arise when the new developers write the codes. If the new developers write these codes with solidity language, then these codes may be accessible by the intruders [12]. To secure the patient records efficiently, the Keyless Signature Infrastructure Blockchain (KSIBC) was used. In this approach, the authorised user verification was done using the Access control List (ACL). If the user was authorised, then they provide the digital signature for promoting integrity. These signatures are maintained as a secret for security purpose [13]. The attribute-based method, combined with multiple authorities, was used for promoting security. This method ensures the patient's privacy and also promote the immutability of EHR [14].

For sharing the medical-related data in a secured manner, the MeDShare approach was used. It monitors whether the authorised sector or the intruder accessed the data and observed that the authorised sector uses those particular data to perform malicious activity [15]. For providing access control, the MeDShare system uses the intelligent contract approach containing data and code that are self-operating. The data-sharing model was designed for the secure transmission of data [16]. The MedBlock, the blockchain-based information handling system, was used to manage the information about the patient in a secured manner. Using this approach, accessing and retrieving the medical-related data was done efficiently [17]. The public key cryptography technique was used for providing security. In this technique, the accessibility and the modification of data were not possible [18].

Blockchain is the methodology in which the transactional data was stored in a secured manner. It acts as the ledger-based approach. In medical data sharing, the blockchain and the InterPlanetary File System were combined to act as a buffer for storing the transactional data in which the health-related information was present. The health-related information was shared between the patient and the medical practitioner. To avoid security and privacy issues due to sharing information, a reliable access control mechanism such as smart contract and the etherium blockchain was incorporated in the blockchain approach. In the blockchain approach, data sharing and data uploading were done efficiently using the intelligent contract approach. In the blockchain, data security was provided for the shared community. The intruders don't have the capability for reading or modifying the information present in the blockchain. Because of the distributed nature of information in the blockchain, the central point of failure was impossible, so that the blockchain approach was used in most industries. The contribution of the proposed paper is as follows;

- To ensure security in sharing medical-related data, the blockchain management system is developed. This approach includes three essential layers: User Authentication, policy-based Electronic Health Record (EHR) manager and Data encryption/decryption.
- The system users are broadly classified into three, such as patient, doctor, and hospital staff. Then based on roles, these three users are divided into eight categories.
- In this initial stage, the authentication of users is verified using a unique id, password and behaviour pattern. Here a tri-factor mechanism is used to verify the user.
- Then the policy based EHR manager grand or restrict the access based on their roles. The EHR maintains a list of k-policies, which acts as a knowledge resource to enable the databank connection.
- In the third component, an enhanced 16-bit XOR cryptography approach is used to encrypt the data while storing and decrypting during retrieval.

The rest of the paper is organised as follows; the literature related to the security enhancement in the blockchain system is given in Section 2. Section 3 describes the proposed blockchain management system. Then Section 4 gives the obtained performance of the proposed system. The subsequent section (Section 5) gives the conclusion of the paper.

2. Related works

Many research works are available for the security enhancement of the blockchain. Some of the works are reviewed in this section.

Yunifa Miftachul Arif *et al.* [19] have developed the blockchain-based data-sharing approach for a decentralised tourism destinations recommendation system. The data-sharing approach acknowledges the information broadcasting between the nodes present in the recommendation system. The recommendation system contains three primary nodes, such as user, server, and sensor node. Here the user node sends the evaluation data of the destination to the server node. The server node sends information about the tourism activities to the user node. The sensor node sends dynamic data such as admiration, weather, and traffic to the user node. Finally, the recommendations process had to be generated.

Rokesh Kumar Yarava and Rajendra Prasad Singh [20] have presented secure and efficient cloud storage auditing based on the Diffie-hellman key exchange. The approach of Diffie-Hellman generate the key which was in the encrypted form and share those encrypted key in between the two parties such as the sender and destination. The ephemeral keys and the new key pair were created using the Diffie-Hellman approach efficiently. Some of the encryption technique, such as the digital signature and Integrated Encryption Scheme (IES), was used for providing security.

Chellan Edward Jaya Singh and Eppies Baburaj *et al.* [21] have presented the image encryption system. In the system, the images were encrypted using the double encryption method and the de-duplication done on the images to enhance security. Initially, the modified Paillier encryption technique was used for promoting the security of images. After that, the XOR encryption was taken place. After performing the XOR encryption, the de-duplication were performed to secure the confidentiality of images.

Clara Kanmani Arulanandu *et al.* [22] have presented the Resource Description Framework (RDF) encryption, and token-based access control system in which sensitive data in an RDF graph was encrypted and all other non-sensitive data were publicly lucid. This framework's three essential procedures were the security process, the decryption process, and the query process. The consequence of the security process was encrypted data, encrypted metadata, and plain text fragments. The technique permits the token-based access control system for the decryption procedure. The query process incorporates the map-reduce framework was for lessening the immense measure of employments. Finally, the query answer was sent to the user in light of the system administrator's Access Token list (AT-list).

Ting Yuan *et al.* [23] have presented the group key distribution scheme with self-healing property that enables users in a dynamic group to establish session keys over an unreliable network with constrained bandwidth resources. The system had limited group membership property with an upper bound on the number of users in the group. The scheme had a better trade-off between storage and communication overhead through modelling and analysis compared to previous work. In addition, the variant of the scheme enables key recovery from a single broadcast message.

System in Ref. [19] proposed a recommendation-based data sharing system. It is suitable for standard or social data but security for handling medical records. In Ref. [20], a key exchange mechanism for effective encryption of data is proposed, but the technique does not concentrate on access control. The system in Ref. [21] have used XOR-based encryption without a proper access control mechanism. Two security mechanisms with proper key distribution were presented in Ref. [22] and Ref. [23]. However, this lack of providing a better mechanism to ensure the access control and data access policy. These issues are concentrated to rectify in the proposed system.

3. Proposed methodology

A secure and distributed blockchain system for hospital data storage is presented. This approach includes four essential components: end-user, policy-based Electronic Health Record (EHR) manager, data encryption/decryption, and data storage approach, such as an Interplanetary File System (IPFS). The system users are broadly classified into three, such as patient, doctor, and hospital staff. Then based on roles, these three users are divided into eight categories. In this initial stage, the users are assigned a unique id used for the authentication propose. Then the policy based EHR manager grand or restrict the access based on their roles. The EHR maintains a list of k-policies, which acts as a knowledge resource to enable the databank connection. In the third component, an enhanced 16bit XOR cryptography approach is used to encrypt the data while storing and decrypting during retrieval. The data are stored in IPFS. The system architecture of the proposed blockchain system is given in Fig. 1.

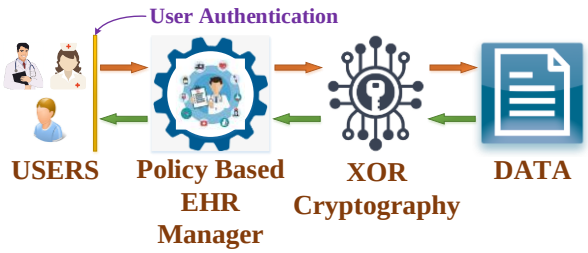

Figure. 1 System architecture

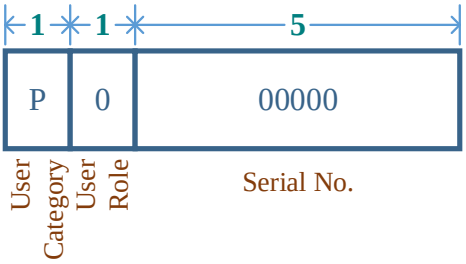

Figure. 2 Format of the user ID

3.1 User assignment and authentication

In this phase, the users of the blockchain are assigned a unique user id. Here the users are broadly classified into the patient, doctor, and hospital staff.

The user ID in this proposed method is assigned as a seven-bit code, in which the first-bit code represents the category of user, the second bit represents the role of the user, and the remaining five bits represents the serial number of the user. In this mechanism, eight types of users consider. Its category and role detail are described in Table 1.

Table 1 showed the user category and rode detail. The table clearly shows that four categories of users with eight roles in total. The formatted user id can help to verify the unique id and to assign an access policy. In addition to the unique user id pattern, a security mechanism is included to ensure the authentication of the user. A tri-factor mechanism for user authentication is applied. The tri-factor user authentication scheme is referred to from Ref. [24].

Table 1. User category and role detail

User Category	Category Code	User Role	Role Code
Admin	A	Admin	1
Staff	H	Front Office	1
		Pharmacy	2
		Staff Nurse	3
Doctor	D	Duty Doctor	1
		Specialist Doctor	2
Patient	P	In-Patient	1
		Out-Patient	2

Figure. 3 Rules pattern

The step-by-step procedure of user tri-factor user authentication is as follows;

Step 1: User ID and authentication password is verified as per similarity match.

Step 2: The user initiates the blockchain access request.

Step 3: The authentication wall evaluates the query frequency, in which the frequent usage of the query is evaluated. If the new query is found as usual, then the authentication wall enables access. Otherwise, the authentication wall restricts user access.

The tri-factor user authentication in the authentication wall can act as gateway security to allow the authentic user to access the blockchain.

3.2 Policy-based EHR manager

In this phase, the EHR manager evaluates the policy to grant access to the blockchain. In this blockchain system, medical records are considering. Every data includes two significant portions, such as personal information (Per_Info) and medical information (Med_Info). The personal information includes the personal detail of the patient. Similarly, the medical information includes medical data related to medication, disease, etc. In these blockchains, the medical record is allowed to access by various time of users. But they are limited to access specific information based on the type of access request. The list of users and the rules used in the EHR manager is given in this section. There are 48 rules constructed for deciding on the EHR manager. The rule pattern is shown in Fig. 3.

In Fig. 3, the rule pattern is given; it includes four portions. The first portion is the user type, which is code as the combination of category code and role code, as in Table 1, e.g., H1 represents front office staff. The second portion represents the Query Type. In the proposed system, three types of query are considered, which are listed underneath.

Query #1: Read/View a Data
Query #2: Modify a Data
Query #3: Add New Data

Rules for Administrative User: Six rules for every function to every information is created for the administrative. In general, the authenticated administrative users are always allowed to access every piece of data in the blockchain. The rules suggested for the administrative user is listed below.

Administrator

<A1/Read_Req/Per_Info/Grand_Access>
<A1/Modi_Req/Per_Info/Grand_Access>
<A1/Add_Req/Per_Info/Grand_Access>
<A1/Read_Req/Med_Info/Grand_Access>
<A1/Modi_Req/Med_Info/Grand_Access>
<A1/Add_Req/Med_Info/Grand_Access>

Rules for Staff User: In this system, three types of staff users, likewise Front Office User, Pharmacy User and Staff Nurse User. Hence 18 rules are constructed for staff user, among six rules per user type.

Front Office User

<H1/Read_Req/Per_Info/Grand_Access>
<H1/Modi_Req/Per_Info/Grand_Access>
<H1/Add_Req/Per_Info/Grand_Access>
<H1/Read_Req/Med_Info/Denial_Access>
<H1/Modi_Req/Med_Info/Denial_Access>
<H1/Add_Req/Med_Info/Denial_Access>

Staff Nurse User

<H3/Read_Req/Per_Info/Grand_Access>
<H3/Modi_Req/Per_Info/Grand_Access>
<H3/Add_Req/Per_Info/Denial_Access>
<H3/Read_Req/Med_Info/Grand_Access>
<H3/Modi_Req/Med_Info/Denial_Access>
<H3/Add_Req/Med_Info/Denial_Access>

Pharmacy User

<H2/Read_Req/Per_Info/Grand_Access>
<H2/Modi_Req/Per_Info/Denial_Access>
<H2/Add_Req/Per_Info/Denial_Access>
<H2/Read_Req/Med_Info/Grand_Access>
<H2/Modi_Req/Med_Info/Denial_Access>
<H2/Add_Req/Med_Info/Denial_Access>

Rules for Doctors: Two types of doctors are considered in the proposed blockchain system. Thus 12 rules are created for the doctor, which is given below.

Duty Doctor

<D1/Read_Req/Per_Info/Grand_Access>
<D1/Modi_Req/Per_Info/Grand_Access>
<D1/Add_Req/Per_Info/Denial_Access>
<D1/Read_Req/Med_Info/Grand_Access>
<D1/Modi_Req/Med_Info/Grand_Access>
<D1/Add_Req/Med_Info/Grand_Access>

Specialist Doctor

<D2/Read_Req/Per_Info/Grand_Access>
<D2/Modi_Req/Per_Info/Denial_Access>
<D2/Add_Req/Per_Info/Denial_Access>
<D2/Read_Req/Med_Info/Grand_Access>
<D2/Modi_Req/Med_Info/Grand_Access>
<D2/Add_Req/Med_Info/Denial_Access>

Rules for Patients: Similar to a doctor, two types of patients are considered, so it contains a total of 12 rules which are listed below.

In-Patient

<P1/Read_Req/Per_Info/Grand_Access>
<P1/Modi_Req/Per_Info/Grand_Access>
<P1/Add_Req/Per_Info/Denial_Access>
<P1/Read_Req/Med_Info/Grand_Access>
<P1/Modi_Req/Med_Info/Denial_Access>
<P1/Add_Req/Med_Info/Denial_Access>

Out-Patient

<P2/Read_Req/Per_Info/Grand_Access>
<P2/Modi_Req/Per_Info/Grand_Access>
<P2/Add_Req/Per_Info/Denial_Access>
<P2/Read_Req/Med_Info/Denial_Access>
<P2/Modi_Req/Med_Info/Denial_Access>
<P2/Add_Req/Med_Info/Denial_Access>

3.3 Medical record encryption/decryption based on 16bit-XOR cryptography

The proposed blockchain system handles a medical record, so it should be secured before it is inserted into a blockchain. Here 16-bit XOR-based cryptography is proposed for the encryption and decryption of medical record. The step-by-step procedure for 16bit-XOR cryptography is given below;

A. Data Conversion Phase

Initially, the input data is converted into 16-bit binary data. In the medical record, some of the data might be in the string. So, the strings are converted to a number using ASCII before binary conversion. The pseudocode for the data conversion is given in Algorithm 1. The converted 16 binary is represented as four 4-bit binary data, further utilised in the subsequent steps.

The pseudocode in Algorithm 1 gives the procedure for data conversion. In the data conversion phase, the primary intention is to convert the input string to binary. Let 'x' be the

Algorithm 1: Pseudocode for data conversion

```
Initialize Data : x
For ( i=1: x ):
    If (x( i ) is string)
        T_x = x( i )        // Individual String
        For ( j = 1:length( T_x ) ):
            // Binary Conversion after ASCII
            C_d ( j )=BIN(ASCII( T_x( j ) ))
        End For
    Else
        // Binary Conversion of Number
        C_d = BIN( x( i ) )
    End If
End For
```

input dataset, 'T_x' be the individual string in the dataset. If the string is a number, then it is converted to binary. Else it is converted to respective ASCII code before converting to binary.

B. Data Encryption/Decryption Phase

Binary data obtained from the previous phase are separated into four groups with 4-bits each. Then each group is split into two, and the group is split based on the ratio of its binary equivalence. Then the split binary sets are separately encrypted by performing an XOR operation. Finally, the encrypted data is stored in the blockchain. The process of encryption is shown in Fig. 4(a).

On the other hand, the data are required to decrypt during retrieval. The medical data decryption in the retrieval process is shown in Fig. 4(b).

4. Results and discussion

The proposed blockchain management system with 16-bit XOR cryptography is implemented using MATLAB 2020b, in windows platform with intel core i5 CPU and 8GB RAM. The performance of the system is evaluated considering a medical dataset UCI library [25].

The effectiveness of the proposed system is evaluated based on the performance like Turnaround time, Tardiness, Actual time delay and Average actual time delay. To justify the effectiveness of the proposed system, it is compared with the existing techniques like XOR [21], ECC [26], RSA [27], AES [28] and DES [29].

The turnaround time of the proposed system is evaluated and which is shown in Fig. 5. The figure clearly shows that the proposed system consumes less time than the other methods. Then Fig. 6 shows the tardiness. The tardiness is measured in the unit of sec, and the proposed system is comparatively better than the existing system with less tardiness.

In Fig. 7, the actual time delay comparison is given; the proposed system has a minor delay than the other two systems. It shows that the proposed

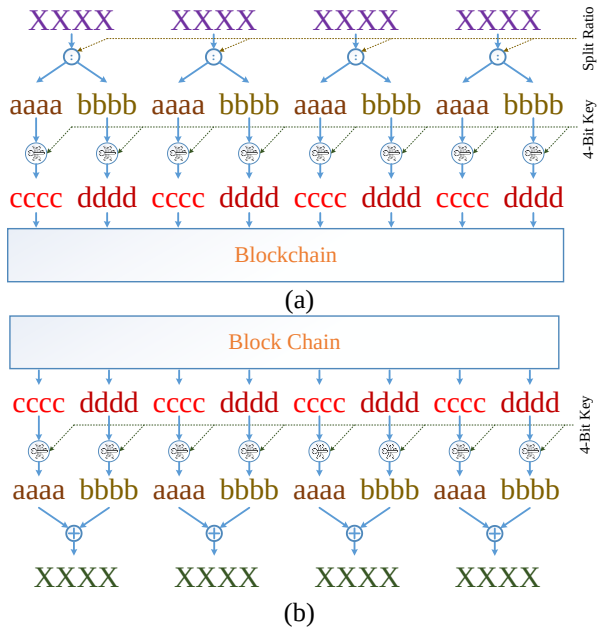

Figure. 4 Flow of cryptographic process for HER: (a) Encryption and (b) Decryption

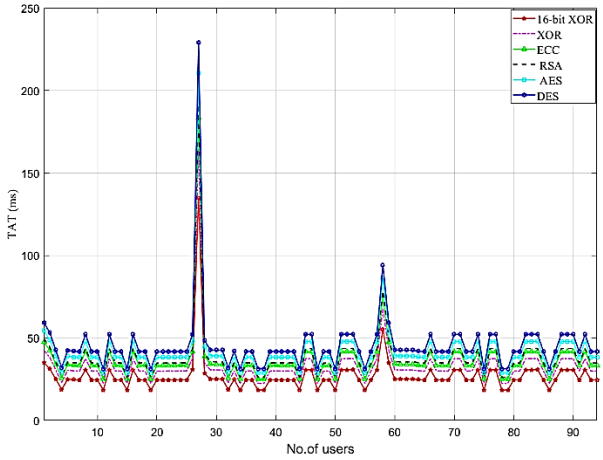

Figure. 5 Performance analysis of turnaround time

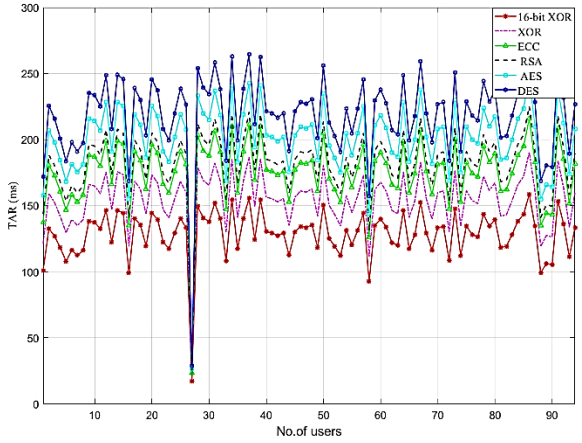

Figure. 6 Performance analysis of Tardiness

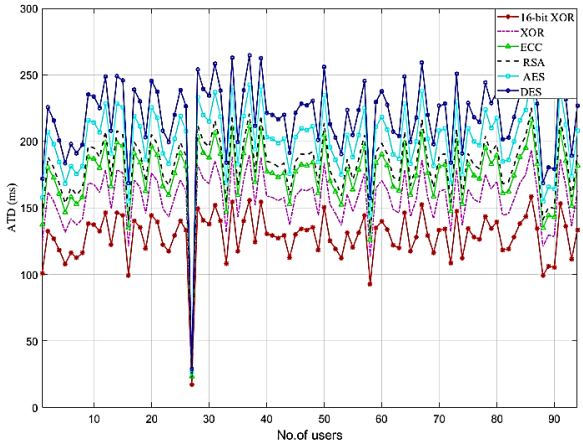

Figure. 7 Performance analysis of actual time delay

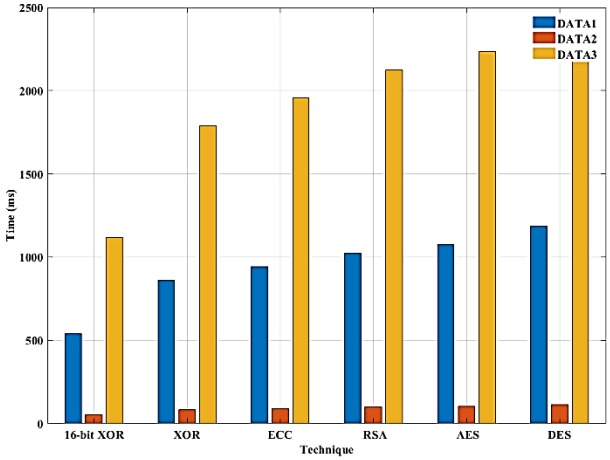

Figure. 8 Performance analysis of encryption time

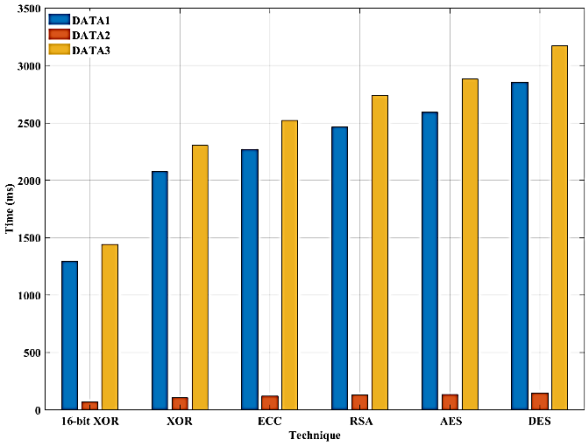

Figure. 9 Performance analysis of decryption time

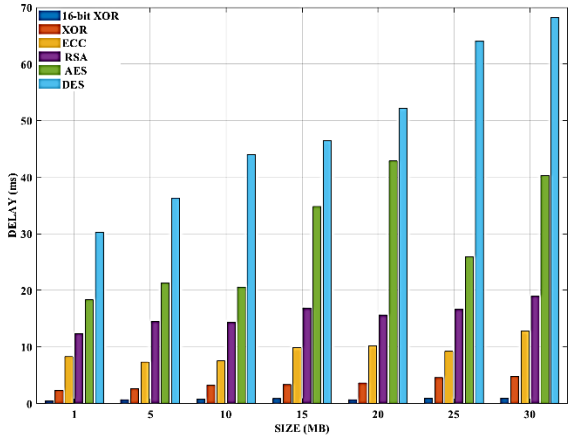

Figure. 10 Performance analysis of delay

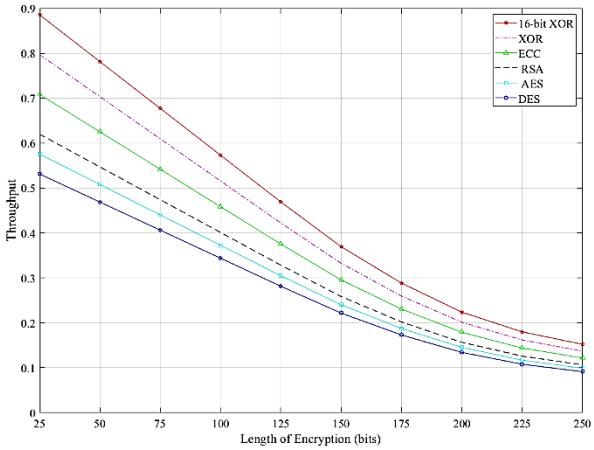

Figure. 11 Performance analysis of throughput

cryptographic scheme consumes less time to made decision. Thus, the system is adequate to maintain security in the medical blockchain.

The encryption time and decryption time comparison are shown in Fig. 8 and 9, respectively. The encryption and decryption performance are compared using three datasets.

For all three datasets, the encryption and decryption time of the proposed system is comparatively less than the other two cryptographic techniques. With fast encryption and decryption, the delay of the proposed system more diminutive than the other techniques, which is shown in Fig. 10.

The throughput comparison of various security scheme is shown in Fig. 11. The figures clearly show that the throughput of the security schemes decreases as the length of the data bits increases. But the proposed system's throughput maintained at the top position with better performance. The performance analysis proves that the proposed EHR management for the blockchain system performs well with improved speed and security.

The comparison charts given in Fig. 5 to 11 show the performance analysis proposed with other existing techniques. In Fig. 5 the turnaround time of various technique is given, in which the turnaround time of 100 users is evaluated. The analysis clearly shows that the turnaround time of the proposed 16-bit XOR is better than the other techniques. Similarly, the Tardiness and Actual time delay of 100 users is shown in Fig. 6 and 7. Both the tardiness and actual time delay of all the user is better in the proposed technique.

On the other hand, Fig. 8 and 9 shows the cumulative encryption and decryption time, respectively. The proposed 16-bit XOR technique consumed less time for encryption and decryption, which minimises the overall processing time. The comparison in Figure 10 shows the overall delay of various techniques, the delay by the proposed 16-bit XOR technique is less than 5ms up to 30MB files. Based on this performance analysis, it is proved that the effectiveness of the proposed 16-bit XOR is better than the other techniques. Ultimately, the proposed 16-bit XOR-based system is recommended for the security of medical record in the blockchain system.

5. Conclusion

An advanced system for the EHR management system in blockchain with better security is proposed. The proposed system considered three layers of process. Each layer concentrated on attaining security. In the first layer, a user authentication wall is considered for verifying the user based on their id, password and behaviour pattern. Then in the second layer, the EHR manager with policies are maintained to check the user query to grand access using 48 rules. Light weight16-bit XOR cryptography is used to convert/retrieve the information to/from cybertext in the last layer. The system is evaluated based using three medical datasets, and its performance is evaluated based on turnaround time, tardiness, actual time delay and average actual time delay. The execution results show better performance with high tardiness and low delay, encryption and decryption time. The overall delay is less than 5ms for processing up to 3MB file. The encryption and decryption time is lower than other techniques for processing both three datasets. The overall performance analysis proved the effectiveness of the proposed system. The system can be further enhanced in future work with the intrusion detection mechanism in the authentication layer.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualisation:- Manikandan Ramamurthy and Shankar Pushpa; methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing:- Manikandan Ramamurthy; review and editing:- Shankar Pushpa.

Acknowledgements

This work was supported by the Department of Computer Science and Engineering, St. Peter's Institute of Higher Education and Research, Tamilnadu, India.

References

[1] S. Ølnes, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing", *Government Information Quarterly*, Vol. 34, No. 3, pp. 355-364, 2017.

[2] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT", *Procedia Computer Science*, Vol. 132, No. 1, pp. 1815-1823, 2018.

[3] J. Y. Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review", *PloS one*, Vol. 11, No. 10, p. e0163477, 2016.

[4] R. Casado-Vara, P. Chamoso, F. De la Prieta, J. Prieto, and J. M. Corchado, "Non-linear adaptive closed-loop control system for improved efficiency in IoT-blockchain management", *Information Fusion*, Vol. 49, No. 1, pp. 227-239, 2019.

[5] M. A. Dorairangaswamy, "A novel invisible and blind watermarking scheme for copyright protection of digital images", *International Journal of Computer Science and Network Security*, Vol. 9, No. 4 pp. 71-78, 2009.

[6] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges", *IJ Network Security*, Vol. 19, No. 5 pp. 653-659, 2017.

[7] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: A survey on applications and security privacy challenges", *Internet of Things*, Vol. 8, No. 1, pp. 100107, 2019.

[8] Y. L. Gao, X. B. Chen, Y. L. Chen, Y. Sun, X. X. Niu, and Y. X. Yang, "A secure cryptocurrency scheme based on post-quantum blockchain", *IEEE Access*, Vol. 6, No. 1, pp. 27205-27213, 2018.

[9] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions", *Future Generation Computer Systems*, Vol. 97, No. 1, pp. 512-529, 2019.

[10] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralised privacy-preserving healthcare blockchain for IoT", *Sensors*, Vol. 19, No. 2 pp. 326, 2019.

[11] R. Manikandan, P. A. Kumar, and R. Govindaraju, "Code Security By Confusing Logic Flow Using Self Modifying Code", *International Journal of Innovative Trends and Emerging Technologies*, Vol. 1, No. 1, pp. 90-96, 2015.

[12] A. Singh, R. M. Parizi, Q. Zhang, K. K. R. Choo, and A. Dehghantanha, "Blockchain smart contracts formalisation: Approaches and challenges to address vulnerabilities", *Computers & Security*, Vol. 88, No. 1, p. 101654, 2020.

[13] G. Nagasubramanian, R. K. Sakthivel, R. Patan, A. H. Gandomi, M. Sankayya, and B. Balusamy, "Securing e-health records using keyless signature infrastructure blockchain technology in the cloud", *Neural Computing and Applications*, Vol. 32, No. 3 pp. 639-647, 2020.

[14] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems", *IEEE Access*, Vol. 6, No. 1, pp. 11676-11686, 2018.

[15] K. Raja, K. Suresh Babu, and R. Manikandan, "A Mechanism to Inhibit Unsolicited Texts from OSN User Walls", *International Journal of Computer Science and Engineering Communications*, Vol. 3, No. 4, pp. 1210-1215, 2015.

[16] Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain", *IEEE Access*, Vol. 5, No. pp. 14757-14767, 2017.

[17] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: Efficient and secure medical data sharing via blockchain", *Journal of medical systems*, Vol. 42, No. 8 pp. 1-11, 2018.

[18] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives", *Cryptography*, Vol. 3, No. 1, p. 3, 2019.

[19] Y. M. Arif, H. Nurhayati, F. Kurniawan, S. M. S. Nugroho, and M. Hariadi, "Blockchain-based data sharing for decentralised tourism destinations recommendation system", *International Journal of Intelligent Engineering and System*, Vol. 13, No. 6 pp. 472-486, 2020.

[20] R. K. Yarava and R. P. Singh, "Efficient and Secure Cloud Storage Auditing Based on the Diffie-Hellman Key Exchange", *International Journal of Intelligent Engineering and Systems*, Vol. 12, No. 3, pp. 50-58, 2019.

[21] C. E. J. Singh and E. Baburaj, "XOR Reformed Paillier Encryption Method with Secure De-duplication for Image Scaling and Cropping in Reduced Cloud Storage", *International Journal of Intelligent Engineering and Systems*, Vol. 12, No. 4, pp. 328-337, 2019.

[22] C. K. Arulanandu, S. V. D. Murthy, and G. Nagraj, "Cloud based RDF security: a secured data model for cloud computing", *International Journal of Intelligent Engineering and Systems*, Vol. 11, No. 1, pp.83-93, 2018.

[23] T. Yuan, J. Ma, Y. Zhong, and S. Zhang, "Group Key Distribution with Self-healing Property for Unreliable and Communication-constrained Networks", *International Journal of Intelligent Engineering and Systems*, Vol. 4, No. 1, pp. 1-8, 2018.

[24] H. Lee, D. Kang, J. Ryu, D. Won, H. Kim, and Y. Lee, "A three-factor anonymous user authentication scheme for Internet of Things environments", *Journal of Information Security and Applications*, Vol. 52, No. 1, pp. 102494, 2020.

[25] https://archive.ics.uci.edu/ml/datasets/Heart%2BDisease

[26] K. Sowjanya and M. Dasgupta, "A ciphertext-policy Attribute based encryption scheme for wireless body area networks based on ECC", *Journal of Information Security and Applications*, Vol. 54, No. 1, p. 102559, 2020.

[27] G. W. W. Mukti and H. Setiawan, "Designing and Building Secure Electronic Medical Record Application by Applying AES-256 and RSA Digital Signature", *In IOP Conference Series: Materials Science and Engineering. IOP Publishing*, Vol. 852, No. 1, p. 012148, 2020.

[28] C. Rahmad, A. R. Syulistyo, and A. D. W. Sumari, "Securing the electronic medical record by implementing Advanced Encryption Standard (AES) on the information system of a health service place", *In IOP Conference Series: Materials Science and Engineering, IOP Publishing*, vol. 1073, No. 1, p. 012057, 2021.

[29] D. Vashi, H. B. Bhadka, K. Patel, and S. Garg, "An Efficient hybrid approach of attribute based encryption for privacy preserving through horizontally partitioned data", *Procedia Computer Science*, Vol. 167, No. 1, pp. 2437-2444, 2020.