Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.021822
Article

Blockchain for Securing Healthcare Data Using Squirrel Search Optimization Algorithm

B. Jaishankar[1,*], Santosh Vishwakarma[2], Prakash Mohan[3], Aditya Kumar Singh Pundir[4], Ibrahim Patel[5] and N. Arulkumar[6]

[1]Department of Electronics and Communication Engineering, KPR Institute of Engineering and Technology, Coimbatore, 641407, India
[2]Department of Computer Science and Engineering, National Institute of Technology, Arunachal Pradesh, 791112, India
[3]Data Science and Analytics Centre, Karpagam College of Engineering, Coimbatore, 641032, India
[4]Department of Electronics and Communication Engineering, Arya College of Engineering and Information Technology, Kukas, 302028, India
[5]Department of Electronics and Communication Engineering, B V Raju Institute of Technology, Narsapur, 502313, India
[6]Department of Computer Science, CHRIST (Deemed to be University), Bangalore, 560029, India
*Corresponding Author: B. Jaishankar. Email: b.jaishankar@kpriet.ac.in
Received: 15 July 2021; Accepted: 19 October 2021

Abstract: The Healthcare system is an organization that consists of important requirements corresponding to security and privacy, for example, protecting patients' medical information from unauthorized access, communication with transport like ambulance and smart e-health monitoring. Due to lack of expert design of security protocols, the healthcare system is facing many security threats such as authenticity, data sharing, the conveying of medical data. In such situation, block chain protocol is used. In this manuscript, Efficient Block chain Network for securing Healthcare data using Multi-Objective Squirrel Search Optimization Algorithm (MOSSA) is proposed to generate smart and secure Healthcare system. In this the block chain is a decentralized and the distributed ledger device that consists of various blocks linked with digital signature schemes, consensus mechanisms and chain of hashing, offers highly reliable storage capabilities. Further the block chain parameters, such as block size, transaction size and number of block chain channels are optimized with the help of MOSSA. With the evolution of the MOSSA provide new features for enhancing security and scalability. The simulation process is executed in the JAVA platform. The experimental result of the proposed method shows higher throughput of 26.87%, higher efficiency of 34.67%, lowest delay of 22.97%, lesser computational overhead of 37.03%, higher storage cost of 34.29% when compared to the existing method such as Block chain-ECIES-HSO, Block chain-hybrid GO-FFO, Block chain-SDN-HSO algorithm for healthcare technologies.

Keywords: Multi-objective squirrel search optimization algorithm; Blockchain; healthcare; key generation; security

1 Introduction

The Healthcare system consists of various organizations that has health related data of large number of patients that are stored in a system that are secured by various protocols [1,2]. Now a days securing health related data becomes a great challenge because, various hackers are involving into the system and the nodes in the systems are damaged due to the natural calamities [3,4]. The healthcare data is very sensitive and it needs various protocols to store and secure the data in protected manner [5,6]. Sharing medical data is one of the crucial prominent services as it deals with the life of the patient [7]. When the data is shared and if there is any delay, it means the patient's condition is critical [8]. The Block chain-based health care technology is used to store and secure the medical data [9]. In this block chain plays a decentralized and distributed technology for providing the healthcare data of patient to central authority and to doctors [10]. Its main role is to collect the data from various sources that includes patient details, doctor's availability, ambulance services [11]. Then the messages are entered into the block chain. When too many messages enter into the system, the transferring of data is delayed and hence the central authority checks the type of the message whether it is important or unimportant and then sends to the doctor [12,13]. There are various devices used for storing and sharing, the medical details that causes delay and potential leakage of the information. The previously used devices are Internet of things (IoT), sensing technologies and 5G [14,15]. The leakage of medical information while storing, sharing and in maintaining the personal details are the problems in previous works [16]. The leakage of the medical data occurs, when many internet systems are linked with the health care organizations, that the patients get confused in which system they are transferring the message. The previous system uses centralized devices and the third-party systems where the messages are not secure and the leakage occurs [17]. The block chain does not take the third-party invitation (TP) and it is a decentralized device that works very fast in storing and sharing the data [18].

In this manuscript, Efficient Block chain [19] Network for securing Healthcare data using Multi-Objective Squirrel Search Algorithm (MOSSA) [20] optimization is proposed. The block chain is a decentralized and the distributed ledger device that consists of various blocks linked with digital signature schemes, consensus mechanisms and chain of hashing, offers highly reliable storage capabilities. The novelty of this paper is to reduce the computational overhead, key generation time and encryption time and the security is verified with Integrity and Authentication.

2 Literature Survey

In 2021, Velmurugadass et al. [21] have presented a Blockchain based security in cloud computing through IoT location using Elliptic Curve Integrated Encryption Scheme (ECIES) algorithm and cryptography hash algorithm. In this the keys are generated by using the Harmony Search Optimization (HSO). Then the incoming packets are encrypted using the ECIES process. Then the Software Defined Network (SDN) controller is used to manage the block chain data and it is stored in the Hash algorithm using the cryptographic SHA-256. Then the experimental results are determined with response time, accuracy, throughput and total change security parameters. This method has the limitation such as incoming data increases the computational overhead that delays and decreases the performance.

In 2021 Jamil et al. [22] have presented a novel block chain-based integrity and reliable veterinary clinic information management system using predictive analytics for provisioning quality health services. In this a novel blockchain-based Reliable and Intelligent Veterinary Information Management System (RIVIMS) with smart convention and ML techniques is used.

In 2019 Pourvahab et al. [23] have presented a new digital forensic structural design using fast-growing Software-Defined Networking (SDN) and Blockchain technology [24] for Infrastructure-as-a-Service (IaaS) cloud.

3 Proposed Blockchain Network for Securing Healthcare Data Using MOSSA Optimization

Fig. 1 shows the Block diagram for Block chain Network for securing Healthcare data using MOSSA optimization. The Healthcare system consists of two main parts such as (a). Local Area Network (LAN), (b). Block chain. The parameter description of the block diagram.

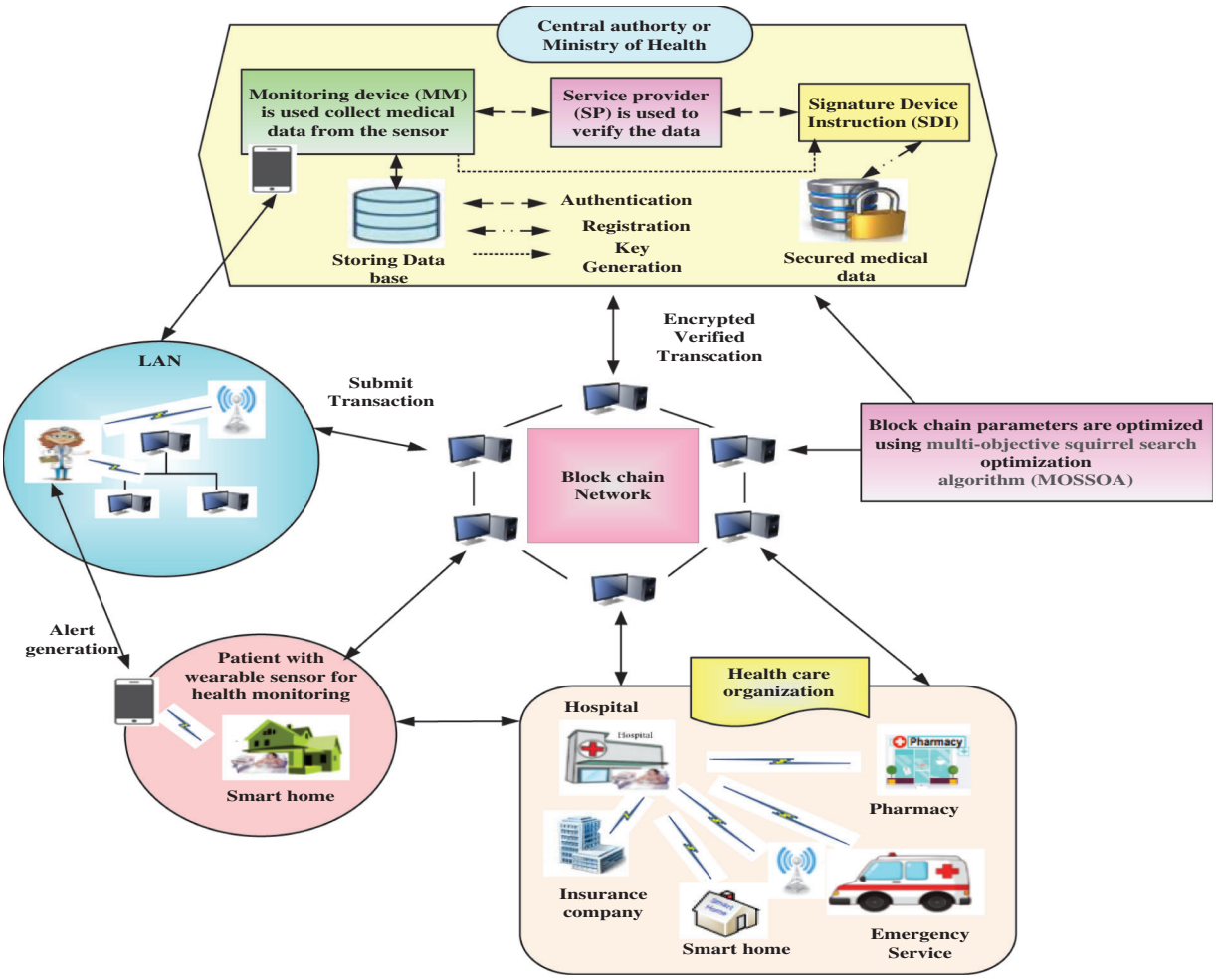

Figure 1: Block diagram for blockchain network for securing healthcare

3.1 Local Area Network

The main purpose of the LAN is to collect and share the medical data to the block chain network. Then the shared data is stored in the block chain and the validities are trusted in the large storage and to avoid the computational complexity for minimizing the scalability.

3.1.1 Internet of Medical Things (IoMT)

The Body Area Sensor Network (BASN) is placed in the patients' body to monitor the health condition of the patients in the smart environment. Then the BASN sensors are linked to the smart phones, IP cameras and the external medical and nonmedical devices. If any changes occur in patient's body, the Patient Data Provider (PDP) raises an alarm to the service provider (SP).

3.1.2 Internal Edge (IE)

The main purpose of the IE is to detect the incoming medical or nonmedical data that is delivered on the basis of the data type, supported application and the condition of the patient.

3.1.3 Local Healthcare Service Provider (LHSP)

The LHSP system is placed in the hospital to monitor and to provide the healthcare services for the local patients, records the patient's condition and to provide the fast emergency services (Ambulance) and to monitor the patients those who are connected with the body sensors.

3.2 Block Chain Network

The block chain network is mainly used to store and share the healthcare data in a secured manner. It consists of several units for collecting and sharing the data in a secured manner. The block chain network is widely used in areas such as Insurance companies, Pharmacies, Ministry of Public Health (MOPH), Storing procedures, Security Analysis, Block verification. These are explained as follows

3.2.1 Insurance Companies

In the health care system, the availability of the insurance companies is digitized for paying the hospital bills and the extra charges for the treatment of the patients. This process enhances the quality of the services and reduces the cost.

3.2.2 Pharmacies

The pharmacies play an important role in sharing and storing the prescriptions of patients. Then the pharmacies have the link with the prescribers for confirming the dosage of the tablet. In this way it secures the healthcare information in the block chain.

3.2.3 Ministry of Public Health (MOPH)

The MOPH is used to monitor the quality and the efficiency of the healthcare services by coordinating with the various health organizations. It provides the high quality of services for transferring medical data to their partners namely health insurance Company.

3.2.4 Storing Procedures

The large amount of the data is entered into the system by continuously monitoring the patients' details to find if the data is important or not, so the unimportant data is stored in one block with less security and the important data is stored in another block in the block chain with high security with great encryption using hash tables. The block chain consists of Monitoring Management (MM) for storing the data which collects the sensor data from the health care organizations with the help of Service Providers (SP). The SP consists of Keys that is used to generate privacy and security functions such as Signature Device Instruction (SDI).

3.2.5 Key Generation Phase

In this the keys are generated on the basis of the monitoring management (MM), and service providers (SP). Then the key generation phase is denoted by the functions of the x, y parameters. The SP and MM key generation procedures are explained below.

Step 1. Initialization

In this the incoming data is initialized in the block chain phase for generating the keys on the basis of the MM and stored in the hash tables. By using hash tables, the block chain changes the passwords periodically, so the hackers will not hack the details or the medical data.

Step 2. Generating Random Number

In this the SP_x generates the random numbers which is larger than 256 bits and the incoming data is stored in bits in the form of hash tables. Then the random number is denoted by $K(RN)$, where RN represents the random number for storing the data, K represents the hash tables.

Step 3. Verifying the result

In this a private key KP_{SP_x} is generated by satisfying the conditions as $1 < 256 - bitnumber < m$, Where $m \approx 2^{256}$, in this way the result is satisfied or return to step 1. With the help of the KP_{SP_x} a public key is generated and the equation is given below,

$$BK_{SP_x} = KP_{SP_x} \times F \tag{1}$$

where BK_{SP_x} represents the public key generated on the basis of the SP_x, F represents the constant point in the Spec256k1 standard called generator point. KP_{SP_x} is the private key generated on the basis of the SP_x. The SP_x consists of the keys in the form of BK_{SP_x}, KP_{SP_x}. From this KP_{SP_x} is the public key which is used to verify the signature for identifying the nodes. These keys are always secret when the data storing and transferring takes place and it should be backed up and protected that is encrypted in the SDI. The random generated key is given below,

$$\mu_m \leftarrow \{0,1\}^* \tag{2}$$

where μ_m represents the number of one-time passwords, with the authentication preset. The authentication result is given below,

$$\mu_0 = Bina(ID_{SP_x}) \tag{3}$$

Eq. (3) represents the key generation in the block chain by using the hash tables and the medical data is stored in the hash tables and the data is secured from the cyber attacks. In this way the keys are generated. In this SP periodically send the updated key generation to the block chain module.

3.2.6 Registration Phase

The registration phase is used to register the newly entering data with the private key that is used to check whether it is important or not and it is stored in a particular block. Then this block is controlled by the process of the MM and the SP. The newly registered ID is given by the following equation.

$$NR = \{\mu_0, \mu_1, t, r_0, ID_{SDI}\} \tag{4}$$

where μ_0 is utilized to detect the transaction of MM_{xy}, r_0 represents the time, μ_0, μ_1 represents the new data entering into the blocks, ID_{SDI} represents the new ID registered in the block chain.

3.2.7 Signing and Verification Process

The main purposes of the MM_{xy} is that the gathered data is sent to the block chain blocks securely and periodically. In this SP_x calculates the hash of the gathering message $l = f(n)$ and then produces the new data that is formulated below.

$$r = f(l, \mu_x) \tag{5}$$

Eq. (5) represents the incoming message and the message generated in the MM_{xy} is given as,

$$MM_{xy} = \{t, r_0, ID_{SDI}\} \tag{6}$$

Then the central authority checks the medical data and the patients' conditions, if any changes occurred in the patient's body an alarm is raised or message is transferred. While receiving the data, MM_{xy} produces a signature for the gathering message and the signing equation is given as

$$sign_n = \left\{ ID_{MM_{xy}}, R_j, \mu_x V_x \right\} \tag{7}$$

Eq. (8) explains the signing of the incoming message by the process of hash tables in various blocks in the block chain. Then the encrypted message is given by $Em(n)_{KP_{SP_x}}$ and the message is transformed in the form of encrypted message, signing message and the root message. The transaction equation is given as

$$Tran_{mes} = \left\{ Em(n)_{KP_{SP_x}}, sign_n, V_x \right\} \tag{8}$$

where $Tran_{mes}$ represents the transaction message, $Em(n)_{KP_{SP_x}}$ represents the Encrypted message, V_x represents the root message. The central authority will verify every data in the block is in a secured manner or not. Every node in the blocks will confirm the integrity of every block. If any node is tampered, the block chain checks and protects the message that is not to be hacked by the hackers and also checks the execution time.

3.2.8 Security Analysis

Block chain systems controls or manages the patients' records and the data is stored in various nodes present in the blocks that are accessed with security and integrity.

3.2.9 Message Integrity and Authentication

The MM communicates with the blocks in the block chain and holds the keys. When the blocks receive the requests from the central authority, it verifies the signatures and the data are encrypted using the private key. In this the Message Integrity and Authentication is ensured by the MM keys and the randomness of the central authority (CA).

3.3 Optimized Block Chain Parameters for Storing and Securing Healthcare Medical Data Using MOSSOA

MOSSOA is the novel meta-heuristic algorithm which is used to solve the environmental issues and to reduce the latency and the computational cost in the systems. In this MOSSOA is used to optimize the block chain parameters in the storing and securing the medical healthcare data in the block chains and to increase the transaction speed by reducing delay and the computational cost.

3.4 Step by Step Procedure of Proposed DS-DSAE-EGDO Algorithm

In this the dynamic foraging and the seasonal adapting process will used in the exploration (storing medical data) and the exploitation phases (transferring medical data) as shown in Fig. 2. The step-by-step procedure for MOSSOA algorithm are given below

Step 1: Initialization

In this the population of the MOSSO algorithm is initialized as m number of the squirrels. In this the assumption is taken from the squirrels of the deciduous forest by assuming single squirrels in the tree.

Step 2. Random generation

In this the positions of the M individual squirrels are selected in random manner. The populations is arranged in the ascending order to minimize the storing and securing problem.

Step 3. Fitness Evaluation

In this the fitness is evaluated in three classifications such as squirrels positioned in hickory trees $\left(H_g\right)$, acorn tree $\left(H_\beta\right)$, normal trees (H_m). The squirrels with minimum fitness value is denoted by $\left(H_g\right)$, the

squirrels in the fitness rank is denoted by (H_β) and it ranges from 2 *to* $M_x + 1$, (H_m) represents the remaining part of the squirrel.

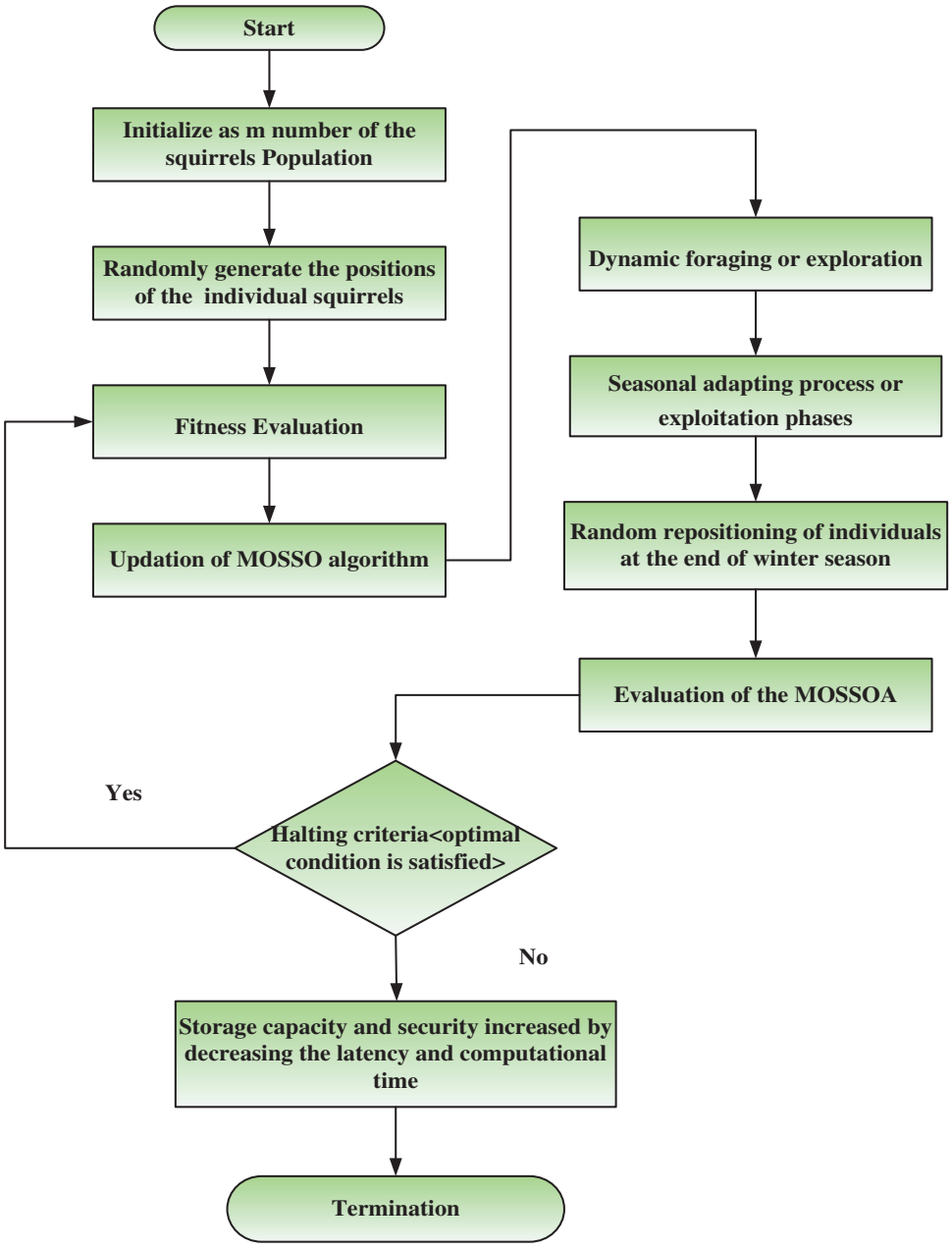

Figure 2: Flow chart for multi-objective squirrel search optimization algorithm (MOSSOA)

Step 4. Updation of MOSSO algorithm

The MOSSOA algorithm consists of three main phases such as 1. Dynamic foraging or exploration (storing medical data) 2. Seasonal adapting process or exploitation phases (transferring medical data) and 3. The Random repositioning of individuals at the end of winter season.

Step 5. Dynamic foraging or exploration

The dynamic foraging is also known as the exploration phase that is used to solve the problems in the block chain and the computational cost is reduced by increasing the storage capacity. In this the positions of the individual squirrels gliding from the acorn trees to the hickory trees are given below in Eq. (9), in this way the medical data are stored and then transferred to the central authority.

$$A_{zx}^{k+1} = \begin{cases} A_{zx}^{k} + f_h D_v \left(A_{zf}^{k} - A_{zx}^{k} \right) & if\ t_1 \geq L_{fl} \\ Random\ location, & otherwise \end{cases} \tag{9}$$

In this the positions of the individual squirrels are gliding from the normal trees to the acorn trees and hickory trees are given in below Eq. (10),

$$A_{x}^{k+1} = \begin{cases} A_{x}^{k} + f_h D_v \left(A_{zf}^{k} - A_{x}^{k} \right) & if\ t_2 \geq L_{fl} \\ Random\ location, & otherwise \end{cases} \tag{10}$$

$$A_{x}^{k+1} = \begin{cases} A_{x}^{k} + f_h D_v \left(A_{f}^{k} - A_{x}^{k} \right) & if\ t_3 \geq L_{fl} \\ Random\ location, & otherwise \end{cases} \tag{11}$$

where t_3, t_3 and t_3 represents the random number in the range of [0,1], L_{fl} represents the predator presence probability, A_f^k represents the location of individual squirrel entered into the hickory tree, k represents the current iterations, D_v represents the gliding constant and it is used to balance the exploration and exploitation phase, f_h represents the gliding distance and its equation is given as,

$$f_h = \frac{k_h}{\tan(\psi)} \tag{12}$$

where k_h is represented as the constant value 8, $\tan(\psi)$ represents as the gliding angle and it is formulated as

$$\tan(\psi) = \frac{F}{K} \tag{13}$$

where F and K is represents as the drag respectively and lift forces and it is given as;

$$F = \frac{1}{2\gamma N^2 Z V_F} \tag{14}$$

$$K = \frac{1}{2\gamma N^2 Z V_K} \tag{15}$$

where γ, N, Z represents the density of the air, speed and the surface area of the body respectively and V_F, V_K represents the drag and the lift coefficients respectively.

Step 6. Seasonal adapting process or exploitation phases

The squirrels are affected by the seasonal fluctuations in the foraging behavior and it is noted that the squirrels are active in the autumn season compared to the winter season. Then the Seasonal adapting process or exploitation phase equation is given by,

$$X_v^k = \sqrt{\sum_{l=1}^{f} \left(A_{xy,l}^k - A_{g,k}^k\right)^2} \quad y = 1, 2, \ldots, M_x \tag{16}$$

Then the minimal seasonal constant is given as

$$X_{\min} = \frac{10e^{-6}}{(365)^{k/(k_{\max}/2.5)}} \tag{17}$$

where k and $k_{\max}$ represents the current and the maximum iteration values respectively. Then the higher $X_{\min}$ value represents the exploration and the lower value enhances the exploitation phase.

Step 7. Random repositioning of individuals at the end of winter season

In this the computational cost is reduced. During winter the squirrels become less active compared to the autumn season. It is noted that if $X_v^k \leq X_{\min}$, it is in winter season. Then the flying locations of the squirrels are given by,

$$A_{xnew}^{k+1} = A_K + levy(a) \times (A_W - A_K) \tag{18}$$

where A_W and A_K represents the lower and the upper bounds of the squirrels respectively.

Step 8. Evaluation of the MOSSOA

Hera, a new population $A_{xnew}^{'}$ is generated with the estimation of the squirrel's individuals on the basis of the Dynamic foraging behavior, Seasonal adapting and intelligence, Random repositioning procedures. Then to solve the problem pareto-dominance and the Crowding distance (CD) measures are calculated. In this $A^{'}$ and $A_{xnew}^{'}$ is determined for optimizing the problem:

$$\begin{aligned} &A^{'} \; with \; A_{xnew}^{'} \left(a^k < a_{new}^k\right) \\ &A_{new}^{'} \; with \; A^{'} \left(a_{new}^k < a^k\right) \\ &A^{'} \; and \; A_{xnew}^{'} \; are \; not \; controls \;\; in \;\; the \; individual \; squirrels \end{aligned} \tag{19}$$

Then the pareto-dominance is given as

$$a^{k+1} = \begin{cases} a^k & if \; a^k < a_{new}^k \\ a_{new}^k & f \; a_{new}^k < a^k \\ CL(a^k, a_{new}^k) & otherwise \end{cases} \tag{20}$$

where $CL(a^k, a_{new}^k)$ is represents as the low crowded solution among the $A^{'} \; and \; A_{xnew}^{'}$.

Step 9. Termination

In this step, the optimal weight parameters of block chain are optimized with the help of MOSSOA. Finally, the objective is to increase the storage capacity of the block chain and to increase the security of the medical healthcare data and to reduce the computational cost and latency.

4 Results and Discussion

In this segment, Efficient Block chain Network for securing Healthcare data using Multi-Objective Squirrel Search Algorithm (MOSSA) optimization is performed on JAVA platform.

4.1 Evaluation Metrics

The various performance measures have been utilized to calculate the results for increasing the security and the privacy of the block chain. The storage cost, Average delay, Computational time, Throughput, Efficiency, Response time are calculated as follows

In this block chain healthcare technique, the storage is calculated on the basis of the data stored in the Monitoring devices (MM) and the service providers. Then the storage cost $Cost_{storage}(total)$ equation is given as

$$Cost_{storage}(total) = k_{KP_{SPx}} + k_{BK_{SPx}} + k_{time} + k_{transaction} \times N_{MM} \times \left(R_{cert}/R_{\text{int}era} \times 2.628 \times 10^6\right) \tag{21}$$

where BK_{SP_x} and KP_{SP_x} represents the public key and private key generated on the basis of SP_x. In this SP_x consists of the keys in the form of BK_{SP_x}, k_{time} represents the response time, $k_{transaction}$ represents the transaction time, N_{MM} represents the storage cost, R_{cert} represents the certifications of the key generation cycles in the SDI, $R_{\text{int}era}$ represents the MM interact with the SDN in every minute, k represents the data length. In this the MM is determined by calculating the length of the hash chain and the data is stored in 2.628×10^6 bit number with the help of hash tables.

4.2 Computational Time Cost

To find how much time is taken for the message to reach from patient to the Monitoring device and then to the doctor. From this the computational time is calculated as

$$cc_{time} = \psi + 2\varphi + \zeta + \eta \tag{22}$$

where cc_{time} represents the computational cost time, ψ is given as $O_{cc}(\log_2 k_{hash-chain})$, from this the operation takes *approximately* $1050\,Mb/s$, ζ represents the verification time, η represents the efficiency of the system and the efficiency is defined by the number of images divided into energy input image and energy output image by 100%.

$$efficiency\,\eta = \frac{Energy\ of\ input}{Energy\ output} \times 100\% \tag{23}$$

4.3 Simulation Phase 1: Performance Comparison of Various Methods

Figs. 3–8 shows the simulation result of an Efficient Block chain Network for securing Healthcare data using Multi-Objective Squirrel Search Algorithm (MOSSA) optimization. The various evaluation metrics like delay, throughput, efficiency, computational time, response time and storage cost are analyzed in this segment (Table 1).

Table 1: Simulation parameter

Parameter	Value
Simulation area	10000 m
No of nodes	2000, 3000, 4000, 5000, 6000, 7000, 8000, 9000
Size of block	1024 bytes
Population size	5000
Total number of time periods in a data collection round.	3000 s
Range of transmission	500 m
Number routing protocol (Block chain)	1
Key size	256 bits

Fig. 3 demonstrates the performance of the Storage cost for proposed Block chain-MOSSOA used in healthcare systems. In this, at node 1, the proposed method shows 24.56%, 26.49%, 32.54%, higher storage cost than the existing method such as Block chain-ECIES-HSO, Block chain-hybrid GO-FFO, Block chain-SDN-HSO algorithm for healthcare technologies respectively. With the succeeding nodes, the proposed method shows higher performance of storage cost than the existing methods as shown in the figure.

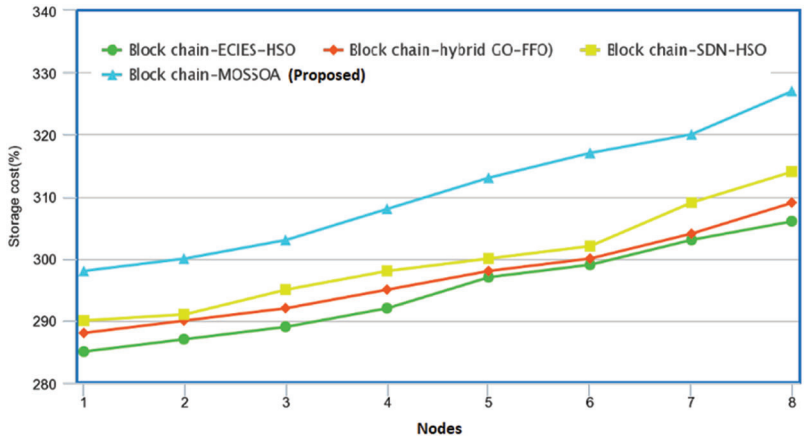

Figure 3: Performance of storage cost

Fig. 4 demonstrates the performance of the delay for proposed Block chain-MOSSOA used in healthcare systems. In this, at node 1, the proposed method shows 26.64%, 28.64%, 38.53%, lower delay than the existing method such as Block chain-ECIES-HSO, Block chain-hybrid GO-FFO, Block chain-SDN-HSO algorithm for healthcare technologies respectively. With the succeeding nodes, the proposed method shows lower performance of delay than the existing methods as shown in the figure.

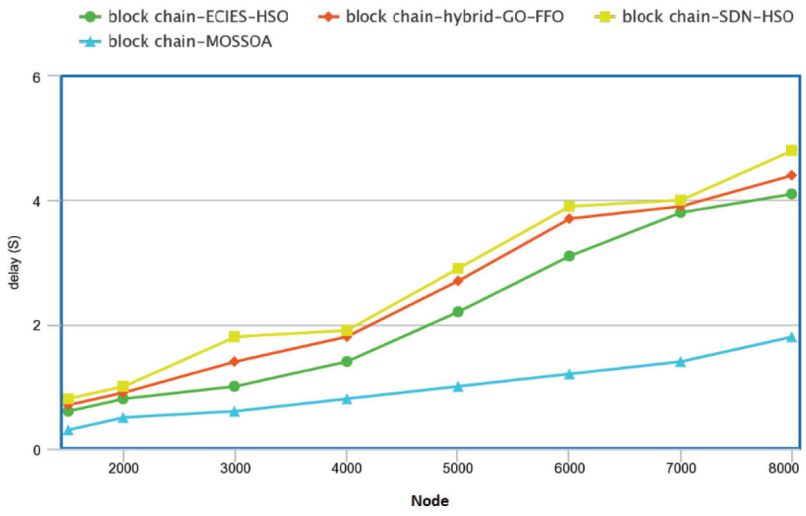

Figure 4: Performance of delay

Fig. 5 demonstrates the performance of the computational overhead for proposed Block chain-MOSSOA used in healthcare systems. In this, at node 1, the proposed method shows 23.74%, 16.75%,

42.63%, lower computational overhead than the existing method such as Block chain-ECIES-HSO, Block chain-hybrid GO-FFO, Block chain-SDN-HSO algorithm for healthcare technologies respectively. With the succeeding nodes, the proposed method shows lower performance of computational overhead than the existing methods as shown in the figure.

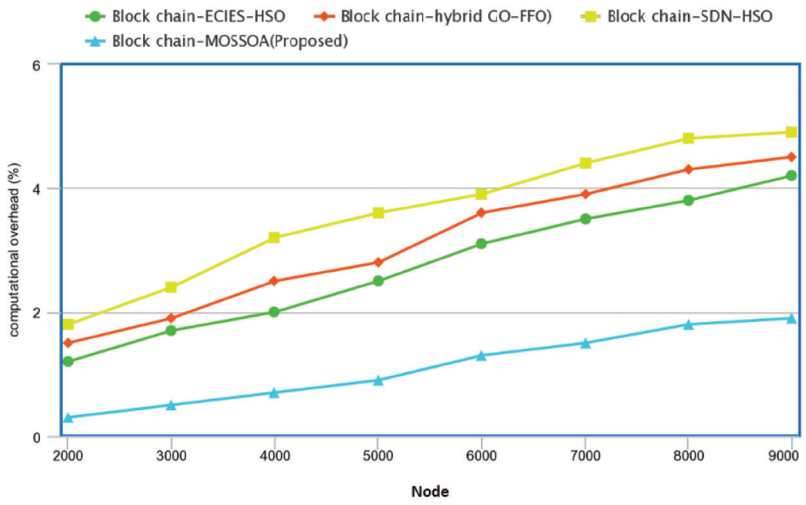

Figure 5: Performance of computational overhead

Fig. 6 demonstrates the performance of the computational time for proposed Block chain-MOSSOA used in healthcare systems. In this, at node 1, the proposed method shows 34.42%, 27.75%, 45.31%, lower computational time than the existing method such as Block chain-ECIES-HSO, Block chain-hybrid GO-FFO, Block chain-SDN-HSO algorithm for healthcare technologies respectively. With the succeeding nodes, the proposed method shows lower performance of computational time than the existing methods as shown in the figure.

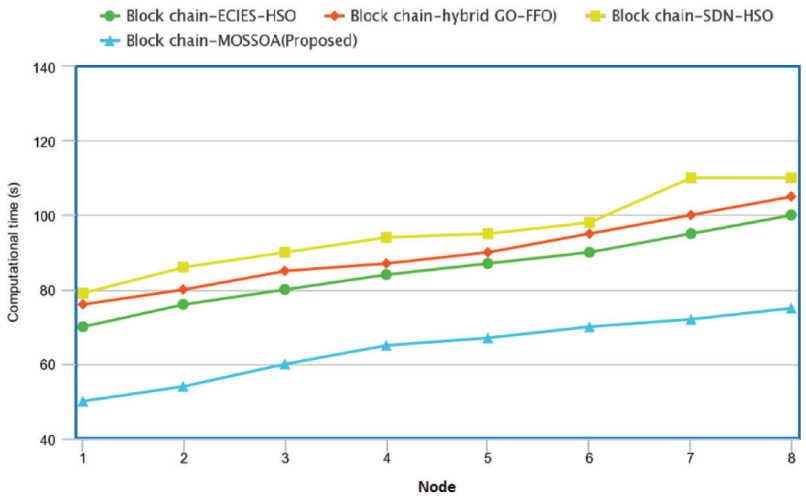

Figure 6: Performance of computational time

Fig. 7 demonstrates the performance of the throughput for proposed Block chain-MOSSOA used in healthcare systems. In this, at node 1, the proposed method shows 27.86%, 33.53%, 27.64%, higher

throughput than the existing method such as Block chain-ECIES-HSO, Block chain-hybrid GO-FFO, Block chain-SDN-HSO algorithm for healthcare technologies respectively. With the succeeding nodes, the proposed method shows higher performance of throughput than the existing methods as shown in the figure.

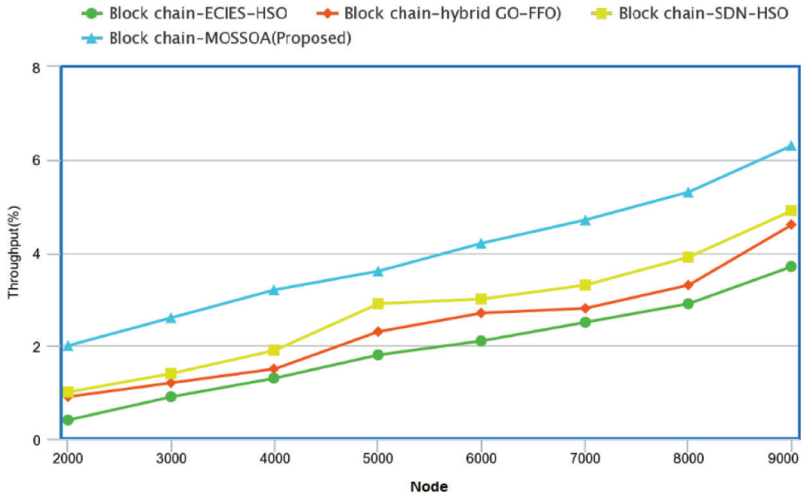

Figure 7: Performance of throughput

Fig. 8 demonstrates the performance of the Efficiency for proposed Block chain-MOSSOA used in healthcare systems. In this, at node 1, the proposed method shows 24.54%, 26.87%, 29.62%, higher efficiency than the existing method such as Block chain-ECIES-HSO, Block chain-hybrid GO-FFO, Block chain-SDN-HSO algorithm for healthcare technologies respectively. With the succeeding nodes, the proposed method shows higher performance of efficiency than the existing methods.

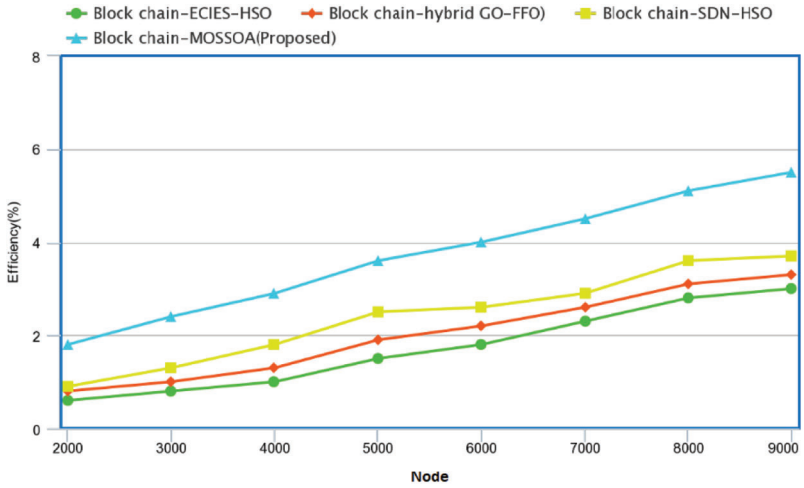

Figure 8: Performance of efficiency

5 Conclusion

In this manuscript, Efficient Block chain Network for securing Healthcare data using Multi-Objective Squirrel Search Optimization Algorithm (MOSSA) is proposed. The aim of this paper is to generate smart

and secure Healthcare system, leveraging advances in block chain technologies permits remote monitoring and fast emergency response. Further the block chain parameters, such as block size, transaction size and number of block chain channels are optimized with the help of MOSSA. With the evolution of the MOSSA provide new features for enhancing security and scalability. The effectiveness of the proposed system is evaluated by distinct measures. The experimental result of the proposed method shows better performance compared to the existing method such as Block chain-ECIES-HSO, Block chain-hybrid GO-FFO, Block chain-SDN-HSO algorithm for healthcare technologies.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] N. Reibling, M. Ariaans and C. Wendt, "Worlds of healthcare: A healthcare system typology of OECD countries," *Health Policy*, vol. 123, no. 7, pp. 611–620, 2019.

[2] M. Chen, W. Li, Y. Hao, Y. Qian and I. Humar, "Edge cognitive computing based smart healthcare system," *Future Generation Computer Systems*, vol. 86, no. 6116, pp. 403–411, 2018.

[3] S. Sambit, D. Sanchali and D. Swapan, "A new healthcare diagnosis system using an IoT-based fuzzy classifier with FPGA," *Journal of Supercomputing*, vol. 76, no. 8, pp. 5849–5861, 2020.

[4] P. Gope, Y. Gheraibia, S. Kabir and B. Sikdar, "A secure IoT-based modern healthcare system with fault-tolerant decision making process," *IEEE Journal of Biomedical and Health Informatics*, vol. 25, no. 3, pp. 862–873, 2020.

[5] U. Gowshika and T. Ravichandran, "A smart device integrated with an android for alerting a person's health condition: Internet of things," *Indian Journal of Science and Technology*, vol. 9, no. 6, pp. 1–12, 2016.

[6] M. Chen, W. Li, Y. Hao, Y. Qian and I. Humar, "Edge cognitive computing based smart healthcare system," *Future Generation Computer Systems*, vol. 86, no. 2, pp. 403–411, 2018.

[7] G. Yang, M. A. Jan, V. G. Menon, P. G. Shynu, M. M. Aimal *et al.,* "A centralized cluster-based hierarchical approach for green communication in a smart healthcare system," *IEEE Access*, vol. 8, pp. 101464–101475, 2020.

[8] A. H. Sodhro, S. Pirbhulal, G. H. Sodhro, A. Gurtov, M. Muzammal *et al.,* "A joint transmission power control and duty-cycle approach for smart healthcare system," *IEEE Sensors Journal*, vol. 19, no. 19, pp. 8479–8486, 2018.

[9] S. Tuli, N. Basumatary, S. S. Gill, M. Kahani, R. C. Arya *et al.,* "Healthfog: An ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments," *Future Generation Computer Systems*, vol. 104, no. 2, pp. 187–200, 2020.

[10] R. Farah Sayeed, S. Princey and S. Priyanka, "Deployment of multicloud environment with avoidance of ddos attack and secured data privacy," *International Journal of Applied Engineering Research*, vol. 10, no. 9, pp. 1–8, 2015.

[11] X. Li, X. Huang, C. Li, R. Yu and L. Shu, "EdgeCare: Leveraging edge computing for collaborative data management in mobile healthcare systems," *IEEE Access*, vol. 7, no. 10, pp. 22011–22025, 2019.

[12] B. Karthikeyan, T. Sasikala and S. B. Priya, "Key exchange techniques based on secured energy efficiency in mobile cloud computing," *Applied Mathematics & Information Sciences*, vol. 13, no. 6, pp. 1039–1045, 2019.

[13] I. Yaqoob, K. Salah, R. Jayaraman and Y. Al-Hammadi, "Blockchain for healthcare data management: Opportunities, challenges, and future recommendations," *Neural Computing and Applications*, vol. 34, no. 3, pp. 1–16, 2021.

[14] E. S. Madhan and R. Annamalai, "A novel approach for vehicle type classification and speed prediction using deep learning," *Journal of Computational and Theoretical Nanoscience*, vol. 17, no. 5, pp. 2237–2242, 2020.

[15] R. S. Jenifer and J. Arunajsmine, "Social media networks owing to disruptions for effective learning," *Procedia Computer Science*, vol. 172, pp. 145–151, 2020.

[16] J. E. Thoma and M. A. Waite, "Experiences of nurse case managers within a central discharge planning role of collaboration between physicians, patients and other healthcare professionals: A sociocultural qualitative study," *Journal of Clinical Nursing*, vol. 27, no. 5–6, pp. 1198–1208, 2018.

[17] C. Saravana Kumar, "An authentication technique for accessing de-duplicated data from private cloud using one time password," *International Journal of Information Security and Privacy*, vol. 11, no. 2, pp. 1–10, 2017.

[18] D. Paulraj, "An automated exploring and learning model for data prediction using balanced CA-SVM," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 5, pp. 4979–4990, 2021.

[19] H. Zhang, J. Wang and Y. Ding, "Blockchain-based decentralized and secure keyless signature scheme for smart grid," *Energy*, vol. 180, no. 2, pp. 955–967, 2018.

[20] V. P. Sakthivel, M. Suman and P. D. Sathya, "Combined economic and emission power dispatch problems through multi-objective squirrel search algorithm," *Applied Soft Computing*, vol. 100, no. 7, pp. 106950, 2021.

[21] P. Velmurugadass, S. Dhanasekaran, S. S. Anand and V. Vasudevan, "Enhancing blockchain security in cloud computing with IoT environment using ecies and cryptography hash algorithm," *Materials Today: Proceedings*, vol. 37, pp. 2653–2659, 2021.

[22] N. Iqbal, F. Jamil, S. Ahmad and D. Kim, "A novel blockchain-based integrity and reliable veterinary clinic information management system using predictive analytics for provisioning of quality health services," *IEEE Access*, vol. 9, pp. 8069–8098, 2021.

[23] M. Pourvahab and G. Ekbatanifard, "Digital forensics architecture for evidence collection and provenance preservation in IaaS cloud environment using SDN and blockchain technology," *IEEE Access*, vol. 7, pp. 153349–153364, 2019.

[24] A. A. Abdellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini *et al.,* "ssHealth: Toward secure, blockchain-enabled healthcare systems," *IEEE Network*, vol. 34, no. 4, pp. 312–319, 2021.