International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

# A Novel Hybrid Optimization Approach for Securing Health Information using Block Chain

[1]Sunil Gupta, [2]Ritika Mehra, [3]Srikanth V, [4]Mohan Vishal Gupta

**Submitted:**17/04/2023 **Revised:**12/06/2023 **Accepted:**21/06/2023

**Abstract***:* Protecting patients' medical records from unapproved entry, communicating with transports such as ambulances, and employing intelligent electronic health monitoring. Due to a lack pertaining to the countless the healthcare system's expert design of security protocols, numerous security risks exist, including authenticity and data sharing, and medical data transmission. In such instances, Utilization of the block chain protocol. This study proposes an scalable block chain network for healthcare data security utilizing a novel elephant herding integrated salp swarm optimization (EHISSO) to generate a wise with a safe healthcare infrastructure. In the context, block chain is a distributed ledger that distributed ledger system and distributed ledger technology comprised of multiple segments connected by digital signature schemes and consensus mechanisms, and a a series of hashes, and provides highly secure storage capabilities. EHISSO is used to optimize the parameters of including block capacity, number of transactions, and the quantity of block chain channels. With the evolution of EHISSO, provide new features that improve protection and scalability. For healthcare technologies, the experimental results of the recommended procedure are greater to those of conventional approaches such as KNN, LSTM, and VGG.

***Keywords:*** *Healthcare system, security, block chain, elephant herding integrated salp swarm optimization (EHISSO).*

## 1. Introduction

The healthcare system is made up of numerous entities that hold patient health information in a system that is protected by various rules. Securing health-related data is becoming increasingly difficult due to the involvement of numerous hackers and the harm that natural disasters are causing to system nodes ([1]. Healthcare data must be stored and secured according to a number of rules because it is extremely sensitive. Sharing medical information is one of the most important and well-known services since it affect the patient's life [2]. The medical data is stored and secured using block chain-based technologies in the healthcare industry. A decentralized and distributed technology called block chain is used in this system to provide clinicians and the government with patient healthcare data (Li et al., 2019). Its primary function is to gather information from many sources, including patient information, doctor availability, and ambulance services. A block chain is then updated with the messages. The central authority determines if the communication is relevant or not before sending it to the doctor because when the system receives too many communications, data transfer is slowed. Medical information is stored and shared through a variety of methods, which might create delays and information leaks. Internet of things (IoT), sensors, as well as 5G were previously used gadgets. Previous efforts have had issues with the leaking of medical data while maintaining, exchanging, and preserving the personal information [3]. When there are numerous internet systems connected to healthcare institutions, it causes patients to become confused about which system they should be sending their message to, which results in the leaking of medical data. The prior approach made use of Centralized hardware and external systems, which led to leakage and insecure messaging. Using a decentralized system like the block chain that stores and shares data very quickly and does not accept third-party invitations [4].Unified and distributed ledger technology called the block chain that comprises of several blocks connected by consensus algorithms, digital signature methods, and chains of hashing, provides extremely stable storage capabilities. The innovative aspect of this research is the reduction of computing cost, key generation time, and encryption time [5]. Integrity and Authentication are used to confirm security. Figure 1depicts the health care system. The research, an elephant herding integrated salp swarm optimization (EHISSO) optimization-based efficient block chain network for protecting healthcare data is suggested.

*1Associate professor, School of Computer Science & System, JAIPUR NAITONAL UNIVERSITY, JAIPUR, India, Email Id: sunil95@rediffmail.com*
*2Professor, School of Engineering and Computer, Dev Bhoomi Uttarakhand University, Uttarakhand, India, Email Id: dean.socse@dbuu.ac.in*
*3Associate Professor, Department of Computer Science and IT, Jain(Deemed-to-be University), Bangalore-27, India, Email Id: vsrikanth743@gmail.com*
*4Assistant Professor, College of Computing Science and Information Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India, Email id: mvgsrm@indiatimes.com*

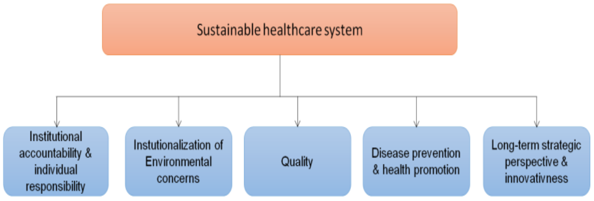
Sustainable healthcare system
Institutional accountability & individual responsibility
Instutionalization of Environmental concerns
Quality
Disease prevention & health promotion
Long-term strategic perspective & innovativness

**Fig.1** Health care system

## 2. Related Works

The study [6] examined and classifies the benefits of drawbacks of using use of blockchain technology the healthcare system. Blockchain, healthcare, benefits, and dangers were combined to search databases like PubMed, CINAHL, IEEE, Springer, and ScienceDirect. We checked the back-reference lists to find other pertinent references. The PRISMA framework was used in the study to diligently search for and analyze the various models that were suggested, prototyped, and/or put into practice. All 143 papers from this study's bibliometric and functional distribution were shown. The 61 papers that covered prototypes, pilot projects, or implementations were analyzed for the study [7]. The study [8] research into blockchain applications in the healthcare sector. It begins by talking about how medical data is managed, as well as how medical records are shared, how images are shared, and how logs are managed. The study [9] examined the fundamental utility utilization utilizing of blockchain technology in the medical profession by perspective of healthcare customers. We created 16 examples of information exchange regulated Web-based experiments in order to identify possible block chain technology applications in healthcare practices. In total, 16 web-based tests were conducted with 2013 respondents. The reaserch [10] evaluated, and synthesize peer-reviewed publications that used or proposed using blockchain to enhance services and processes in healthcare, health sciences, and health education. The study [11] 2018 discovered a few IoT use cases highlighting that BCMs are just one element of the IoT Security (IoTSec) system, where BCMs are essential parts. The study [12] mentioned secure data exchange method based on blockchain is suggested for vehicular networks (VNs). In addition to regular nodes, edge service providers are introduced to efficiently handle service provisioning. Thus they may communicate easily with one another, the edge service providers are positioned close to the regular nodes. Interplanetary File System (IPFS) is a networked file storage platform utilized to house the enormous volume of data generated by smart automobiles. The research [13] offered a thorough a description of block chain for big data with a focus on present practices, potential applications, and future objectives. First, we give a succinct introduction of big data, blockchain technology, and the justification for integrating them. The study [14] defined keywords "block chain," "healthcare," and "electronic health records" including variants to conduct a systematic search of all pertinent articles of study applications of blockchain technology medical assistance in three easily available databases, including ScienceDirect and IEEE, and Web of Science. The study [15] examined the most recent developments in the systems that use block chain technology to ensure information security; this study conducts a thorough literature review. Universal blockchain-based security architecture has been proposed after the fundamental needs of smart agriculture have been determined. The examined projects have undergone a thorough cost study. The study [16] proposed a system called HaBiTs where interoperability is made possible via Smart Contracts (SCs) and security is attained by immutability [17]. SC is a created portion of code in Sturdiness or another language designed specifically for block chains to build the blockchain fosters confidence between all parties involved and do away with the requirement for a middleman to facilitate data sharing [18].

## 3. Methodology

Blockchain technology has the potential to transform the healthcare sector by enhancing data security, interoperability, and patient privacy.

### 3.1 Local Area Network

The Body Area Sensor Network (BASN) is inserted into the patient's body to track their health in the smart environment. The external medical and non-medical devices are then connected to the IP cameras, smart phones, and BASN sensors. The Patient Data Provider (PDP) notifies the service provider (SP) of any alterations the person's body in the event that they take place.

### 3.2 Internal Edge (IE)

The primary function of the IE is to identify approaching medical and non-medical data based on the data type, supported applications, and patient state.

### 3.3 Local Healthcare Service Provider (LHSP)

The LHSP network is installed at the medical center keep track of and offer medical care to neighboring patients. It also keeps track of patients' conditions, dispatches an ambulance quickly in an emergency, and monitors people who have links to body sensors.

### 3.4 Block Chain Network

The primary application of utilizing the block chain network safely store and distribute healthcare data. It is made up of various components for securely gathering and distributing data. Block chain networks are frequently used employed in sectors including the Ministry of Public

Health (MOPH), Insurance firms, Pharmacies, Storing practices, Security evaluation, and Block-level validation.

### 3.5 Insurance Companies

The ability of insurers to pay hospital bills and additional costs for patients' treatment is computerized in the healthcare system. The cost is decreased while the quality of the services is improved through this method.

### 3.6 Pharmacies

The exchange and storage of patient prescriptions is a crucial function of pharmacies. Then, the pharmacies have a connection with the prescribers to confirm the medicine's dosage. In this approach, the block chain's healthcare data is secured.

### 3.7 Ministry of Public Health (MOPH)

The MOPH collaborates with many health groups to keep an eye on effectiveness and quality of healthcare services. When delivering health information to their companions, particularly health insurance companies, it offers high-quality services.

### 3.8 Storing Procedures

The system receives a large amount of data, and it constantly checks the patient information to determine whether it matters or it doesn't. As a result, the critical data is saved in a block with good encryption and high security, while the trivial information is placed in a with weakened security. The monitoring management (MM), which stores the data and gathers sensor information from healthcare businesses with the aid of service providers (SP), is part of the block chain. The SP is made up of Keys that are utilized to produce discretion and safety features like Signature Device Instructions (SDI).

### 3.9 Key Generation Phase

In this, the monitoring management (MM) and service providers (SP) are used to produce the keys. The x and y parameter functions are then used to indicate the key generation phase. The steps for creating SP and MM keys are described here.

### 3.10 Step 1. Initialization

The incoming information is set up in this process' block chain phase so that keys can be generated based on the MM and saved in hash tables. The block chain uses hash tables to reset the passwords on a regular basis, preventing hackers from accessing personal information or medical records.

### 3.11 Step 2. Generating Random Number

In this the $TO_v$generates random digits with a length exceeding 256 bits, and stores incoming data as array tables. The number at random is then inticated by $LO_{TO_v}$

### 3.12 Step 3. Verifying the result

Here, a secret pass code $LO_{TO_v}$ if the conditions are met, The outcome is satisfactory or the process returns to step 1. With the assistance of $LO_{TO_v}$ the following equation describes the process of generating a public key:

$$AL_{TO_v} = LO_{TO_v} \times E \qquad (1)$$

Where $AL_{TO_v}$represents the public key that was derived from the $TO_v$, $E$ symbolizes the constant point known as generator point in the Spec256k1 standard. $LO_{TO_v}$Based on which algorithm is the secret key generated$TO_v$. The $TO_v$ consists of the keys formatted as$AL_{TO_v}$,$LO_{TO_v}$. From this $LO_{TO_v}$ identifies the public key utilized to validate signature used to identify nodes. These credentials are never revealed during data storage or transmission, and they must be backed up and protected using encryption$TO_v$. The randomly generated key appears below,

$$\mu_n \leftarrow \{0,1\} * \qquad (2)$$

Where $\mu_n$ demonstrates the total number of instances credentials in use, using the predetermined authentication. The authentication outcome is displayed below,

$$\mu_0 = Bina\left(JC_{TO_v}\right) \qquad (3)$$

Eq. (3represents the generation of keys in the block chain through the use of hash tables; Medical information is recorded in hash structures; data is stored protected from cyber assault. Consequently, credentials are created. Send the updated iteration of keys periodically to the block chain module using this$JC$.

### 3.13 Registration Phase

During the registration phase, new accounts are created data associated with the private key that is used to determine its significance, and it is then stored in a specific block. This segment is then managed by the procedure of the$NN$. The recently enrolled $JC$ the following equation holds.

$$MQ = \left\{\mu_0, \mu_{1,}s, q_0, JC_{TCJ}\right\} \qquad (4)$$

Where $\mu_0$is used to monitor the transaction of$NN_{vz}$, $q_0$ demonstrate the time, information entering the sections,$JC_{TCJ}$ represents the new $CJ$ recorded within the block chain.

### 3.14 Signing and Verification Process

The primary objectives of the $NN_{vz}$ are that collected data is regularly and securely transmitted in regard to block chain blocks. In this $TO_v$ computes the message digest for the group $k = \ e$ and then generates the new data presented below.

$$q = e(k, \mu_v) \qquad (5)$$

Eq. (5) represents both the inbound and outgoing messages in the $NN_{vz}$ is given as,

$$NN_{vz} = \{s, q_0, JC_{TCJ}\} \tag{6}$$

The central administration then examines the medical records and the patients' circumstances; if there have been alterations in the individual's physique, an alarm is activated or a message is sent.. While receiving the data, $NN_{vz}$produces the signature and equation for the assembling message are as follows:

$$sign_m = \{JC_{NN_{vz}}, Q_i, \mu_v, X_v\} \tag{7}$$

Eq. (8) explains how hash tables in a number of segments of the block chain are used to authenticate incoming messages. Signature message and origin message. Given below is the transaction equation:

$$Tran_{mes} = \left\{FN(m)_{LOTO_v}, sign_{m,}X_v\right\} \tag{8}$$

Where $Tran_{mes}$ indicates the message transaction, $FN(m)_{LOTO_v}$ stands for the encrypted message, $X_v$ embodies the fundamental principle. The governing body will confirm whether or not every piece of data in the block is encrypted. Every node in the blocks will validate the integrity of every block. If any node is tampered with, the block chain verifies and protects the message that should not be hijacked by hackers, as well as verifies the execution time.

### 3.15 Elephant Herding Integrated Salp Swarm Optimization (EHISSO)

**Elephant Herding Integrated Optimization (EHO)**

The social interaction and behavior of elephant populations served as inspiration for the development of language. The Elephant Herding Optimization (EHO) algorithm for solving global optimization problems. EHO has numerous applications in a variety of domains, including the localization of nodes in WSNs, for which typical benchmark problems exist. Problems with static drone placement, image thresholds with multiple levels, etc. The objective of the heuristic search is to identify the social coexistence of elephants in herds led by a matriarch, from which adult male progeny separate to live independently while maintaining communication with the rest of the herd.

Due to the autonomy and structural communication among elephants within and outside the same clan, there are two families distinct environments: one in which elephants are social and function under the influence of a matriarch, and another in which male calves depart the herd. These environments are distinguished by their administrators for updating and separating.

The populace is separated into $v$ clans. The updating operator has been determined by reordering each solution $i$ in the clan $dj$ due to the influence of the matriarch $dj$ wwhich has the highest fitness value in generation, as shown in Equation 9.

$$v_{new,dj,i} = v_{dj,i} + \alpha \times \left(v_{best,dj} - v_{dj,i}\right) \times q, \tag{9}$$

Where$\beta$ ∈[0,1identifies the factor that influences the $v_{center,dj,}$ on the current individual.

As D represents the complete size of the search space, calculation of the clan's geographic centroid appears below , xcenter,ci,d for $d$ −th dimension problem:

$$v_{new,dj,i} = \beta \times v_{center,dj,} \tag{10}$$

Where $\beta \in [0,1]$ identifies the variables that influence the v_(center,dj) on the updated individual. As D represents the total dimension of the search space, the calculation for the clan center is as follows ci , $v_{center,dj,}$ for $d$−th dimension problem

$$:v_{center,dj,c} = \frac{1}{m_d^j} \times \sum_{i=1}^{c} v_{dj,i,c,} \tag{11}$$

Where $1v_{center,dj,c}$ , $dj, i, c$ is the number of elephants in clan , and $dj, i, c$ is the d-th of the elephant individual $dj, i, c$ . The separating operator may be represented by:

$$v_{worst,cj} = v_{min} + (v_{max} - v_{min} + 1) \times rand \tag{12}$$

:Where $v_{max}$and individual position's upper and lower limits, respectively. $v_{worst,cj}$ Is the worst member of the clan , and rand∈[0,1] is a number generated by homogeneous distribution.

### 3.16 Salp Swarm Optimization

Salp Swarm Optimization (SSO) is a metaheuristic optimization algorithm inspired by the behavior of salps, a type of marine organism. The first salp in the chain is the leader. It regulates the population's movement direction. Following one another, the remaining operatives move closer and closer to the leader. In the algorithm's semantics, they are referred to as follower agents. This distinct behavior strengthens the algorithm's ability to exploit local ranges. SSO Optimization has the disadvantage of settling on a local optimal solution when the population leader cannot relocate to a more advantageous region. In this paper, we propose two strategies to increase the effectiveness of the original SSO.

During the leader stage, the leader is vital to the entire population. The leader controls the trajectory of the search, which is always moving closer to the food source. The position update formula is shown in Eq. (13).

$$v_c^1 = \begin{cases} E_c + d_1\big((wa_c - ka_c)d_2 \geq 0.\big)d_3 \geq 0.5 \\ E_c + d_1\big((wa_c - ka_c)d_2 \geq 0.\big)d_3 < 0.5 \end{cases} \tag{13}$$

Where $v_c^1$ and $E_c$ indicate the leader's position and sustenance source in the $d_2$dimensional space, respectively. $wa_c$ And $ka_c$ show the upper bound and the lower bound of the d-th dimension, respectively. The governing variables $d_2$ and $d_3$ are interval contains arbitrary numbers. The coefficient $d_1$ it serves an essential role in coordinating exploration and exploitation and is defined as follows:

$$D_1 = 2f^{-(eEFt/maxEFt)^2} \tag{14}$$

Where $EFt$ the current number of assessments, and $maxEFt$ is the utmost amount of ratings. The remaining salps are the successors, which progressively ascend to the position of leader during the iteration process; the position of the follower is revised by Eq. (15).

$$v_c^m = (v_c^m + v_c^{m-1})/2 \tag{15}$$

Among them, $\mathrm{v}_c^m$ indicates the longitude of m adherent agent in c dimension space and n ≥2.

## 4. Result

We suggested a Deterministic Variational Deep Bayesian Neural Network in this paper. Storage cost, computational time, throughput, and efficiency are the usual evaluation criteria. Additionally, we contrasted our recommended approach DVDBNN with other popular techniques like KNN, LSTM, and VGG.

### 4.1 Storage cost

Storage expenses varies according to several factors, including the type storage medium used, the amount of space needed, and the facility or service provider you select. The classic mechanical storage units known as HDDs are frequently seen in servers and desktop computers. Dollars per terabyte (TB) are used to calculate HDD storage costs. In Figure 2 and Table 1, the storage cost of the proposed technique is compared to that of the traditional methods. Figure 2 shows that the proposed method's storage cost is lower when compared to conventional methods.

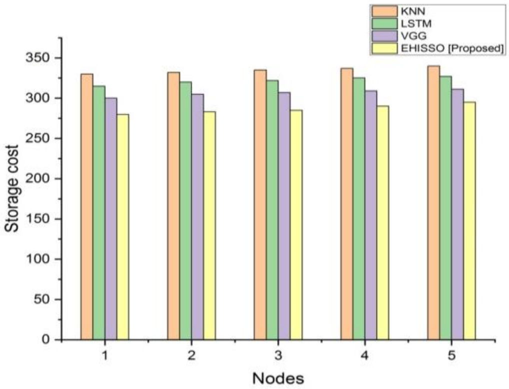

**Fig: 2** Performance of storage cost

**Table:1** Computation analysis of storage cost

| Nodes | KNN | LSTM | VGG | EHISSO [Proposed] |
|---|---|---|---|---|
| 1 | 330 | 315 | 300 | 280 |
| 2 | 332 | 320 | 305 | 283 |
| 3 | 335 | 322 | 307 | 285 |
| 4 | 337 | 325 | 309 | 290 |
| 5 | 340 | 327 | 311 | 295 |

### 4.2Computational time

Computational time, commonly referred to as execution time or runtime, is the length of time required for a computer program or algorithm to finish running. Depending on how the program is executed, it is frequently expressed in terms of seconds, milliseconds, or microseconds. In Figure 3 and Table 2, the computational time of the proposed technique is compared to that of the traditional methods. Figure 3 shows that the proposed method's computational time is lower when compared to conventional methods.

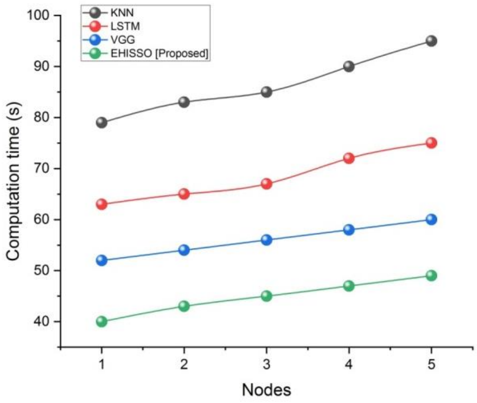

**Fig: 3** Performance of computation time

**Table:2** Computation analysis of computation time

| Nodes | KNN | LSTM | VGG | EHISSO [Proposed] |
|---|---|---|---|---|
| 1 | 79 | 63 | 52 | 40 |
| 2 | 83 | 65 | 54 | 43 |
| 3 | 85 | 67 | 56 | 45 |
| 4 | 90 | 72 | 58 | 47 |
| 5 | 95 | 75 | 60 | 49 |

### 4.3 Throughput

The throughput of a system or process is the speed at which data, information, or other materials may be processed or transferred. The effectiveness and capacity of a system are frequently measured in a variety of scenarios, including computer networks, telecommunications, manufacturing, and transportation. In Figure 4 and Table 3, the recommended method's throughput technique comparable to that of the traditional methods. Figure 4 shows that the proposed method’s throughput is higher when compared to conventional methods.

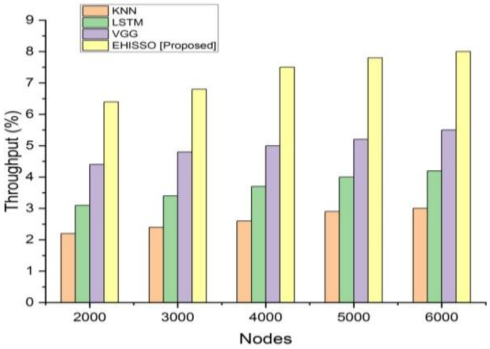

**Fig: 4** Performance of Throughput

**Table: 3** Computation analysis of Throughput

| Nodes | KNN | LSTM | VGG | EHISSO [Proposed] |
|---|---|---|---|---|
| 2000 | 2.2 | 3.1 | 4.4 | 6.4 |
| 3000 | 2.4 | 3.4 | 4.8 | 6.8 |
| 4000 | 2.6 | 3.7 | 5 | 7.5 |
| 5000 | 2.9 | 4 | 5.2 | 7.8 |
| 6000 | 3 | 4.2 | 5.5 | 8 |

### 4.4 Efficiency

Efficiency is the capacity to complete activities or produce desired results with the least amount of resource waste, including time, energy, or materials. It frequently relates to increasing productivity and streamlining procedures. In Figure 5 and Table 4, the efficiency of the proposed technique is compared to that of the traditional methods. Figure 4 shows that the proposed method’s efficiency is higher when compared to conventional methods.

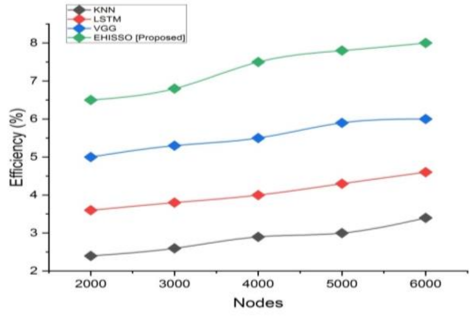

**Figure: 5** Performance of Efficiency

**Table: 4** Computation analysis of Efficiency

| Nodes | KNN | LSTM | VGG | EHISSO [Proposed] |
|---|---|---|---|---|
| 2000 | 2.6 | 3.8 | 5.3 | 6.8 |
| 3000 | 2.9 | 4 | 5.5 | 7.5 |
| 4000 | 3 | 4.3 | 5.9 | 7.8 |
| 5000 | 3.4 | 4.6 | 6 | 8 |
| 6000 | 2.6 | 3.8 | 5.3 | 6.8 |

## 5. Conclusion

Block chain is a developing technology with potential for use in the healthcare industry. It offers quite a few useful distributing and storing properties, consisting of decentralization, immutability, transparency, and traceability. Issues with interoperability, absence of technical expertise and security concerns, and using block chain technology in the healthcare sector carries concerns, including issues with authorization. Since there is a lack of research directing healthcare organizations to implement public, private, and hybrid block chain design types, it is crucial to provide information pertaining to distinctions between each block chain design in future work.

## References

[1] Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S.A. and Faxvaag, A., 2020. Blockchain in healthcare and health sciences—A scoping review. International Journal of Medical Informatics, 134, p.104040.

[2] Shen, B., Guo, J. and Yang, Y., 2019. MedChain: Efficient healthcare data sharing via blockchain. Applied sciences, 9(6), p.1207.

[3] Li, H., Zhu, L., Shen, M., Gao, F., Tao, X. and Liu, S., 2018. Blockchain-based data preservation system for medical data. Journal of medical systems, 42, pp.1-13.

[4] Wang, X., Zha, X., Ni, W., Liu, R.P., Guo, Y.J., Niu, X. and Zheng, K., 2019. Survey on blockchain for Internet of Things. Computer Communications, 136, pp.10-29.

[5] Puthal, D., Malik, N., Mohanty, S.P., Kougianos, E. and Yang, C., 2018. The blockchain as a decentralized security framework [future directions]. IEEE Consumer Electronics Magazine, 7(2), pp.18-21.

[6] Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M. and He, J., 2018, June. Blochie: a blockchain-based platform for healthcare information exchange. In 2018 ieee international conference on smart computing

(smartcomp) (pp. 49-56). IEEE.

[7] Rajan, S. ., & Joseph, L. . (2023). An Adaptable Optimal Network Topology Model for Efficient Data Centre Design in Storage Area Networks. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 43–50. https://doi.org/10.17762/ijritcc.v11i2s.6027

[8] Abu-Elezz, I., Hassan, A., Nazeemudeen, A., Househ, M. and Abd-Alrazaq, A., 2020. The benefits and threats of blockchain technology in healthcare: A scoping review. International Journal of Medical Informatics, 142, p.104246.

[9] Chukwu, E. and Garg, L., 2020. A systematic review of blockchain in healthcare: frameworks, prototypes, and implementations. Ieee Access, 8, pp.21196-21214.

[10] De Aguiar, E.J., Faiçal, B.S., Krishnamachari, B. and Ueyama, J., 2020. A survey of blockchain-based strategies for healthcare. ACM Computing Surveys (CSUR), 53(2), pp.1-27.

[11] Esmaeilzadeh, P. and Mirzaei, T., 2019. The potential of blockchain technology for health information exchange: experimental study from patients' perspectives. Journal of medical Internet research, 21(6), p.e14184.

[12] Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S.A. and Faxvaag, A., 2020. Blockchain in healthcare and health sciences—a scoping review. International Journal of Medical Informatics, 134, p.104040.

[13] Minoli, D. and Occhiogrosso, B., 2018. Blockchain mechanisms for IoT security. Internet of Things, 1, pp.1-13.

[14] Javed, M.U., Rehman, M., Javaid, N., Aldegheishem, A., Alrajeh, N. and Tahir, M., 2020. Blockchain-based secure data storage for distributed vehicular networks. Applied Sciences, 10(6), p.2011.

[15] Deepa, N., Pham, Q.V., Nguyen, D.C., Bhattacharya, S., Prabadevi, B., Gadekallu, T.R., Maddikunta, P.K.R., Fang, F. and Pathirana, P.N., 2022. A survey on blockchain for big data: approaches, opportunities, and future directions. Future Generation Computer Systems.

[16] Hussien, H.M., Yasin, S.M., Udzir, S.N.I., Zaidan, A.A. and Zaidan, B.B., 2019. A systematic review for enabling of develops a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. Journal of medical systems, 43, pp.1-35.

[17] Deshpande, V. (2021). Layered Intrusion Detection System Model for The Attack Detection with The Multi-Class Ensemble Classifier . Machine Learning Applications in Engineering Education and Management, 1(2), 01–06. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/10

[18] Vangala, A., Das, A.K., Kumar, N. and Alazab, M., 2020. Smart secure sensing for IoT-based agriculture: Blockchain perspective. IEEE Sensors Journal, 21(16), pp.17591-17607.

[19] Gupta, R., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M.S. and Sadoun, B., 2019, August. Habits: Blockchain-based telesurgery framework for healthcare 4.0. In 2019 international conference on computer, information and telecommunication systems (CITS) (pp. 1-5). IEEE.

[20] Parvin, S., Nimmy, S.F., Venkatraman, S., Abed, S.E. and Gawanmeh, A., 2021. A KNN approach for blockchain based electronic health record analysis. In Proceedings of the 27th International Conference on Systems Engineering, ICSEng 2020 (pp. 455-464). Springer International Publishing.

[21] Li, Z., Guo, H., Barenji, A.V., Wang, W.M., Guan, Y. and Huang, G.Q., 2020. A sustainable production capability evaluation mechanism based on blockchain, LSTM, analytic hierarchy process for supply chain network. International Journal of Production Research, 58(24), pp.7399-7419.

[22] Ramanan, M., Singh, L., Kumar, A.S., Suresh, A., Sampathkumar, A., Jain, V. and Bacanin, N., 2022. Secure blockchain enabled Cyber-Physical health systems using ensemble convolution neural network classification. Computers and Electrical Engineering, 101, p.108058.

[23] Parvin, S., Nimmy, S.F., Venkatraman, S., Abed, S.E. and Gawanmeh, A., 2021. A KNN approach for blockchain based electronic health record analysis. In Proceedings of the 27th International Conference on Systems Engineering, ICSEng 2020 (pp. 455-464). Springer International Publishing.