International Journal of Engineering

Journal Homepage: www.ije.ir

Security and Data Privacy of Medical Information in Blockchain Using Lightweight Cryptographic System

R. P. Puneeth*[a,b], G. Parthasarathy[b]

[a] *Department of Computer Science and Engineering, NMAM Institute of Technology-Affiliated to NITTE (Deemed to be University), India*
[b] *School of Computing and Information Technology, REVA University, Karnataka, India*

PAPER INFO

Paper history:
Received 21 September 2022
Received in revised form 10 January 2023
Accepted 01 March 2023

Keywords:
Data Security
Blockchain
Lightweight Cryptographic System
Intuitionistic Derivative Symmetrical Encryption Algorithm
Differential Hashing Pattern
Decentralization
Electronic Health Records

ABSTRACT

In the healthcare system and hospital environment, the data security and the data connectivity are the major factors to consider for patient data management system. For that, there are several techniques are used to preserve and arrange the patient data with enhanced security system. In that, Blockchain structure of data management improves the secure data storage and transmission process. In the data security system, the quality measure can be validate by means of the size of key that are used for the encryption process. Combined with the blockchain, the encryption model is to be improved for the solve the problem in data security system. This also needs to focus on the size reduction of data storage due to the large key size of encrypted data. In the proposed work, Intuitionistic Derivative Symmetrical Encryption (IDSE) Algorithm based security algorithm along with blockchain function was integrated to form the authorized data storage and transmission process. For the key pattern generation, Differential Hashing Pattern (DHP) based key pattern extraction model was used for high speed data transmission and to reduce the size of data that are encrypted. The features that are considered for the appropriate security system are the data transmission pattern with respect to the time and the hashing model of key generation. In the result analysis, the performance of the IDSE-DHP are validated with the parameters of data transmission and loss rate in the Blockchain and with the throughput related features.

***doi**: 10.5829/ije.2023.36.05b.09*

1. INTRODUCTION

One of the emerging technologies, blockchain offers a number of intriguing features that can undoubtedly address current problems in real-time applications. Blockchain encourages decentralization, more openness, better traceability, and safe architecture as opposed to centralized approach, secretive, exclusive, and modifiable alternatives. The adoption of blockchain in the healthcare industry offers a number of interesting alternatives for enabling safe stakeholder communications and an effective method of clinical report distribution. The use of blockchain along with cloud environment [1] and the other database management system, the data security and the transmission rate are mainly considered. Similarly, with the combination of cloud data retrieval process, the intermediate needs to act the perfect data management for fast data transmission process. To achieve this, the block computing was introduced for the analyzing of parameters from blocks with enhanced model of data transmission between the blocks and cloud storage system. This forms the edge of hash-key connectivity with secured communication model. It performs the functionalities of data computing, storage utilizes, and the related structure of services that are in the networking system and its management. The blockchains are used with these arrangements for fast computing and the data transmission between the cloud and the end device. The basic structure of Blockchain connectivity to the clod based on the block computing is shown in Figure 1.

In this figure, the architecture of the blockchain model was sub-classified into three stages such as, cloud environment, block computing and the end-user of patient blocks. The blocks are connected to the data link unit to retrieve data from the cloud to local system while

*Corresponding Author Institutional Email: puneeth.reval313@gmail.com (R. P. Puneeth)

Please cite this article as: R. P. Puneeth, G. Parthasarathy, Security and Data Privacy of Medical Information in Blockchain Using Lightweight Cryptographic System, ***International Journal of Engineering, Transactions B: Applications***, Vol. 36, No. 05, (2023) 925-933

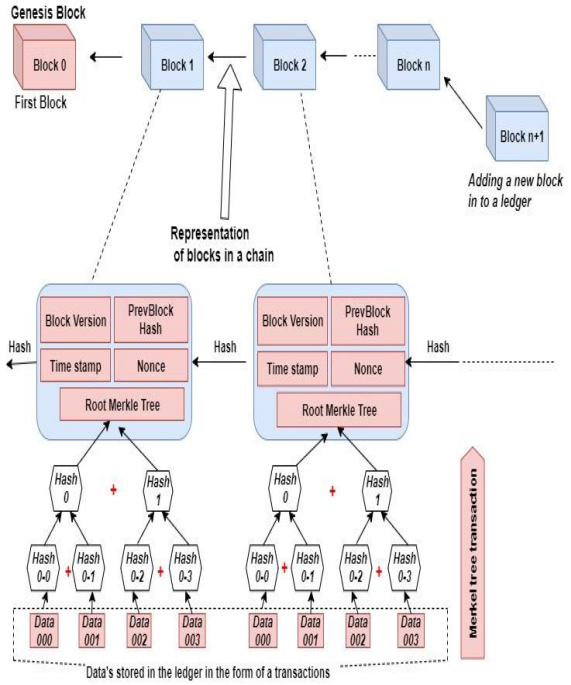

Figure 1. Basic architecture of blockchain

at the dynamic hash-key structure. The block computing and the other controllers are done in the data link unit that controls the flow of data transmission to the blocks and cloud storage. Here, the data security can also process under the controlling unit which forms the secure hash-key combination. The data link placement and the structure are referred to route the patient blocks based on the index and coverage size. In that, some of the algorithm that are used for security model such as Adaptive Data Dissemination Protocol (AddP) [2], intelligent forwarding method [3], Random Fire-Fly [4], map-based relaying algorithm (MBR) [5], adaptive beacon generation rate (ABGR) [6], etc. are implementing the appropriate feature selection for security block identification with the hash-key security problem.

From these arrangements, to achieve the better transmission rate and to increase the throughput parameters in the hash-key formation, the security block selection needs to select with the best appropriate block that is to achieve the best matching with the parameters that are related to the data transmission. This can also combine with the Block computing technique to enhance the security experience and enhance the high speed data transmission. This was enhanced in the proposed technique based on the batching process of data security algorithm to achieve the parameters range. The hash-key security in the proposed architecture can be achieved by using the light-weight key generation model and the hashing key pattern to enhance the speed of performance and the secure data transmission rate.

The objective of the proposed model of appropriate security and the Blockchain security can be listed as follows:

- To estimate the hash-key properties and the block characteristics based on the pattern extraction and security system in blockchain.
- To perform the appropriate selection of best security block by using the Intuitionist Derivative Symmetrical Encryption (IDSE) Algorithm that validates the data size and the identification of block index.
- To estimate the relevant features attributes that are to find the best selection of parameters that are can be used for data arrangement in the blockchain with the proper link structure.
- To enhance the hash-key security model in the blockchain architecture based on the key pattern extraction and the combination of block computing technique.
- To implement the Differential Hashing Pattern method of encryption model for the secure data transmission with light-weighted architecture for high speed data transmission model.

The full description about the proposed architecture and the algorithm descriptions are explained in the following sections. According to that, the survey of various types of hash-key security system and the security algorithms are explained with its merits and demerits in section I. the IDSE and the DHP based secure appropriate security algorithm are explained in the section II. The simulation parameters and the performance validation of the proposed model with the comparison chart and the table results are described in the section III. Finally, the conclusion of proposed model was justified and the future works are presented in section IV.

1. 1. Related Works The brief surveys of related works for the proposed algorithms are reviewed and find the merits and demerits of those existing algorithms in this section. This was also to analyze the limitations of existing algorithms that are identified for the different types of existing data security model. In this, the survey is divided as the two categories such as for the appropriate security system and hash-key security system in the dynamic blockchain architecture.

Ismail et al. [7] proposed the novel model of Adaptive Byte Hybrid Automatic Repeat reQuest (AB-HARQ) based intelligent communication system for the blockchain in the application of road safety system which can avoid the accidents. To overcome the problem of non-line of sight (NLOS) blocks by introducing broadcasting storm and channel congestion during data dissemination. For this weighted inertia-based dynamic virtual bat algorithm (WIDVBA) [8] based appropriate security algorithm. Bhattacharya et al. [9] proposed a

novel model of forwarding scheme to deliver data based security algorithm for time management in data transmission. A survey of different blockchain communication algorithm was presented in literature [10, 11].

In high dynamic topology, Saif et al. [12] proposed GHN model that works on the selective block security to prevent unwanted data flooding. Batch technique and the certificate-less ring signature (CL-RS) for data validation were performed by Wang et al. [13]. This paper focused on the data security and privacy issue in the blockchain communication. Similarly, the challenges in the data security such as time-consuming certificate revocation list (CRL) checking, computation overhead and identity revocation problem are validated by Abdul Rahoof et al. [14]. To overcome the flooding problem in Blockchain architecture, Optimized Link State Allocation Protocol (OLSR) performs the multipoint relay scheme (MPR) which is to manage the data congestion in the hash-key. Pandey and Ratnesh [15], Puneeth and Parthasarathy [16] proposed a cyber-security system in the blockchain hash-key. These implements the set of NIST tests based on the self-checking process to identify the DOS attack and protect the data from attackers. Farouk et al. [17] proposed the comprehensive identity authentication scheme (CIAS) based an encryption model which is worked as the asymmetrical model. This provides the security and privacy to the blockchain communication system. A blockchain based mobile edge computing was performed by Puneeth and Parthasarathy [18]. This provides the trusted central entities that are in the single point failure cases. Similarly, while facing the challenges in the security model of blockchain hash-key. Saha et al. [19] proposed intelligent transportation system (ITS) for secure data transmission to overcome the issues in the hash-key environment. Also, Zaabar et al. [20] presented an overview of blockchain security system and the privacy design of algorithm. For reliable data acquisition in the blockchain. Yaqoob et al. [21] proposed a dynamic entity-centric trust model of blockchain security system. Similarly, to manage the DDOS attack. El-Rahman and Ala-Saleh [22] proposed Trust-based Framework for Reliable Data Delivery and DoS defense (TFDD) for the blockchain architecture for the development of intrusion detection module. Li et al. [23] implemented the Massive Open Online Courses (MOOCs) based on the blockchain model. In that, the system requires more learning records to perform the secure data storage process. For that, Electronic Learning Records (ELRs) was used in the MOOCs to perform efficient conditional anonymity, secure storage, and sharing without the need for sophisticated cryptographic calculations. Ajao et al. [24], Liu et al. [25] Kumar and Rakesh [26] Jafar [27], Jyoti and. Chauhan [28] proposed a crypto-hashing technique to secure the data by the encryption process and the data privacy detection system.

2. MATERIALS & METHODS

The methodology structure and the algorithm details are explained briefly in this section. Figure 2 shows the flow diagram of proposed work model for the appropriate security and secure transmission system. In this security system, the patient details are preserved by generating an efficient key pattern for the indexing of data blocks to represent the private key for individual patients. The blocks are considered for the overall hospital management system. This it contains the details of doctor and the patient information in the overall hospital database. The link information about the patient and doctor details are preserved by the proposed Intuitionist Derivative Symmetrical Encryption (IDSE) algorithm. The combination of the proposed key pattern and the encryption model increased the data security system compare to traditional encryption model.

The symmetrical encryption system has the advantage of data storage of larger data size and the less time complexity. And in the medical field the patient's data such as MRI, CT-SCAN, X-Ray and other information's are of higher size. Also, the random key generation helps to improve the secure data storage in a model. For that, the hashing technique enhances the random key pattern and provides better security parameters for the huge amount of data storage in the blockchain environment.

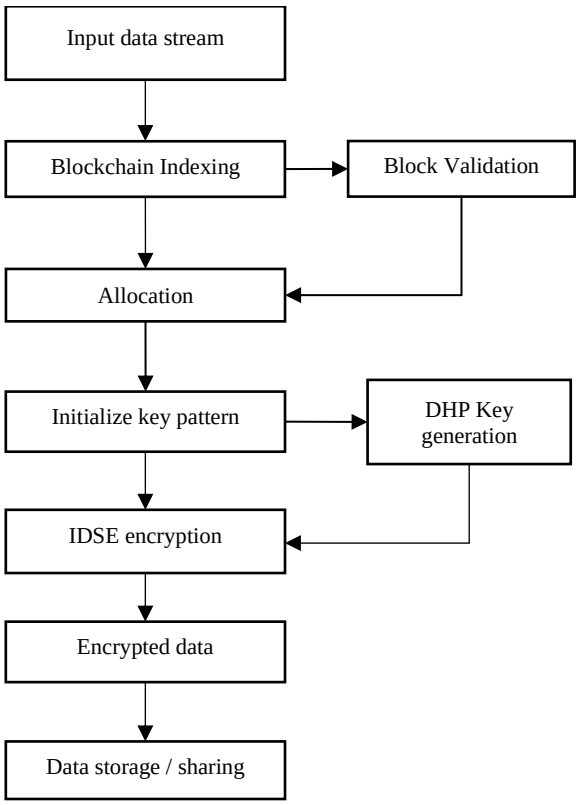

Figure 2. Overall flow of the proposed system

Similarly, the hash-key generation system achieved the high throughput of random key generation for the secure data transmission model and also for the data management process. Since, the encryption time is depending on the amount of data and the size of key formation. This can be reduced by the implementation of DHP based data encryption model that achieved the light-weight encryption model. This can be achieved the high speed transmission rate than by using other state-of-art methods. The proposed work is segmented as two major class that are listed as follows.

A. Intuitionistic Derivative Symmetrical Encryption,
B. Differential Hashing Pattern.

2. 1. Intuitionistic Derivative Symmetrical Encryption The main intension of this data security algorithm is to optimize the data size with high security model. For this process, the light-weight encryption model was integrated to achieve the high security model with reduced size of data bits. This overall encryption model is depending on the hash key pattern generation block to retrieve the encoded data from the bit stream of data. The architecture of the encryption and the decryption model is shown in Figure 3. In that the encoder was divided as two individual blocks to represent the generation of random address and the random key value for the data encoding process. This it refers the generation of private and public key pattern generation for the overall encryption model. The step-by-step procedure with the equation model of IDSE algorithm is presented in Algorithm 1.

Algorithm 1. IDSE based Data Security algorithm

Input: Data samples (D_i)
Output: Encrypted Data (E_D)
Select the random key size as 64-bit chipper (R_b).
Split the data samples into 16-bit block size. This can be represent as the function block f_k.
Construct the data blocks.
Retrieve the $R_{a_i}f_k$ by extracting the 16-bit blocks from Equation (1).
Construct M1, M2, M3, M4 matrix from Equations (2) to (5) based on the block function 'f'.
Estimate the keys as K1, K2, K3, K4 from Equations (6) to (9).
Estimate the key K5 from Equation (10).
Perform the XOR operation to extract the bitwise character '$Y_{o_{i,j}}$' and concatenate encrypted bit sequence from Equation (11).

Let the message can be segment as the blocks which can be represent as in Equation (1).

$$Ra_i f_k = f(Rb_i f_k) \quad (1)$$

where,

$$Rb_i f_k = \left\| \left(R_{b_{4(j-1)+i}} \right)_{j=1}^{4} \right.$$

To estimate the encryption key pattern, the transformation can be estimate by the random table value that are from the Hexa-decimal value. The table can be represented by the matrixes M1, M2, M3 and M4, respectively. This can be followed by the Equations (2) to (6).

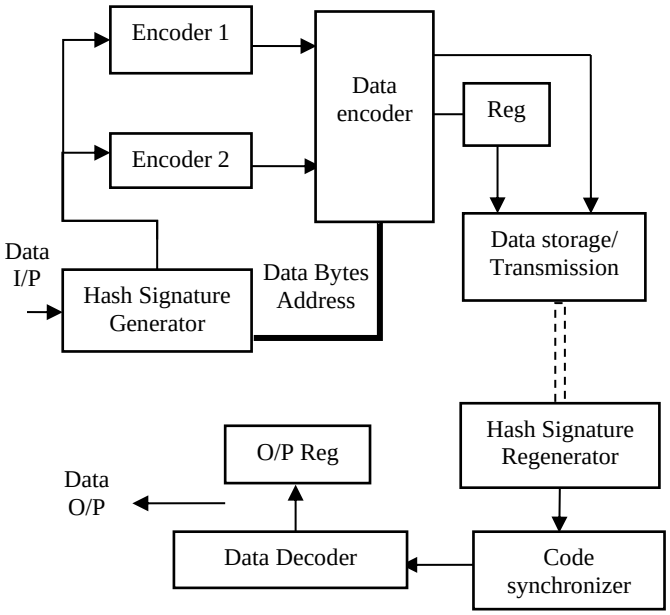

Figure 3. Architecture Diagram of Proposed Data Storage/ Transmission System

$$M1 = \begin{bmatrix} Ra_1f_1 & \dots & Ra_1f_4 \\ \dots & \dots & \dots \\ Ra_1f_{13} & \dots & Ra_1f_{16} \end{bmatrix} \quad (2)$$

$$M2 = \begin{bmatrix} Ra_2f_1 & \dots & Ra_2f_4 \\ \dots & \dots & \dots \\ Ra_2f_{13} & \dots & Ra_2f_{16} \end{bmatrix} \quad (3)$$

$$M3 = \begin{bmatrix} Ra_3f_1 & \dots & Ra_3f_4 \\ \dots & \dots & \dots \\ Ra_3f_{13} & \dots & Ra_3f_{16} \end{bmatrix} \quad (4)$$

$$M4 = \begin{bmatrix} Ra_4f_1 & \dots & Ra_4f_4 \\ \dots & \dots & \dots \\ Ra_4f_{13} & \dots & Ra_4f_{16} \end{bmatrix} \quad (5)$$

The key pattern can be represented by concatenating the bit sequences that are for each block which can be estimated by Equations (6) to (10).

$$K1 = \{\{a_4, \dots a_1\}, \{a_5 \dots a_8\}, \{a_{12} \dots a_9\}, \{a_{13} \dots a_{16}\}\} \quad (6)$$

$$K2 = \{\{b_4, \dots b_1\}, \{b_5 \dots b_8\}, \{b_{12} \dots b_9\}, \{b_{13} \dots b_{16}\}\} \quad (7)$$

$$K3 = \{\{c_4, \dots c_1\}, \{c_5 \dots c_8\}, \{c_{12} \dots c_9\}, \{c_{13} \dots c_{16}\}\} \quad (8)$$

$$K4 = \{\{d_4, \dots d_1\}, \{d_5 \dots d_8\}, \{d_{12} \dots d_9\}, \{d_{13} \dots d_{16}\}\} \quad (9)$$

$$K5 = \bigoplus_{i=1}^{4} K_i \quad (10)$$

From this the ciphered data can be represented as in Equation (11).

$$E_D = \{R_{51}, R_{52}, R_{53}, R_{54}\} \quad (11)$$

where,

$$R_{o_{i,j}} = \begin{cases} Y_{x_{i,j}} \odot K_i \quad ; \quad j = \{1, 4\} \\ Y_{x_{i,j+1}} \oplus K_i; \quad j = 2 \\ Y_{x_{i,j-1}} \oplus K_i; \quad j = 3 \end{cases}$$

2. 2. Hashkey Generation using DHP From the cryptographic system, the data security can be defined by the bit size of random key that are initialized for encryption process**.** The more the size of key size can increase the security level in traditional cryptographic system. This will lead to increasing the data size for storage and transmission process. This may also lead to reduce the throughput of overall system. To overcome, the key pattern are needs to improve and to reduce the size of key with the rate of high security level. This can be achieved by using the light-weight cryptographic system. Compare to the traditional model such as AES, DES, ECC and other types of encryption techniques, the key size was managed and the size was appropriately used according to the properties of data streams that are to transmit over the hash-key structure.

The detailed steps for the DHP based data encryption model was described in Algorithm 2.

Algorithm 2. Differential Hashing Pattern (DHP)

Input: Data input, D_r
Output: Hash key patternE_T.

For$i = 1\ to\ n$loop// 'n' is the size of data,T_i in meta-blocks M_v
For$j = 1\ to\ m$loop all resources // Loop running for all the selected resources R_j
Calculate the pattern of key formation, $C_{ij} = D_{ij} + R_j$
Where, R_j – Random weight value for the related parameters of data structure. Ranges from 0->1.
While Key_Bins in Mv do
Find the bins of data structure for each data samples with respect to time.

$$T_k = sort(C_i(t))$$

Find the respective key bits to encrypt the data from T_k.

$$Y = min(T_k)$$

Estimate binaries for$Y$ to the random sequenceR_j
Make zero's in$T_k$that are irrelevant to the pattern fromM_v
End while
Update R_j
Update C_{ij} for all i
End loop 'j'
Perform XOR operation to represent the hash key result of overall bit size$E_T(i)$
End loop 'i'.

3. RESULTS AND DISCUSSION

In this section, the simulation results and the testing analysis of the proposed model of blockchain security system. The performance of the proposed work was validated by the comparison of data delivery ratio with the delay rate and other related parameters from existing security algorithm and the hash-key system. Here, the overall design work was implemented in the PYTHON tool for the version of 3.8. the comparison parameters are considered for the traditional security system and for proposed blockchain based data security model. The environmental setup for the result analysis are referred by Li et al [23] and Ajao et al. [24]. In this, the comparison results are validated for the amount of data packets that are considered for data transmission and the storage system from the traditional model and by the blockchain model. The size of data packets was varied according to the size what are specified by Li et al. [23]. To estimate the performance of data security, the comparison is taking in the part of number of packets that are considered for the transmission and amount of time taken to transmit it. The testing results are calculated from the data transmission structure of blockchain architecture to

represent the QoS in a hash-key. The parameters that are considered for the comparison are can be listed as follows:

1. Data Delivery Ratio % (DDR),
2. Data Confidentiality Ratio % (DCR),
3. Data Integrity Ratio % (DIR),
4. Privacy Preserving Ratio % (PPR) and
5. Time Consumption (Sec)

3. 1. Data Delivery Ratio The Data Delivery Rati (DDR) in the unit of percentage is referred to estimate the amount of data that are successively transmitted to the destination with minimum amount of loss. This can be calculated by the ratio of amount of data that are received at the destination block to the total number of data that are transmitted by the source. This can be represented as in Equation (12). This can be multiplied by 100 to get the value in terms of percentage.

$$DDR = \frac{Total\ No.\ of\ data\ samples\ received}{Total\ No.\ of\ data\ sent} \quad (12)$$

The line graph in Figure 4 shows the comparison result of proposed model with the other existing models of blockchain security system introduced by Ajao et al. [24].

3. 2. Data Confidentiality Ratio (%) The IDSE-DHP based appropriate security system achieved the better DCR rate by referring the data loss ratio. This parameter is to calculate the amount of data that are not able to reach the destination which may fail to data loss. This can be represented as in Equation (13).

$$DCR = \frac{(No.of\ Sensitive\ Patient\ Data)}{Total\ No.of\ Data\ samples} \quad (13)$$

3. 3. Data Integrity Ratio (%) The Data Integrity Ratio refers the ratio of number of user data at the receiver without changes (N_{UD}) to the total number of data samples (T_D). This was represented in Equation (14). Figure 5 shows the comparison chart of the DIR (%).

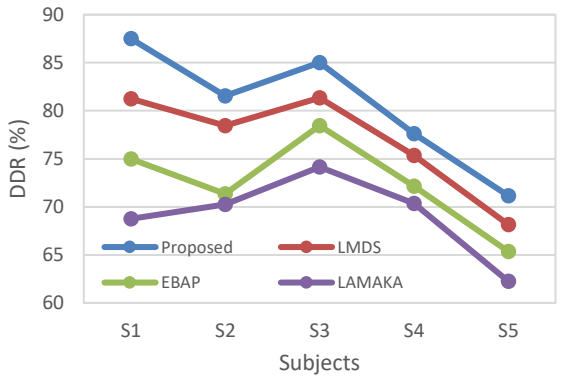

Figure 4. DDR analysis by Ajao et al. [24]

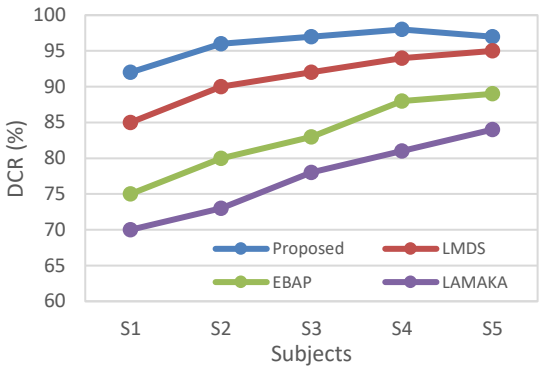

Figure 5. Data Confidentiality Ratio analysis by Ajao et al. [24]

$$DIR = \frac{N_{UD}}{T_D} \times 100 \quad (14)$$

3. 4. Privacy Preserving Rate The privacy preserving rate refers the ratio of number of user data that are in the encrypted form and was secured (N_{SD}) to the total number of available data samples (T_D). This was represented in Equation (15). Figure 6 shows the comparison chart of the PPR.

$$PPR = \frac{N_{SD}}{T_D} \quad (15)$$

The proposed encryption model in the blockchain system was analyzed with the traditional encryption system such as RES, DES and AES techniques for the parameters of Encryption and decryption time referred by El-Rahman and Ala-Saleh [22] in Figures 7 and 8, respectively. The execution time of the encryption system in the blockchain system refers the time consumption for the execution of encryption and the total transmission time. Figure 9 shows the total transmission time in (s) that are compared from the existing IoMT [23] model of data security in blockchain system.

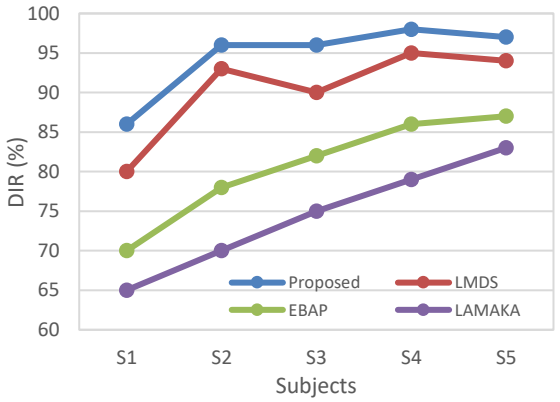

Figure 6. Data Integrity Ratio analysis by Ajao et al. [24]

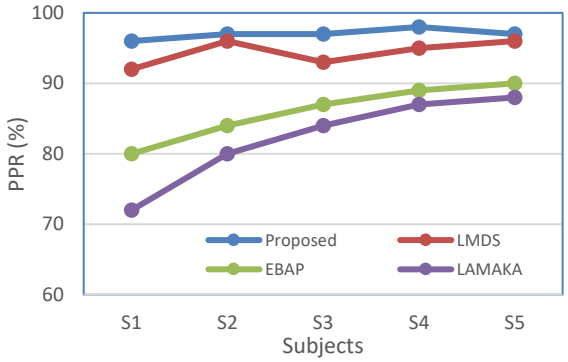

Figure 7. Privacy Preserving Rate by Ajao et al. [24]

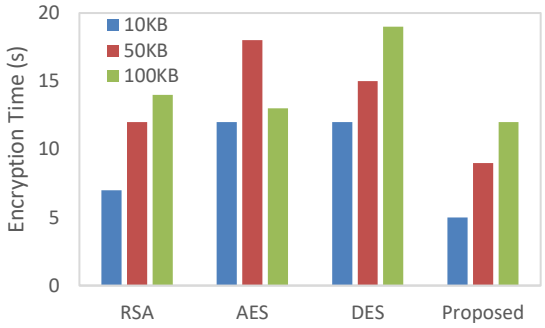

Figure 8. Encryption Time (s) [21]

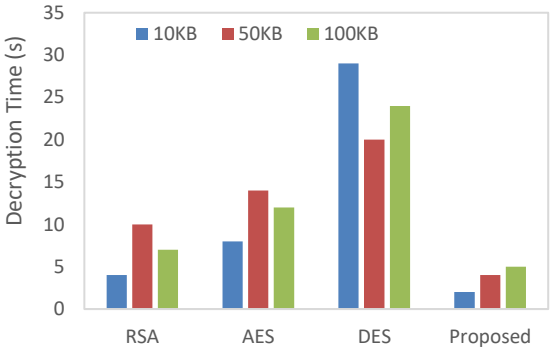

Figure 9. Decryption Time (s) [22]

3. 5. Storage Size Consumption The data storage size was depending on the encryption size and the selective key size for the data security model. This was estimated for the data size in the range of (kB). Figure 10 shows the storage consumption of proposed model compare to other existing systems [23]. This was also evaluated for the different transmission process that are represented in Figure 11 referred to Ajao et al. [24].

The Table 1 and Figure 12, shows the comparison result of proposed encryption time with other existing methods of encryption system. Here the parameters are validated based on the size of file to be encrypted and the number of users that are initialized for the encryption process respectively.

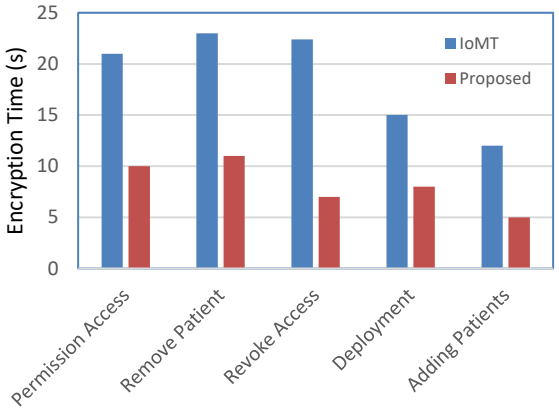

Figure 10. Execution time (s) [23]

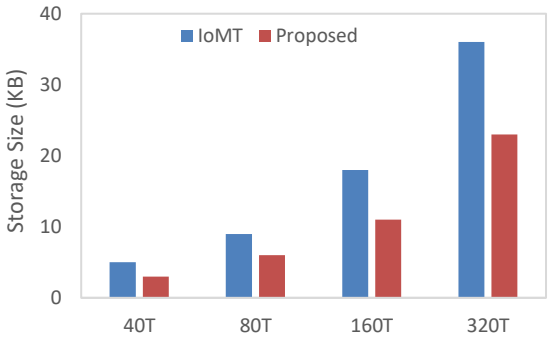

Figure 11. Storage Size (KB) [23]

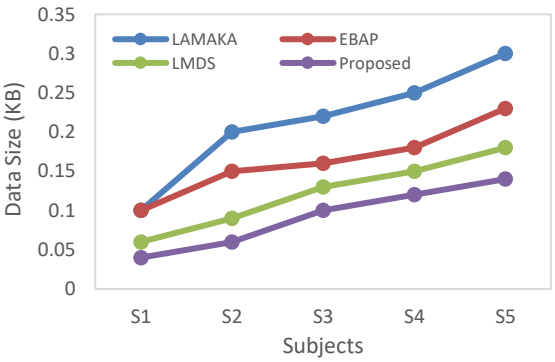

Figure 12. Storage Size (KB) [24]

TABLE 1. Comparison result of encryption time (s) [27]

File Size	Encryption Time (s)				
	BHA	ISA	CGA	BSCDP	Proposed
128	7.6	7.4	3.6	1	0.87
256	12	8.5	5.1	2.7	1.75
512	31	20	8.7	3.5	2.65
768	37.5	24	10	5	4.75
1024	47.8	37.8	12	8.7	7.2

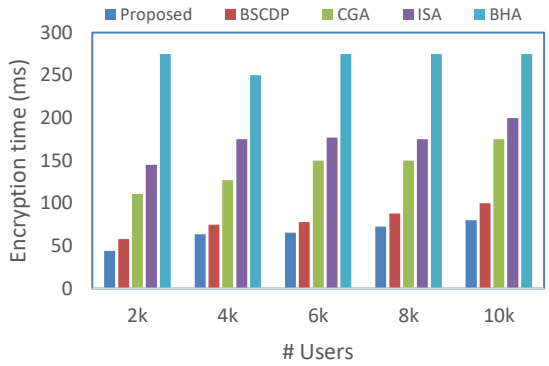

Figure 13. Execution time (ms) [28]

4. CONCLUSION

The security of medical data can be increased through encryption; however encryption and decryption both demand a lot of processing resources. The need for high security, low computational-power encryption techniques is critical. This paper proposed a novel model of blockchain security system with appropriate hash-key security algorithm to achieve high speed data transmission rate. The Intuitionistic Derivative Symmetrical Encryption (IDSE) based data encryption model presented lightweight cryptographic system to reduce the key size based on the hashing technique to generate the random key. This type of data security system along with the blockchain improves the prediction rate and the better security model to achieve the retrieval rate from cloud environment. Similarly, the Differential Hashing Pattern (DHP) based encryption model makes the overall system as light-weighted encryption model for enhanced transmission rate and the improved value of throughput. The analytical results show the performance of proposed design that represents the proposed method gives the less value of delay rate in millisecond and the improved value of data loss ratio at different number of patient blocks. The overall process of this paper was validated for the environment of hospital data management system for patient blocks.

In future, the appropriate security and security system in the blockchain architecture are can be improved by an enhanced model of machine learning technique with data security function in block computing. The hash-key security can be focused on the space complexity by the design of key management.

5. REFERENCES

1. Jameii S. M. and Khanzadi K., "A Latency Reduction Method for Cloud-fog Gaming based on Reinforcement Learning", ***International Journal of Engineering, Transactions C: Aspects,*** Vol. 35, No. 09, (2022) 1674-1681. https://doi.org/10.5829/ije.2022.35.09c.01
2. Fan, K., Wang, S., Ren, Y., Li, H. and Yang, Y., "Medblock: Efficient and secure medical data sharing via blockchain." ***Journal of Medical Systems,*** Vol. 42, No. 8, (2018), 1-11. https://doi.org/10.1007/s10916-018-0993-7
3. Kim, M. G., Lee, A. R., Kwon, H. J., Kim, J. W. and Kim, I. K., "Sharing Medical Questionnaries based on Blockchain," IEEE International Conference on Bioinformatics and Biomedicine (2018), 2767-2769. https://doi.org/10.1109/BIBM.2018.8621154
4. Hussein, A., F., ArunKumar, N., Gonzalez, G., R., Abdulhay, E., Manuel, R., S., J., Tavares. and Hugo C. V., "A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform", ***Cognitive Systems Research***. Vol. 52, (2018), 1-11. https://doi.org/10.1016/j.cogsys.2018.05.004
5. Ramani, V., Kumar, T., Bracken, A., Liyanage, M. and Ylianttila, M., "Secure and Efficient Data Accessibility in Blockchain Based Healthcare Systems," IEEE Global Communications Conference (GLOBECOM). (2018), 206-212. https://doi.org/10.1109/GLOCOM.2018.8647221
6. Zhu, L., Wu, Y., Gai, K. and Choo, K-K, R., "Controllable and trustworthy blockchain-based cloud data management" ***Future Generation Computer Systems,*** Vol 91, (2019), 527-535. https://doi.org/10.1016/j.future.2018.09.019
7. Ismail, L., Materwala H. and Zeadally, S., "Lightweight Blockchain for Healthcare," ***IEEE Access***, Vol. 7, (2019), 149935-149951. https://doi.org/10.1109/ACCESS.2019.2947613.
8. Chen, Y., Ding, S., Xu, Z., Zheng, H. and Yang S. "Blockchain-Based Medical Records Secure Storage and Medical Service Framework" ***Journal of Medical System,*** Vol. 43, No. 1, (2019), 1-9. https://doi.org/10.1007/s10916-018-1121-4
9. Bhattacharya, P., Tanwar, S., Bodkhe, U., Tyagi, S. and Kumar, N. "BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications," ***IEEE Transactions on Network Science and Engineering,*** Vol. 8, No. 2, (2021), 1242-1255. https://doi.org/10.1109/TNSE.2019.2961932
10. Zhou, T., Li, X. and Zhao, H., "Med-PPPHIS: Blockchain-Based Personal Healthcare Information System for National Physique Monitoring and Scientific Exercise Guiding" ***Journal of Medical System,*** Vol 43, No 9, (2019), 1-23. https://doi.org/10.1007/s10916-019-1430-2
11. Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P. and Yu, N., "Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data" ***IEEE Internet of Things Journal***, Vol. 6, No. 5, (2019), 8770-8781. https://doi.org/10.1109/JIOT.2019.2923525
12. Saif, S., Biswas, S. and Chattopadhyay, S. "Intelligent, Secure Big Health Data Management Using Deep Learning and Blockchain Technology: An Overview" ***Deep Learning Techniques for Biomedical and Health Informatics***, Springer, Vol 68. (2020), 187-209. https://doi.org/10.1007/978-3-030-33966-1_10
13. Wang, Z., Luo, N. and Zhou, P. "GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare", ***Journal of Parallel and Distributed Computing,*** Vol. 142, (2020), 1-12, https://doi.org/10.1016/j.jpdc.2020.03.004
14. Abdul- Rahoof T.P. and Deepthi V.R. "Health Chain: A Secure Scalable Health Care Data Management System Using Blockchain" ***Proceedings Springer***, (2020), 380-391. https://doi.org/10.1007/978-3-030-36987-3_25
15. Pandey, P. and Litoriya, R. "Securing and authenticating healthcare records through blockchain technology" ***Cryptologia***, Vol. 44, No. 4, (2020), 341-356. https://doi.org/10.1080/01611194.2019.1706060
16. Puneeth, R.P. and Parthasarathy, G. "A Survey on Security and Interoperability of Electronic Health Records Sharing Using

Blockchain Technology" ***Acta Informatica Pragensia,*** Vol. 12, No. 1, https://doi.org/10.18267/j.aip.187

17. Farouk, A., Alahmadi, A., Ghose, S. and Mashatan, A. "Blockchain platform for industrial healthcare: Vision and futureopportunities" ***Computer Communications***, Vol. 154, (2020), 223-235. https://doi.org/10.1016/j.comcom.2020.02.058
18. Puneeth, R.P. and Parthasarathy, G. "A Comprehensive Survey on Privacy-Security and Scalability Solutions for Blockchain Technology", ***Smart Intelligent Computing and Communication Technology IOS Press.*** (2021), 173-178, https://doi.org/10.3233/APC210031
19. Saha, S., Majumder, A., Bhowmik, T., Basu, A. and Choudhury, A. "A Healthcare Data Management System on Blockchain Framework" ***Communication and Networking,*** (2021), 1-5. https://doi.org/10.1109/SMARTGENCON51891.2021.9645890
20. Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M. and Abid, M. "HealthBlock: A secure blockchain-based healthcare data management system", ***Computer Networks,*** Vol 200, (2021). https://doi.org/10.1016/j.comnet.2021.108500
21. Yaqoob, I., Salah, K., Jayaraman, R. and Al-Hammadi, Y. "Blockchain for healthcare data management: opportunities, challenges, and future recommendations" ***Neural Computing and Applications,*** Vol. 34, No. 14, (2021), 1-16. https://doi.org/10.1007/s00521-020-05519-w
22. ElRahman, S.A. and Alluhaidan, A.S. "Blockchain technology and IoT-edge framework for sharing healthcare services." ***Soft Computing***, Vol. 25, No. 21, (2021), 13753-13777. https://doi.org/10.1007/s00500-021-06041-4
23. Li, D., Han D., Zheng Z., Weng, T., H., Li H., Liu H., Castiglione A. and Li K.-C., "MOOCsChain: A blockchain-based secure storage and sharing scheme for MOOCs learning." ***Computer Standard and Interface- Elsevier***, Vol. 81, (2022). https://doi.org/10.1016/j.csi.2021.103597
24. Ajao, L.A., Umar, B.U., Olajide, D.O. and Misra, S. "Application of Crypto-Blockchain Technology for Securing Electronic Voting Systems" ***Springer Innovations in Communication and Computing. Springer,*** (2022). https://doi.org/10.1007/978-3-030-89546-4_5
25. Liu, J., Zhao, J., Huang, H. and Xu, G. "A novel logistics data privacy protection method based on blockchain" ***Multimed Tools and Applications***, Vol. 81, (2022), 23867-23887. https://doi.org/10.1007/s11042-022-12836-w
26. Kumar, R. and Tripathi, R. "Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology" ***Journal of Supercomputing,*** Vol. 77, (2021), 7916-7955. https://doi.org/10.1007/s11227-020-03570-x
27. Jafar, A. A. "Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare" ***Computer Communications***, Vol. 170 (2021), 200-208. https://doi.org/10.1016/j.comcom.2021.02.002.
28. Jyoti A. and Chauhan, R., K. "A blockchain and smart contract-based data provenance collection and storing in cloud environment" ***Wireless Networks,*** Vol. 28, No. 4, (2022), 1541-1562. https://doi.org/10.1007/s11276-022-02924-y

Persian Abstract

چکیده

زمینه و هدف: در سیستم مراقبت های بهداشتی و محیط بیمارستان، امنیت داده ها و اتصال داده ها از عوامل اصلی برای سیستم مدیریت داده های بیمار است. برای آن، چندین تکنیک برای حفظ و مرتب کردن داده های بیمار با سیستم امنیتی پیشرفته استفاده می شود. به این ترتیب، ساختار بلاک چین مدیریت داده، فرآیند ذخیره سازی و انتقال ایمن داده را بهبود می بخشد. اهداف: در سیستم امنیت داده، معیار کیفیت را می توان با استفاده از اندازه کلیدی که برای فرآیند رمزگذاری استفاده می شود، تایید کرد. در ترکیب با بلاک چین، مدل رمزگذاری برای حل مشکل در سیستم امنیت داده ها بهبود می یابد. این همچنین باید بر کاهش اندازه ذخیره سازی داده ها به دلیل اندازه کلید بزرگ داده های رمزگذاری شده تمرکز کند. روش‌ها: در کار پیشنهادی، الگوریتم امنیتی مبتنی بر الگوریتم رمزگذاری متقارن مشتق شهودی (IDSE)همراه با عملکرد بلاک چین برای تشکیل فرآیند ذخیره‌سازی و انتقال داده مجاز یکپارچه شد. برای تولید الگوی کلید، مدل استخراج الگوی کلید مبتنی بر الگوی درهم‌سازی دیفرانسیل (DHP)برای انتقال داده‌ها با سرعت بالا و کاهش اندازه داده‌هایی که رمزگذاری شده‌اند، استفاده شد. ویژگی هایی که برای سیستم امنیتی مناسب در نظر گرفته می شود، الگوی انتقال داده ها با توجه به زمان و مدل هش سازی تولید کلید است. نتایج: در تجزیه و تحلیل نتایج، عملکرد IDSE-DHP با پارامترهای انتقال داده و نرخ تلفات در بلاک چین و با ویژگی‌های مربوط به توان عملیاتی تایید می‌شود.