Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 8, pp. 2483–2494
DOI : 10.47974/JDMSC-2132

A novel optimization-based blockchain technology using health care data for enhancing security and privacy in the medical system

K. Kavita [^]
Department of Mathematics
BVRIT HYDERABAD College of Engineering for Women
Hyderabad 500090
Telangana
India

Raghavendra Kulkarni [†]
Department of Computer Science
Amrita School of Computing
Amrita Vishwa Vidyapeetham
Mysuru 570026
Karnataka
India

A. Hanumat Prasad [§]
Department of Computer Science and Engineering
Kallam Haranadha Reddy Institute of Engineering & Technology
Guntur 522019
Andhra Pradesh
India

Balajee Jeyakumar [‡]
Department of Artificial Intelligence and Data Science
Mother Theresa Institute of Engineering and Technology
Palamaner
Chittoor 517408
Andhra Pradesh
India

[^] *E-mail:* kavitha.k@bvrithyderabad.edu.in
[†] *E-mail:* raghavendrakulkarni@my.amrita.edu
[§] *E-mail:* hanuma.alahari@gmail.com
[‡] *E-mail:* balajeej04@gmail.com

Manyam Thaile [$]
Department of Information Technology
Anurag University
Venkatapur, Ghatkesar
Medchal–Malkajgiri District
Hyderabad 500088
Telangana
India

Santosh Gore *
Sai Info Solution
Nashik 422002
Maharashtra
India

Abstract

This study introduces an Ant Lion-based Advanced Encryption Standard with Blockchain (ALAESB) model to enhance security and privacy in healthcare data management. Utilizing cloud storage, Electronic Health Records (EHR) are encrypted using AES and authenticated via blockchain. The methodology integrates hash functions and Merkle trees for data validation and secure block storage. Key generation is optimized through antlion fitness updates, ensuring efficient encryption and decryption processes. The model aims to mitigate privacy risks and secure patient data access for healthcare providers, emphasizing reliability and integrity in medical data handling.

Subject Classification: *68P25, 68P27.*

Keywords: *Blockchain, Advance standard encryption, Patient data, Session key, Cloud.*

1. Introduction

Blockchain-based healthcare technology offers advanced storage, trust in data sharing, and decentralized transactions in the healthcare sector [1][2]. Confidentiality and sanctuary concerns are the emphasis of information sharing in the sector. Healthcare providers need secure, fast access to critical patient data for treatment decision-making, recommendations, diagnosis, and quality care services. Blockchain provides a secure distributed ledger for sharing medical information, data verification, secure storage, and data sharing [3].

[@] *ORCID-ID :* **0000-0003-1814-5913**

[$] *E-mail:* **manyamthaile@gmail.com**
* *E-mail:* **sai.info2009@gmail.com (Corrsponding Author)**

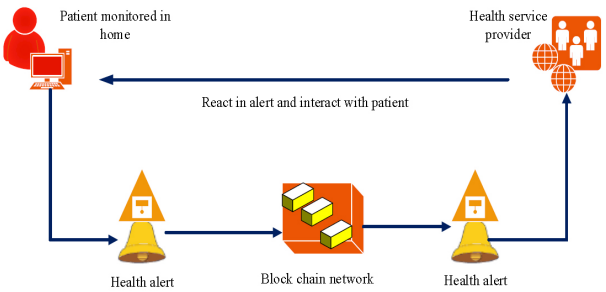

Figure 1

Remote patient monitoring system

Figure 1 shows the blockchain technology offers innovative methods for executing transactions, storing information, and establishing trust in an open environment [4][5]. It is particularly useful in managing medical records, patient data, and insurance claims. However, private information in medical data, particularly in Electronic Health Records (EHR), poses risks such as information tampering and disclosure [6][7]. The growing interest in blockchain technology is driven by the probable for e-health and medical services. Healthcare providers can access, analyze, and provide timely medical support using mobile devices [8][9]. To enhance security and privacy in healthcare data, a novel optimization-based blockchain model is designed. This model involves collecting and training patient datasets, designing an ALAESB model in the cloud, transferring datasets, generating session keys, handling encryption, and storing data in blocks [10]. The model's performance is compared with other techniques in standings of dispensation time, encryption period, decryption time, and latency.

2. Related work

Gautam Srivastava et al. [11] developed the Patient-Oriented Privacy Preserving (PP) Access Control (POPPAC) technique for accessing and controlling private medical information using blockchain technology. The model offers high reliability and bandwidth but faces security issues. Shekha Chenthara et al. [12] developed the PP technique through a health chain with blockchain technology to ensure data sanctuary and patient confidentiality while transferring sensitive data to healthcare providers. The model offers better security against cyber-attacks but has high scalability and confidentiality issues. Dinh et al. [13] proposed a new EHR sharing technique that syndicates the Interplanetary File System (IPFS)

and blockchain in the cloud platform. The model achieves low latency, and high privacy and security levels, but less integrity and information leakage issues. Majid Bayat et al. [14] proposed efficient and secure attribution encryption and blockchain for recording and storing medical data and protecting user privacy. Yi Chen et al. [15] proposed a novel storage technique for managing personal medical data using cloud storage and blockchain, comparing its features with traditional schemes. The designed model doesn't depend on single or third parties but has absolute power to affect the processing system but lower sharing rates.

3. System Model and Problem Definition

Limited storage capacity in hospitals increases the risk of storing medical private information. Cloud databases store provider signatures, session keys, references, EHR, and medical records. Blockchain technology stores all data transactions, providing efficient and safe storage of patient EHR. However, challenges such as data confidentiality, sharing, authentication, security, interoperability, and security remain. Patients can access stored data using session keys, but these challenges must be addressed for effective and secure storage.

Figure 2 shows the novel optimization-based cryptographic technique with blockchain is being developed to secure Electronic Health Records (EHR) from third parties and attacks, addressing the main issue of scalability and data integrity due to the centralization of blockchain storage and the potential for unauthorized access.

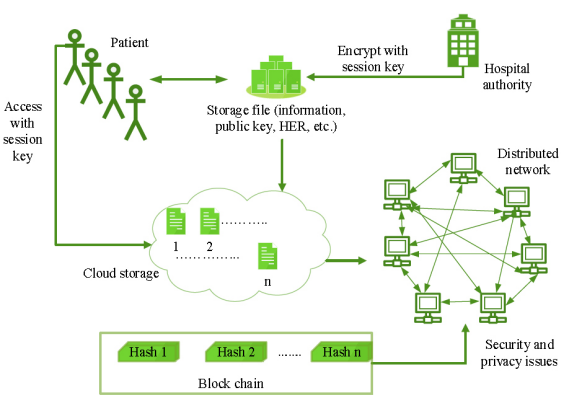

Figure 2

System model and problem definition

4. Proposed System

The design of an Ant Lion-based Advanced Encryption Standard with Blockchain (ALAESB) aims to boost the sanctuary and confidentiality of patient healthcare data. The model stores patient data in the cloud under the name of Electronic Health Record (EHR), accessed by organization administrators. The model stores hash health records and vast data in the encryption process, allowing only true patient records to be added to the blockchain for authentication. The architecture is illustrated in Figure 3.

The EHR is stored in a cloud database encrypted using AES, a unique civic key cryptographic algorithm, generating a robust blockchain solution. Keys are generated during encryption, and the model's performance is enhanced by updating the antlion fitness. Blockchain blocks are verified using an optimized algorithm, each containing a hash function.

$$h_{ash}12 = h_{ash}(h_{ash1} + h_{ash2}) = h_{ash}[(T_{x1}.h_{ash}) + (T_{x2}.h_{ash})]$$

The model uses a Merkle tree structure to store data in blocks, with the previous hash for block validation and the timestamp representing the block's creation time. Nonce generates the hash value at a difficult level. EHR is encrypted and stored in a cloud database, with hash values recorded using Ant Lion Fitness.

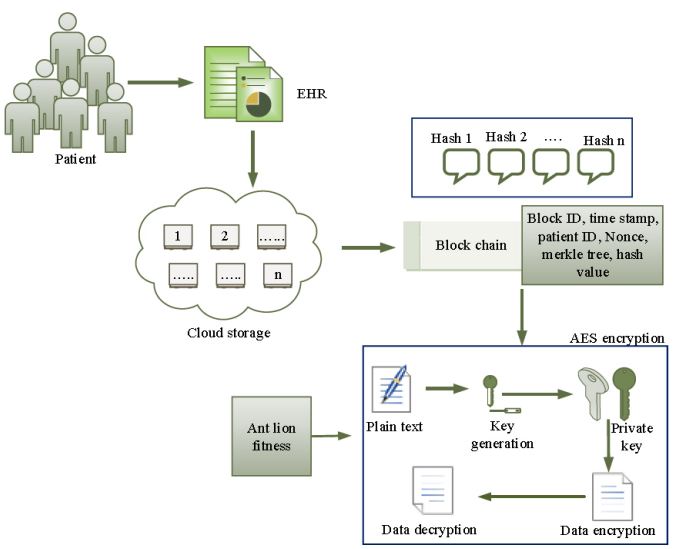

Figure 3

Proposed methodology

4.1 *Ant Lion-based Advanced Encryption Standard*

Generally, the symmetric algorithm is used for the encryption of healthcare data which contains private key encryption for encryption and decryption using the same key. Initially, key generation is more essential to communicate the data among hospitals service providers, and authorized medical entities. It contains the K_{mk} main key for generating the session key based on the main key. In this phase, update the antlion fitness for enhancing the performance of key generation. It is one of the hunting mechanisms that attack the prey. Moreover, randomly walk to the target region and find out the prey with high fitness. This fitness is used for our designed model, generating a suitable key to the patient dataset. The keys are generated using Eqn. (1)

$$K_g = A_f^t + \frac{K_{MK}}{S_{ky}}(h_{ash1} + h_{ash2})B_1B_2 \tag{1}$$

Let (Aft be the fitness of the antlion, and let Sky be a session key which is assumed to be treated as bilinear pairing. The resulting key was derived based on the hash value. Thereafter, from the hash value, the patient derives two random numbers, i.e., x and y. After that, the patient computes the key proportional value, which is obtained using Equation (2).

$$SK_g = (G = D^{(\theta+\mu)/\alpha}B_1\,B_2) \tag{2}$$

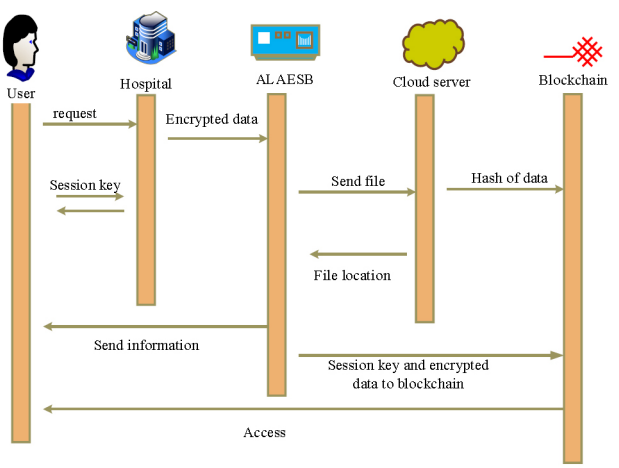

Figure 4

Process of the designed model

Finally, provides the secure key of healthcare data to the medical entities and patients also session key is generated to encrypt and decrypt the data through the identical key. Thus, the session key is equal to the $xy = x(yB) = xyB$ likewise $yX = y(xB) = xyB$. So, patients, system administrators or staff, and doctors used this designed technique for sharing the key through a secure network. The process of the designed model is shown in Figure 4.

Moreover, the hash function is helpful for message authentication and other authentication. Generally, the hash value is infeasible for identifying the original messages. So, the hash function is obtained using Eqn. (3)

$$h_{ash}(x) = h_{ash}(y) \tag{3}$$

This encryption of health data for the patients is based on particular attributes, and the patient generates an appropriate pair of private keys to gain access to his details. The generated information is then encrypted, and the patient's information is signed using a private key. The details of this patient are then stored later on the blockchain. In addition, the suggested model generates a random key to encrypt the data, which transmits the encrypted data to the patient. The encryption of data is done using Equation (4)

$$g_k(s) = S_{ky}, Q_s(t) = S_{sk}^i, (K_g = P_{at})_{i \in S_{ky}} = P(t) \rightarrow c(t) \tag{4}$$

Let, p(t) be represented as input data and c(t) is painstaking as cipher text. Moreover, patient data are encrypted through the private key $Q_s(t)$ by random locations in the cloud. Moreover, changes in the original data cause the hash value that cannot ensure the modified medical data.

The encrypted data is directed to the blockchain, where medical chronicles are arranged based on time and stored in blocks with hash values. The encrypted data is securely transmitted to the patient through the session key Sky, which provides a unique ID based on stored data, as shown in Eqn. (5).

$$P_a(ID, S_{ky,} Address, folder, access) \tag{5}$$

$$store(ID, S_{ky}, EHR) = hash\_ID \tag{6}$$

The model securely stores encrypted data under sleeve, binder, and hash ID, and encrypts and uploads EHR data to a cloud database. The model generates a session key for decryption, allowing access to the

patient. This model achieves low processing, encryption, and decryption times, ensuring the security of medical data.

5. Results and Discussion

The ALAESB framework is implemented in a Python tool and its efficiency is measured against existing techniques. 200 patient data is collected and trained, with the method encrypting data using blockchain to secure it from third parties. The model's efficiency is verified by comparing it with other models, ensuring a secure and efficient system.

Table 1
Validation of Encryption Time

Metrics	No. of data	BbPIM	PIPER	SEHRB	Proposed
Encryption time (ms)	50	0.5	0.7	0.13	0.05
	100	0.10	0.23	0.19	0.09
	150	0.17	0.31	0.27	0.12
	200	0.25	0.42	0.36	0.15
Decryption time (ms)	50	0.1	0.5	0.7	0.02
	100	0.5	0.9	0.13	0.09
	150	0.7	0.11	0.17	0.15
	200	0.25	0.18	0.26	0.17
Throughput (Kbps)	50	450	270	345	850
	100	412	263	333	840
	150	386	250	320	832
	200	340	233	311	811
Processing time (ms)	50	165	130	170	60
	100	174	140	176	65
	150	188	147	181	72
	200	198	156	188	79
Network Latency (ms)	50	65	80.4	112	30
	100	71.5	86.43	122.5	33.4
	150	79	91.4	129	38
	200	84.2	99.8	133.5	41.6

5.1 *Performance Metrics*

The ALAESB technique, implemented in Python, is compared to existing techniques like the Blockchain-based Patient Information Medical System, Privacy Preservation of EHR, and Secure EHR-based Blockchain, based on performance metrics such as throughput, encryption time, latency, and decryption time. Figure 5-7 shows the performance result of proposed model.

5.2 *Encryption duration*

The encryption duration is the time occupied by an algorithm to generate ciphertext from plain text, indicating the speed and efficiency of the encryption method. It is calculated using Eqn. (7).

$$E_t = \frac{TE_{pt}(byte)}{e_t(ms)} \tag{7}$$

Where TE_{pt} is denoted as total encrypted plain text and ^{i}t is denoted as encryption time. The validation of encryption time is detailed in Table 1.

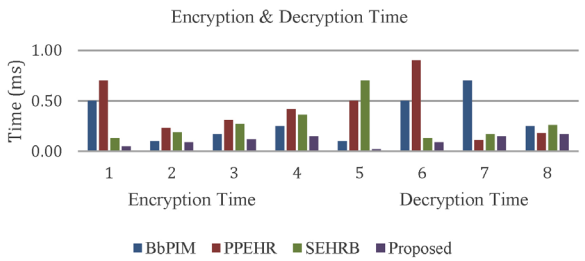

Figure 5

Comparison of encryption and Decryption time

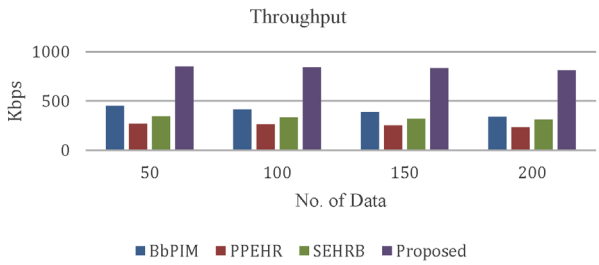

Figure 6

Comparison of Throughput

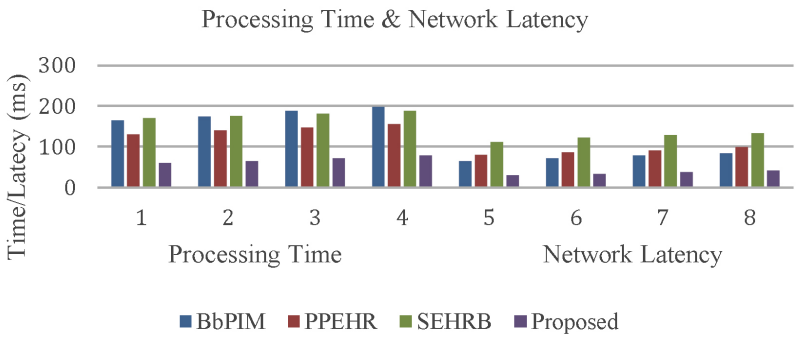

Figure 7

Comparison of Processing Time and Network Latency

6. Conclusion

In this paper, a blockchain-based ant lion AES mechanism is proposed to protect the information and secure data from attacks and third parties. Here, the developed technique employs both encryption technique and optimization techniques. Moreover, antlion optimization is developed to prevent the data from attackers. The hash values in the blockchain separate the data into several blocks. Consequently, the proposed technique has achieved better results. Also, the proposed technique performances are compared in standings of encryption time, decryption period, throughput, processing time, and network latency. Subsequently, the created model accomplished a higher throughput of 850Kbps, and a lower processing time of 60ms while transferring the packets.

References

[1] H. Fatima, M. Khan, A. A. Khan, and M. Nasir, "In search of happiness quotient: An empirical evidence of work-life balance in the Indian health care sector," *Journal of Statistics and Management Systems*, vol. 25, no. 5, pp. 1293-1302 (2022).

[2] S. Khan, A. Al-Dmour, V. Bali, M. R. Rabbani, and K. Thirunavukkarasu, "Cloud computing based futuristic educational model for virtual learning," *Journal of Statistics and Management Systems*, vol. 24, no. 2, pp. 357-385 (2021).

[3] S. Gore, A. S. Deshpande, N. Mahankale, S. Singha, and D. B. Lokhande, "A Machine Learning-Based Detection of IoT Cyberattacks in Smart City Application," in International Conference on ICT for Sustainable Development, Singapore, pp. 73-81 (2023).

[4] N. Mahankale, S. Gore, D. Jadhav, G. S. P. S. Dhindsa, P. Kulkarni, and K. G. Kulkarni, "AI-based spatial analysis of crop yield and its relationship with weather variables using satellite agrometeorology," in 2023 International Conference on Advanced Computing Technologies and Applications (ICACTA), pp. 1-7 (2023).

[5] Priyanka, B. Keswani, and R. Hussain, "Assimilation of blockchain over cloud computing," *J. Discrete Math. Sci. Cryptogr.,* vol. 24, no. 8, pp. 2267-2277 (2021).

[6] G. Ramesh, A. Sharma, D. V. Lalitha Parameswari, Ch. Mallikarjuna Rao, and J. Somasekar, "Blockchain in healthcare : Moving towards a methodological framework for protecting Biomedical Databases," *J. Discrete Math. Sci. Cryptogr.,* vol. 25, no. 4, pp. 891-901 (2022).

[7] A. Panwar and V. Bhatnagar, "Analyzing the performance of data processing in a private blockchain-based distributed ledger," *J. Inf. Optim. Sci.,* vol. 41, no. 6, pp. 1407-1418 (2020).

[8] M. Miah, S. J. Miah, and S. Venkatraman, "Blockchain: At a glance idea for information science researchers," *J. Inf. Optim. Sci.,* vol. 42, no. 7, pp. 1589-1624 (2021).

[9] G. Iovane, L. Sensini, P. Di Geronimo, A. Rapuano, and A. Briscione, "TES: Token evaluation system for blockchain contexts," *J. Interdiscip. Math.,* vol. 25, no. 8, pp. 2093-2111 (2022).

[10] N. Mishra and R. K. Singh, "Prioritisation and security defence algorithm for cloud-specific vulnerability through scoring and base metric group," *J. Interdiscip. Math.,* vol. 23, no. 2, pp. 481-491 (2020).

[11] H. Wu, A. D. Dwivedi, and G. Srivastava, "Security and privacy of patient information in medical systems based on blockchain technology," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 17, no. 2s, pp. 1-17 (2021).

[12] Shekha Chenthara, Khandakar Ahmed, Hua Wang, Frank Whittaker, and Zhenxiang Chen, "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology," PLoS One, vol. 15, no. 12, p. e0243043 (2020).

[13] D. C. Nguyen, L. T. Nguyen, A. T. Nguyen, and N. T. Nguyen, "Blockchain for secure EHRs sharing of mobile cloud-based e-health systems," *IEEE Access,* vol. 7, pp. 66792-66806 (2019).

[14] S. M. Pournaghi, M. Bayat, and Y. Farjami, "MedSBA: A novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," *J. Ambient Intell. Humans. Comput*., vol. 11, no. 11, pp. 4613-4641 (2020).

[15] Y. Chen, X. Wang, J. Liu, and Z. Zhao, "Blockchain-based medical records secure storage and medical service framework," *J. Med. Syst.,* vol. 43, no. 1, pp. 1-9 (2019).

Received February, 2024