Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-024-04780-4

ORIGINAL RESEARCH

An improved blockchain framework for ORAP verification and data security in healthcare

Parag Rastogi[1] · Devendra Singh[2] · Sarabjeet Singh Bedi[3]

Received: 28 July 2023 / Accepted: 28 February 2024

Abstract

Currently, the move from traditional healthcare to smart healthcare systems is greatly aided by current technology. Healthcare proposes a new healthcare model that is patient-centered using advancements in wearable sensors, connectivity, and the Internet of Things (IoT). The administration of enormous amounts of data, including reports and pictures of every individual, increases human labour requirements and security hazards. This study shows how a blockchain-based Internet of Things might improve patient care while lowering costs by using medical resources more wisely. Initially, Resource Provider's IoT data will be sensed and encrypts using Diffie Hellman Galois–Elliptic-curve cryptography (DHG-ECC). Next, from the extracted attributes, the optimal features will be selected by using Pearson Correlation Coefficient based Sand Cat Optimization Algorithm (PCC-SCOA). After that, the selected optimal features will be combined and converted into hashcode using the Digit Folding–Streebog Hashing algorithm. This hashcode will be constructed in the form of Smart Contract. Next, the Resource Requester (Doctor or Nurse) sends the Role Request with the Combined Linear Congruential Generator–Digital Signature Algorithm (CLCG-DSA). The next Resource Requester will be matching the hashed access policy with Blockchain. The proposed models are used to compare the performance of proposed design using feature selection time, Encryption time, Decryption time, security level, signature creation time and signature verification time. Our proposed method DHGECC approach achieves 96.123% higher security.

Keywords Diffie Hellman Galois–Elliptic-curve cryptography · Pearson correlation coefficient based Sand Cat Optimization Algorithm · Digit Folding–Streebog Hashing algorithm · Combined linear congruential generator-digital signature algorithm

✉ Parag Rastogi
parag0305@gmail.com

Devendra Singh
dev625@yahoo.com

Sarabjeet Singh Bedi
dearbedi@gmail.com

[1] Department of Computer Science and Engineering, IFTM University, Delhi Road, NH-24, Lodhipur Rajput, Moradabad, Uttar Pradesh 244102, India

[2] Department of CSE, IFTM University, Delhi Road, NH-24, Lodhipur Rajput, Moradabad, Uttar Pradesh 244102, India

[3] Department of CS and IT, MJP Rohilkhand University, Pilibhit Bypass Rd, Bareilly, Uttar Pradesh 243006, India

1 Introduction

The Internet of Things (IoT) has become a crucial technological advancement in recent years for overcoming challenges related to interoperability, heterogeneity, and Internet-awareness. On the other hand, blockchain is preparing to support infrastructure for security, immutability, and trustlessness. Another industry that directly affects people's lives is healthcare (Ray et al. 2020). A shared or dispersed database keeps track of a growing list of transactions, or blocks, known as the blockchain (BC). Blockchain technology, commonly referred to as the chain of trust, can simplify corporate procedures by providing trust, accountability, and openness (Sadiku et al. 2018). Medical records, prescription drug data, and insurance information have all undergone significant changes thanks to the internet of things paradigm's rapid advancements (Ray et al. 2020; Griggs et al. 2018).

Published online: 12 April 2024

The IoT-based medical devices can assist in the collection of priceless patient data, automate workflows, offer insights into the symptoms and trends of diseases, make remote care easier, and give patients greater choice over their lives and treatments (Tao et al. 2018; Aazam et al. 2020; Ali et al. 2020). A subset of IoT technologies, the Internet of Medical Things (IoMT) consists of interconnected medical and healthcare IT applications and devices. Compared to other IoT systems, IoMT requires a more extensive security architecture because of the sensitivity and stringent rules surrounding healthcare data. Patients can be monitored in real-time with IoT devices. Additionally, they might lessen the necessity of visiting hospitals for regular health examinations. Hospital stays or readmission costs may be decreased with the aid of connected home health monitoring devices. Through warnings and trigger notifications, IoT-enabled medical devices can help with diagnosis before it gets serious (Awais et al. 2019; Zhu et al. 2019; Jiang et al. 2019; Ali et al. 2021). Information can be collected by sensors attached to equipment and sent, where a doctor can look for any potential problems. Vital signs are included in some IoT healthcare solutions. However, breaches of privacy, authorization, and authentication could occur with these solutions (Gholamhosseini et al. 2019; Sicari et al. 2020). The Internet of Things makes it easier and faster, elderly care, and exercise programs (Kaur et al. 2019; Jaigirdar et al. 2019). Medical IoT technology should be trusted for its dependability, privacy, and security requirements (Yaqoob et al. 2022). Physical and technical safeguards have been implemented by the “Health Insurance Portability and Accountability Act (HIPAA)” to stop the healthcare industry's data from getting out. However, these measures were insufficient, and more stringent and up-to-date security standards ought to be implemented (Saxena et al. 2021; Haque et al. 2022).

In spite of requiring a minimum amount of time and space, this study creates a novel, reliable, and universal framework to perform medical data operations via fog node networks and block chain. This framework includes cloud services that include retrieval, collaboration, and secure audiovisual preservation. The main aim of this paper is to design a novel framework to perform efficient Optimized Role-based Access Policy (ORAP) verification with blockchain and Data Security in Healthcare using PCCSCOA-DFSTREEBOG and DHG-ECC with CLCGDSA. User, Resources, Actions, and Ecological factors are among the parts of the model that require ORAP verification. Determining precise and standardized responsibilities that represent the goals and requirements of the corporation is a crucial first step in optimizing RBAC for Identity and Access Management (IAM). Users' roles ought to be determined by the duties and responsibilities they carry out, not by their titles or positions. Additionally, roles ought to be specific enough to prevent permission conflicts or overlaps, but not so specific as to add needless complexity or maintenance burden. Using a role engineering approach, which entails analyzing the current users, resources, and permissions before developing and documenting the roles and their interactions, is an effective approach role.

From aforementioned concerns, the significance of the research as follows:

To better comprehend and construct, security requirements must be established. Healthcare organizations all over the world are transforming into systems that are more user-centered, coordinated, and effective using a variety of multimedia methods. Enormous amounts of data, such as individual reports and photos, increases the need for human labor and poses security risks. IoT in healthcare reduces costs and improves patient care quality to address these issues by efficiently allocating medical resources. Then the contribution of the research is,

- To perform efficient Hashed Access Policy generation, the Digit Folding-based Streebog hashing algorithm will be used.
- To improve the process of Hashed Access Policy generation, Optimized Attributes will be selected by using Pearson Correlation Coefficient based Sand Cat Optimization Algorithm (PCC-SCOA).
- To improve data security, Diffie Hellman Galois –Elliptic-curve cryptography (DHG-ECC) technique will be introduced.
- To perform efficient user verification, Combined Linear Congruential Generator – Digital Signature Algorithm (CLCG-DSA) will be introduced.
- To compare the proposed technique with the existing technique using the result parameters like Hash code generation time, Encryption Time, Decryption and Security Level, attribute selection time, fitness vs iteration, signature generation time, and signature verification time, etc.

The remainder of the research is structured as follows. Section 2 discusses related works. Section 3 describes the proposed methodology. Section 4 presents the results and discussion. Section 5 concludes the research work.

2 Literature review

This review explains a thorough analysis of related research on the many methods that the researchers have employed over the years. The publications that were chosen give a broad overview of various methodologies, classification algorithms, the role that blockchain schemes play in IoMT, as well as the various optimization strategies utilized by various researchers in recent years. Leng et al. (2019) combine upper-level optimization with lower-level self-organization.

A decentralized organizational structure is preferable because centralized control of the IIoT is less flexible in coping with disruptions and changes. A permissioned block chain-driven IIoT can enable partially decentralized self-organization and thus offload and speed up the optimization of industrial planning at a higher level.

Yun et al. (2020), the optimal throughput configuration is dynamically determined through the use of the DQNSB method. The sharded blockchain's security and latency are characterized by us. Taking into account the volume of malicious attacks on the consensus process, the DQNSB system modifies the blockchain parameters to raise the level of security and determines the level of maliciousness using analytical. Awotunde et al. (2022) the complexity and costly characteristics of healthcare system can be reduced through the application of blockchain and improvement on medical record management. This has been proved useful in transactions involving medical records, security of data, smart contacts, and insurance billing and by providing a distributed database of transactions. On the authentication of the users associated with the healthcare records, the blockchain network likewise adheres to the ideal of maximum confidentiality, thus help in securing the medical information.

Khalaf et al. (2021), because it required a data storage solution that was secure, dependable, and completely transparent, blockchain emerged as the preferred IoT-based digital storage on WSN. In accordance with WSN data storage, the paper builds the node recognition mechanism using blockchain technology. In order to make use of it in a variety of forensic investigations and decision-making processes, such data must be safely stored and tracked. To achieve WSN, ODSD uses cutting-edge analytical methods to describe and evaluate the behaviors of wirelessly driven networks.

Shynu et al. (2021), efficient disease prediction services based on safe fog computing on the blockchain for healthcare Diabetes and cardiovascular diseases are taken into account when making predictions. Finally, a feature selection-based adaptive neuro-fuzzy inference system is used to predict the occurrence of diabetes and cardiovascular illnesses (FS-ANFIS).

Le Nguyen et al. (2020) for dependable and secure IoT data exchange, we combine the Secure Ant Colony optimization with the Multi Kernel Support Vector Machine (ACOMKSVM) and Elliptical Curve cryptosystem (ECC).

Mahajan et al. (2023) blockchain-based security solutions have attracted a lot of attention recently since they can offer reliable protection for data storage and sharing with the least amount of computational work.

Akhter et al. (2022) when blockchain (smart contract) technology is combined with conventional database management solutions, it significantly improves data security, authenticity, time management, and other aspects of data administration. As a result, it is difficult to protect data privacy and accountability in the system. Chauhan et al. (2022) Most IoT systems now use blockchain, one of the safe technologies. The Blockchain's obvious features, such as decentralisation, immutability, transparency, security, and privacy, are hardly the important reasons for employing it in medical care settings.

Some of the drawbacks of current research methods are as follows: Because they are connected to a variety of network sharing devices, Internet of Things systems are more vulnerable to cyberattacks. Improved IoT security currently relies on complex and laborious computations. In addition, it is challenging to perform complex computations and secure IoT networks using devices with limited resources. Traditional access control methods that centrally manage user rights and access information make it simple to use a single point of failure. The current methods for IoT healthcare data security use a lot of power and cost more because they require a lot of cryptographic computations. The proposed method has efficient Hashed Access Policy generation, data security and user verification. We have created a novel security issue for IoT-enabled healthcare systems to address this issue.

The work in this paper is motivated from various Literature where data security work has been done in HIE (Healthcare Information Exchange) with a symmetric key approach where everyone has to send their private key while data sharing. The proposed method has efficient Hashed Access Policy generation, data security and user verification. We have created a novel security for IoT-enabled healthcare systems to address this issue.

3 Proposed methodology

The management of enormous data quantities, including reports and photos of every individual, raises security threats and the demand for human labor. IoT in healthcare reduces costs while raising the quality of patient care through efficient use of available resources. This helps to solve these problems. IoT devices, however, are susceptible to numerous dangers that may be started by different intruders. Resource Provider's IoT data will be sensed and encrypts by using the available ECC settings to solve the Discrete Logarithm Problem, attackers can take advantage of existing ECC and commit attacks. Therefore, the main emphasis of IoT explanations should be security. It has been determined that blockchain technology is the best way control system in real-time settings. The shared communications protocols and interface techniques that hosts in a network of communications utilize are specified by the application's layer, which is an intermediate layer of abstraction. It is the layer that is closest to the user, suggesting that direct interaction between the end user as well as the programmed application is possible between the user and the application's layer of data. Figure 1 shows the recommended structure in detail.

The proposed System will start from Resource Provider (Patient with IoT). Initially, Resource Provider's IoT data will be sensed and encrypts using Diffie Hellman Galois–Elliptic-curve encryption (DHG-ECC). By using the available ECC settings to solve the Discrete Logarithm Problem, attackers can take advantage of existing ECC and commit attacks. The Diffie-Hellman Galois Theory will be utilized to produce the secret key, which will then be used throughout the encryption and decryption processes in order to resolve this issue and enhance data security. Elliptic Curve Cryptography (ECC), RSA, and the Diffie-Hellman method will be compared to the suggested encrypted approach. The subsequent stage in the suggested methodology is feature extraction, which consists of eliminating characteristics from the data, including names, phone numbers, addresses, heart rates, ages, sexes, weights, and heights. Through the integration of hybrid deep learning techniques and block chain technology, the proposed framework provides a complete approach to improving security and scalability in healthcare systems. It offers a safe, auditable platform for exchanging and storing medical data while utilizing deep learning's analytical capabilities to glean insightful information. In the end, this framework can enable healthcare organizations to make knowledgeable choices, provide individualized treatment, and enhance patient outcomes in a safe and scalable manner. Using the result parameters such as Encryption time, Decryption time, security level, etc. Meantime, the data attributes such as device name, device address, protocol, port etc. and Resource Provider attributes such as MAC Address, Public Key, etc. will be extracted. Next, from the extracted attributes, the optimal features will be selected by using Pearson Correlation Coefficient based Sand Cat Optimization Algorithm (PCC-SCOA). In order to guarantee the privacy and confidentiality of block chain transactions along with information, cryptographic algorithms are crucial. Block chain transactions promise participant anonymity while maintaining transparency and traceability. This is made possible by cryptographic algorithm, hence the proposed work attains effectively improved block chain system.

Here, there is no significant improvement in the values of fitness of the population from one generation to another generation in the existing Sand Cat Optimization Algorithm. So in order to solve this problem, the Pearson Correlation

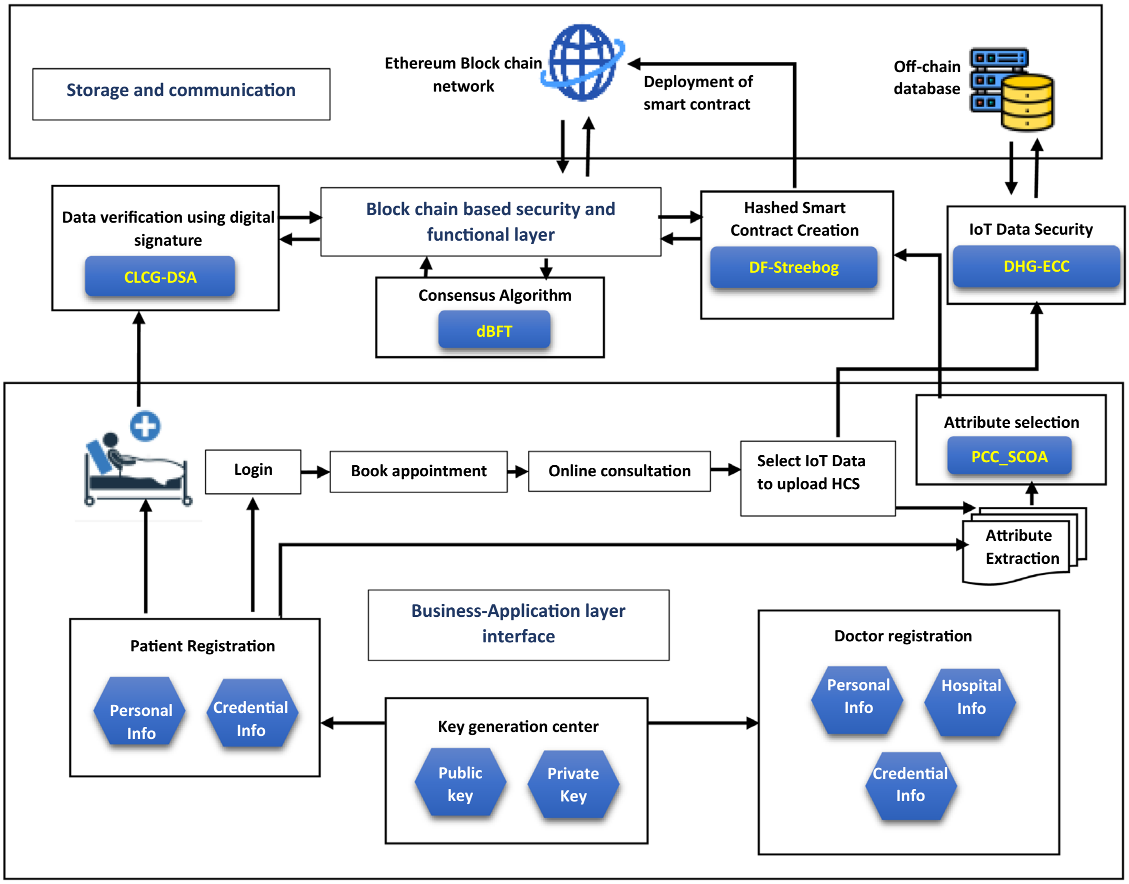


Fig. 1 Framework of proposed methodology

Coefficient technique will be introduced. After that, this proposed modified algorithm will be compared with the existing Spider Monkey Algorithm, Butterfly Optimization Algorithm, Red Fox Optimization Algorithm, and Sand Cat Optimization Algorithm using the result parameters, such as feature selection time, fitness vs iteration, etc.

After that, the selected optimal features will be combined and converted into hashcode using the Digit Folding—Streebog Hashing algorithm. This hashcode will be constructed in the form of Smart Contract. To improve the hashcode generation complexity, the digit folding technique will be added into existing Streebog Hashing algorithm. After that, this proposed modified algorithm will be compared with the existing SHA 512 Hashing Algorithm, MD 5 Hashing Algorithm, Tiger Hashing Algorithm, and Streebog Hashing Algorithm using the result parameters, such as hashcode generation time, hashcode length, etc. After that, this generated hashcode will be sent to Resource Provider. Next, Resource Provider registers their resource with blockchain in delegated Byzantine Fault Tolerance (dBFT) consensus algorithm using this Hashed Smart Contract.

Next, the Resource Requester (Doctor or Nurse) sends the Role Request with the corresponding Digital Signature. Here, the digital signature will be created using Combined Linear Congruential Generator – Digital Signature Algorithm (CLCG-DSA). In Existing DSA, the private key generator is compromised with a random value. So, in order to solve this problem, the Combined Linear Congruential Generator technique will be used to generate the private key. Here, the Resource Provider's ethereum account address and ethereum account public key will be combined with the Resource Requester ethereum account address and ethereum account public key, and the digital signature will be created. While Signature verification time Resource Requester and Resource Provider Hashcode matching will be done. If both hashcodes are matched, the Resource Requester will be added and a smart contract will be created based on their role. In addition, the hashed access policy of the corresponding files has been shared with the resource requester. If the hash code will be available in the blockchain, then the system allows accessing the encrypted data based on their role. If not, the process will be declined. Initially, Resource Provider's IoT data will be sensed and encrypts using Diffie Hellman Galois – Elliptic-curve cryptography (DHG-ECC). The Diffie Hellman Galois – Elliptic-curve cryptography is explained as follows.

3.1 Diffie Hellman Galois–Elliptic-curve cryptography (DHG-ECC)

Pre-processing activities for data cleaning and commotion eliminating are performed. Required data is likewise gathered to display or record for commotion and proper methodologies are determined for managing missing data and representing repetitive data for data normalization.

Text file encryption in the proposed paradigm uses Diffie Hellman Galois–elliptic-curve cryptography. With the use of an ECC key and a shared secret created by Diffie-Hellman, the input text file is converted into an encrypted format before being transferred to the server. Clients might decrypt after a successful key agreement. The aforementioned experiment uses a variety of text files of varying sizes (KB), and evaluation is based on factors including security level, encryption time, and decryption time. The encryption and decryption steps for Diffie Hellman Galois–Elliptic-curve cryptography.

Step 1: The input consists of various text files that range in size, expressed in KB. The files hospitalInfo.txt, patientinfo.txt, patientregistration.txt, and credentialinfo.txt are used as input. After the patient requests a file from the IOT, the server will choose that file to be encrypted.

Step 2: Elliptic curve will produce distinct private and public key pairs after receiving a text file as input. The text file will be encrypted using one of the key pairs created by an elliptic curve that is defined over a field, according to the advance encryption standard. Choose a number, d, from the range of n. We create the public key using the Eq. (1) below,

$$Q = d * P \tag{1}$$

d is a random number between (1 to n-1). P is a curve point. Public key Q. Private key is d. One key will be kept secret with the server, say "d," and one key will be kept hidden with the client, say "e," from among the several key pairs.

Step 3: By achieving a successful key agreement between the two communicating patients and the IOT, Diffie-Hellman will establish the shared secret between client and server. Let's see how the patient and IOT will come to an agreement to create the shared secret.

- They must first agree on a domain parameter (p, a, b, n, G, h).
- 'p' denotes the field where the elliptic curve is characterized, 'a' and 'b' are values defined over the curve, 'G' is the wind turbine point, which is fixed for a curve and recognized to both transacting entities, 'n' is a prime order of the generator point 'G, and 'h' is the plc, which denotes the number of points within the curve; for h = 1, each side will include a elliptic with the patient's and IOT's private keys sharing the same public key.
- If the server has the private key "d" and the patient has the key "e," they will both produce the public key. The generator point, or "G," will be fixed for them both and made known to them both.

- Server will determine its public key by computing Q(a) = dG. Similar to this, the client will calculate its public key, such as Q(b) = eG.
- Now that the shared secret has been calculated by both parties, they can exchange public keys by passing Q(a) to the client and Q(b) to the server.
- The client will calculate eQ and the server will compute dQ(b) (a).
- Assume that "S" stands for "shared secret," and S = dQ(b) = e Q(a) = deG.

As a result, the shared secret will only remain between the server and the client for that specific session, and anyone attempting to crack the shared secret must first figure out how to solve the discrete logarithm issue. Diffie-Hellman will handle the key agreement between client and server when encrypting the input text file on the other side. The client will only be able to decrypt the encrypted text file if the key agreement is successful.

Step 4: Using the Elliptic Curve Cryptography key, encrypt the message. The encrypted content is uploaded to the server using the combined key, which is a shared secret derived through Diffie-Hellman, after encryption has been completed. After a successful key agreement that creates a shared secret between the client and server, the client will download the encrypted file from the server and decode it using the combined key created by ECC and DH.

Step 5: Once the decryption process is complete, the client will have access to the original file. Finally, once encryption and decryption have been completed successfully, Diffie Hellman Galois—Elliptic-curve cryptography analysis is carried out based on specific metrics, such as encryption time, decryption time, and security level. The encryption time indicates how long it took to transform the original text file into the cypher file; the decryption time indicates how long it took to reverse the process. Moving on to storage, which is necessary to gauge the size of an encrypted file or cypher file created after encryption. For that IoT devices typically gather sensor data and send it to an IoT gateway for examination. After that, the data is safely uploaded to cloud storage by utilizing the cryptographic methods. This is the IoT system's backend, where all the data remains stored as well as ready to be utilized by the front-end framework to provide users with insights. Most importantly, the avalanche effect will reveal variations in the cypher file by changing the original input file a bit, and correlation will indicate the dependence between the cypher file and the original file, i.e. whether the relationship among the files is linear and increasing or linear but decreasing; additionally, if correlation is less, then both the cypher file and original file are dissimilar and it is challenging for an intrusive party to distinguish original text from cypher text.

3.2 Pearson correlation coefficient based sand cat optimization algorithm (PCC-SCOA)

We develop a two-stage feature selection technique for the Sand Cat Optimization Algorithm based on Pearson Correlation Coefficient. Utilizing the initial characteristics chosen by Pearson correlation coefficient feature selection techniques. The redundant and unnecessary features are further eliminated in the second stage using Sand Cat Optimization, leaving only the features chosen at the first stage. Each feature's importance is determined by its corresponding value, which is then ordered in order of decreasing importance.

Pearson Correlation Coefficients: The Inverse Pearson Correlation The correlation technique for feature selection is built on coefficients, a measurement of something like the linear relationship between the two variables X and Y. The Pearson Correlation formula is as follows in Eq. (2):

$$CO_{X,Y} = \rho(X, Y) = \frac{cov(X, Y)}{\sigma_X \sigma_Y} \tag{2}$$

where cov is the covariance of X and$Y$, and σ_X and σ_Y are the difference between X and Y's standard deviations. The research contains the covariance and standard deviation calculating formula. To determine the importance of a feature for feature selection, look at the Pearson's correlation between the feature and the class labels. Sand Cat Optimization Algorithm: The ability of sand cats to recognize low-frequency sounds in their environment is what gives the sand cat optimization (SCO) method its name. Hunting and prey assault are the sand cat's two primary activities. Scientific research show that the sand cat has astonishing frequency absorption at frequencies below 2 kHz. Sand cats are around 8 dB more sensitive than house cats at this frequency. The sand cat can follow prey and effectively hunt based on its location because to these distinguishing features. It is also capable of hearing (prey movement). The SCO algorithm uses sand cats to symbolize each variable in the issue. In a d-dimensional optimization space with n sand cats, matrix is identical to $N_{pop} \times N_d, (pop = 1, ..., n)$, as shown in Fig. 2

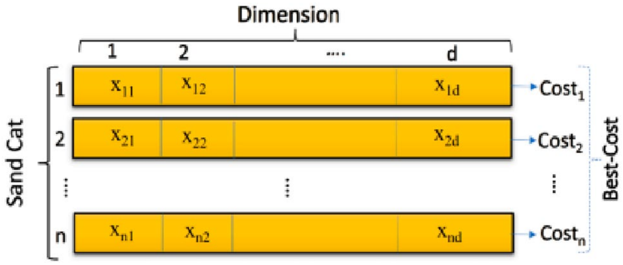


Fig. 2 Initial candidate matrix generation

3.3 Performance measures deep convolutional neural networks

For the purpose of calculating the performance efficacy of this model, a number of industry-standard performance criteria, including accuracy, sensitivity, and specificity, will be taken into account. In this scenario, accuracy would refer to the proportion of instances that properly predicted out of all the available examples. Precision is defined as the proportion of accurate predictions in the occurrences that fall into the positive category. The percentage of accuracy missing or inaccuracy present in the cases is known as classification algorithm. The classifier's effectiveness will be compared to that of other cutting-edge tools for predicting Parkinson's disease.

In the DCNN is a Deep Learning (DL) Method which is not quite the same as should be expected Convolutional Neural Network (CNN) as far as number of stowed away layers normally in excess of 5 which are utilized to remove more highlights and increment the exactness of the forecast. There are two sorts of DCNN, one is expanding the quantity of secret layers or by expanding the quantity of hubs in the secret layer.

Furthermore, a specific fitness function is used to determine the cost (or fitness value) of each sand cat. Each of the sand cats will provide a value for the associated function (i.e., candidate solution). The best solution is determined by the sand cat with the lowest value at the conclusion of an iteration, and in the next iteration, the other candidates (i.e., sand cats) attempt to migrate towards this best-chosen cat. Each sand cat gives a reaction that is indicated. by $X_i = \left(x_{i1}, x_{i2}, \ldots .x_{id}\right), (i = 1, \ldots, n)$. The low-frequency hearing talents of the sand cat are utilised by the SCO algorithm. The sand cat can sense frequencies lower than 2 kHz, as was before mentioned. As a consequence, it is assumed that a sand cat's sensitivity range when looking for prey begins at 2 kHz and stops at 0 kHz. The vector r G is introduced to describe this process and to simulate the method mathematically in Eq. (3).

$$\vec{r}_G = S_M - \left(\frac{S_M \times t}{t_{Max}}\right) \tag{3}$$

The S_M Since it is based on the sand cat's hearing qualities, value should be 2. Additionally, t stands for that may be performed at the most. The Eq. (4) is used to update each search agent's position throughout the search phase depending $(\overrightarrow{POS}_b)$ its current position $(\overrightarrow{POS}_c)$ and its sensitivity range $(\vec{r})$.

$$\overrightarrow{POS}(t+1) = \vec{r}.\left(\overrightarrow{POS}_b(t) - rand(0,1).\overrightarrow{POS}_c(t)\right) \tag{4}$$

Each sand cat has a different, which is determined by Eq. (5), to escape the local ideal trap.

$$\vec{r} = \overrightarrow{r_G} \times rand(0,1) \tag{5}$$

This is denoted by the symbol r _G, is linearly decreased from 2 to 0. Additionally, r displays each cat's sensitivity range. The following Eq. (6) is used to update each sand cat's position both after searching and during the attacking phase of SOC.

$$\overrightarrow{POS}(t+1) = \overrightarrow{POS}_b(t) - \vec{r}.\overrightarrow{POS}_{rnd}.\cos(\theta) \tag{6}$$

where (POS) _(rnd) represents the location of a randomly chosen sand cat based on the following Eq. (7), and is a random angle between 0 and 360.

$$\overrightarrow{POS}_{rnd} = \left|rand(0,1).\overrightarrow{POS}_b(t) - \overrightarrow{POS}_c(t)\right| \tag{7}$$

The final and crucial component of the method for determining when to switch between the investigation (seeking) and exploitation (attacking) phases is the R element.

$$\vec{R} = 2 \times \vec{r}_G \times rand(0,1) - \vec{r}_G \tag{8}$$

The SCO algorithm drives the search units to exploit when R is less than or equal to 1; otherwise, it drives them to explore and find prey. Equation (8) is the SCO algorithm's final updating position equation as a result.

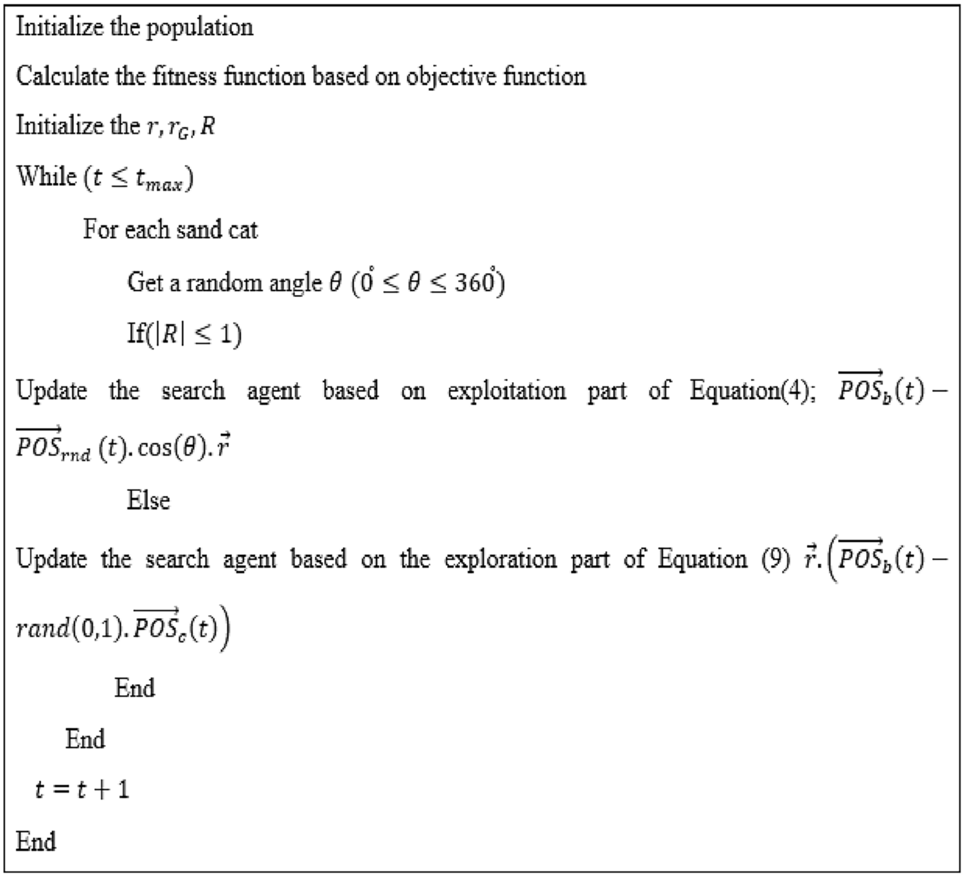
$$\vec{X}(t+1) = \begin{cases} \overrightarrow{POS}_b(t) - \overrightarrow{POS}_{rnd}.\cos(\theta)|R| \leq 1; expoitation \\ \vec{r}.\left(\overrightarrow{POS}_b(t) - rand(0,1).\overrightarrow{POS}_c(t)\right)|R| > 1; exploration \end{cases} \tag{9}$$

When |R| 1, as shown in Eq. (9), sand cats are told to attack their prey; if not, they are instructed to look for another workable solution in the region. The sand cat optimization's pseudocode is contained in Algorithm 1. (SCO). The extracted attributes, the optimal features will be selected by using Pearson Correlation Coefficient based Sand Cat Optimization Algorithm (PCC-SCOA).

Digit Folding—Streebog Hashing algorithm: The DF-SHA technique presents a secure decentralized access control system with blockchain support for Digit folding-streebog hashing. Blockchain technology uses a SmartContract concept. A smart contract is a transaction protocol designed to automatically carry out the provisions of a contract or agreement together with legally necessary events without relying on outside parties. Figure 3 shows how a blockchain is built using the many blocks that make up a chain. Each block in the chain has a root hash, a before it (p_hash). The blockchain contains various transaction data (generally represented as a hash). Information about the students' learning is included in each transaction. Each block also has a block header. The prior block's hash (p_hash), as displayed in the blockchain, is utilized for block verification. When referring to time steps (Ts), the block's creation time is meant. The student data gathering from the dataset is part of each block transaction. The DF-SHA technique presents a secure decentralised access control system with blockchain support for Digit folding-streebog hashing. Before gaining access to the IOT, both the user and the device must be authenticated. To do this, the Device or User must provide the IOT access to their credentials in this case stand in for the registration credentials. The user or device then sends the relevant as shown below Eq. (10),

$$U_i H(UID) \oplus H(UPW) \oplus H(Fv) \tag{10}$$

Algorithm 1 Sand cat optimization algorithm



```
Initialize the population
Calculate the fitness function based on objective function
Initialize the $r, r_G, R$
While $(t \le t_{max})$
        For each sand cat
            Get a random angle $\theta$ $(0^{\circ} \le \theta \le 360^{\circ})$
            If$(|R| \le 1)$
Update the search agent based on exploitation part of Equation(4); $\overrightarrow{POS}_b(t) - \overrightarrow{POS}_{rnd}(t).\cos(\theta).\vec{r}$
            Else
Update the search agent based on the exploration part of Equation (9) $\vec{r}.\left(\overrightarrow{POS}_b(t) - rand(0,1).\overrightarrow{POS}_c(t)\right)$
           End
      End
  $t = t + 1$
End
```

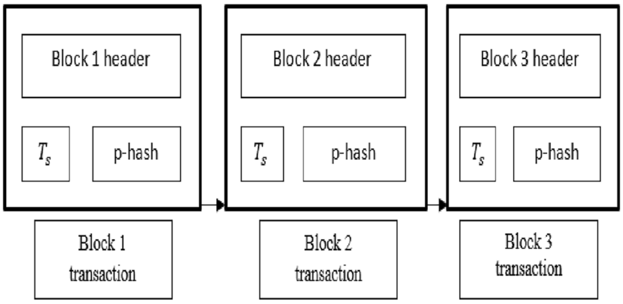


Fig. 3 Construction of Blockchain

Algorithm 2 Streebog Hashing algorithm

```
Start
        Pad (M→ $pad\ M_k)\|M_{(k-1)}\| \dots \|M_0$
            Assign $H_0 = Initial\ value$
$N_0 = 0$
        For $i = 0; i < (K-1); i++$
$H_{(i+1)} = g(H_i, M_i, N_i)$
$N_{(i+1)} = N_i + 512\ mod\ 2^{512}$
$\sum \leftarrow \sum + M_i mod\ 2^{512}$
$H_{(K+1)} = g(H_K, M_k, N_k)$
$N_{(K+1)} = N_k + \rho mod\ 2^{512}$
$\sum \leftarrow \sum + M_k mod\ 2^{512}$
$H_{(K+2)} = g(H_{K+1}, N_{(K+1)}, 0)$
$H = g(H_{(K+2)}, \sum, 0)$
Return $(H)$
End
```

The blockchain's Streebog hashing algorithm is utilized for hash creation. The Streebog hashing method is a brand-new, compact hashing algorithm that uses the stages depicted in the pseudocode below to generate hash values in 256-bit and 512-bit formats: 1 displayed as a function of compression, message M (g). The M is initially separated into I message blocks and padding. Then, each message block Mi is subjected to the compression function. Finally, the sum of all message blocks is used to create. The AuthCre is by message M in the proposed DBA protocol. Each credential is hashed using the Streebog algorithm's process. The Cloud receives this hash value. This signifies that the credentials of the User or Device are unknown to the Cloud. Hash values are used to send all credentials to the cloud. The blockchain server, which is in charge of maintaining the blockchain, receives the AuthCre from the Cloud after that. The blockchain server examines the corresponding block to validate the credentials. The blockchain server delivers a Valid () notification to the Cloud if the credentials are valid. If not, the cloud receives an Ignore () report. Depending on the report the cloud receives, it either approves or rejects the user or device request.

In Fig. 4 only be used to attack Hash schemes of a specific kind, like encounter attacks that use of modified packet attacks. When the input length is 264 bits and the output length is 160 bits, the algorithm has three phases: (1) news that has been stuffed to a length of 512 times less than 64; The procedure for filling is to add a "1" before a "0" until the news reaches the required length; the subsequent request for less than one bit of stuffing; (2) Following the completion of the first step, a further 64 bits were filled before the value; Enter the digit fold 5 word cache to start the cache; each word is 32 bits, as shown by Eq. (11).

$E\{w(kT_0), w^T(jT_0)\} = Q(kT_0)\delta_{kj}(11)$

Find the function key code that corresponds to the shop address, which is one. The function f (key) = key can be used to store M collected data in a storage unit if the maximum key for m is set to 1, although doing so will waste a lot of space or make it impossible to assign that much space. There may be numerous keys that translate to the same hash address after the cryptographic hash transformation since the set secret code is often much bigger than the collection of hash addresses. A different hexadecimal number is changed back into its initial for use as the key value during the radix conversion process. This number is then selected to serve as the hash address. A method of calculating that divides key

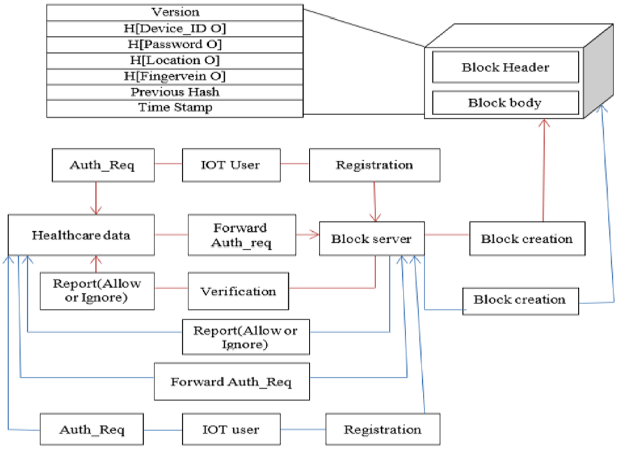


Fig. 4 Process of Digit folding streebog hashing algorithm

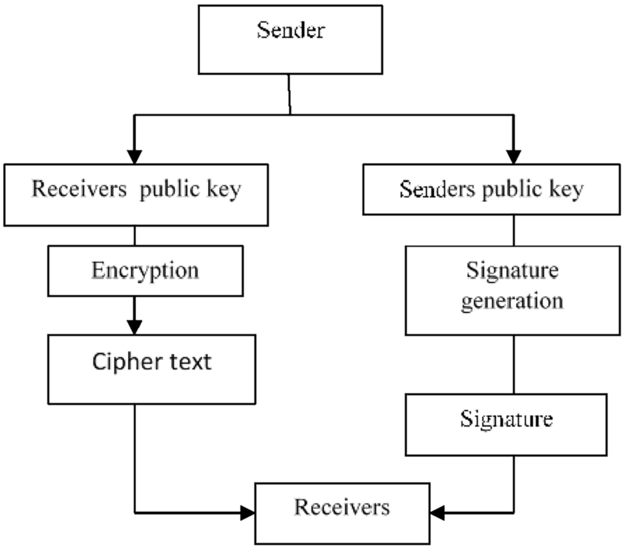


Fig. 5 Flow Process of Signcryption

codes for the same digit into multiple parts, uses, and uses the result as a hash address is referred to as the "digit folding method." Splitting key codes with the same digit is possible. into multiple parts using this technique.

Combined Linear Congruential Generator-Digital Signature Algorithm (CLCG-DSA): Using a Combined Linear Congruential Generator signcryption system, the proposed Combined Linear Congruential Generator—Digital Signature Algorithm technique performs safe data transmission from sender to recipient. To improve the speed of secure data transmission, the Combined Linear Congruential Generator signcryption technique combines three key operations: key generation, signcryption, and decryption. Figure 5 shows the Flow Process of Signcryption.

3.3.1 Key generation

The suggested method first generates key pairs, such as private and public keys. HMAC-SHA256 is one of the key generation protocols included in the proposed research. Consequently, a rapid and elementary protocol that guarantees message integrity and authentication for that particular interaction in a transaction.

This raises the level of confidentiality by making it easier to prevent unauthorized access. While the public key is made available for use in other applications, the private key is kept confidential. The combined congruential linear pseudorandom number generator is typically used to carefully limit the amount of memory that is available as per Eq. (12)–(15).

$$g = z_1.R_1 mod m_1 \tag{12}$$

$$h = z_2.R_2 mod m_2 \tag{13}$$

$$Q = \left[g * h\right] \tag{14}$$

$$P = \left[g, h\right] \tag{15}$$

where, Q indicates a public session key, 'P' denotes a private key. In this way, the pair of session keys are generated.

3.3.2 Signcryption

The suggested Combined Linear Congruential Generator–Digital Signature Algorithm approach accomplishes encryption and digital signature generation simultaneously after generating the pair of keys.

Encryption and signature creation are the two main steps in the signcryption process. The input data, which is plain text, is first encrypted to make it unreadable (i.e. ciphertext). Let's have a look at the encrypted data CD1, CD2, CD3, CDn. This is how the encryption procedure is carried out.

Let's treat the data CD as normal text. The input data's ciphertext is obtained as Eq. (16),

$$K \leftarrow CD^2 mod Q_r \tag{16}$$

where K denotes a ciphertext of original data CD,Q_r is a session public key of the receiver. The sender's private key is generated concurrently with the signature. A legitimate digital signature is used to confirm that the original material is real and was not changed by any outsiders. As a result, the secret private key is used to generate digital signatures. A hash value is used to create this digital signature. Any function that converts data of random size into data of predetermined length is known as a hash value. Consider the random number "R," which is used to create the signature as Eq. (17):

$$\beta_s = h(CD||R) \tag{17}$$

From (14), β_s indicates a sender-generated signature, () The hash function in cryptography represents a concatenation. The recipient receives the encrypted data together with the signed message.

3.3.3 Unsigncryption

The proposed method also performs unsigncryption, which includes decryption and signature verification at the receiver end. The unsigncryption procedure receives the ciphertext as input. The sender's public key is used to first confirm the signature Eq. (18). first calculate,

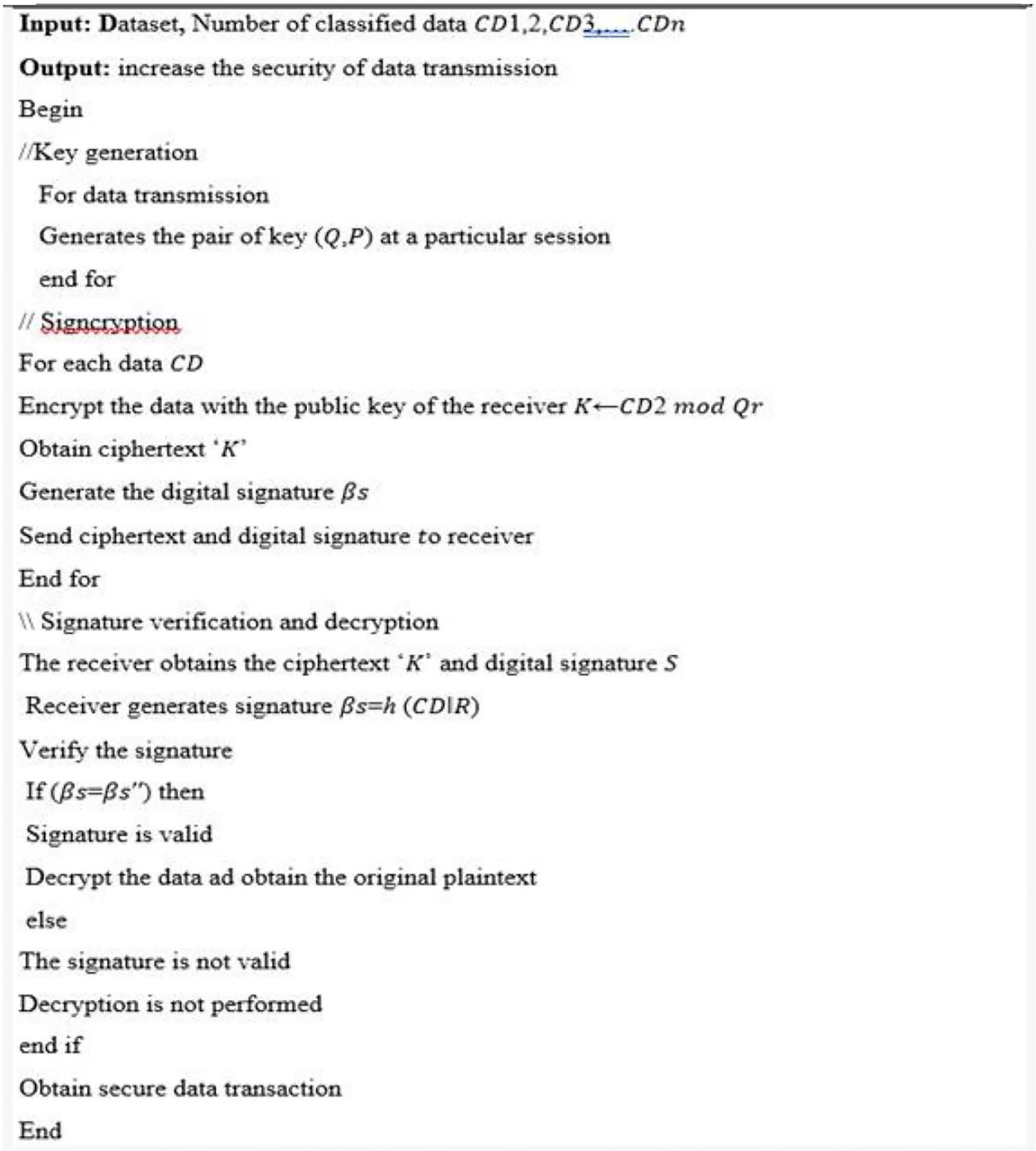
$$\beta s\prime = h(CD||R) \tag{18}$$

where, $\prime =$ denotes a receiver signature. Verifies that the generated signature is s$\prime =$ matches a signature produced at the sender's' before concluding. Both signatures must match for it to be considered valid and the recipient to be considered approved. The original data was then delivered to the authorised user. If the signature is not legitimate, the receiver is considered to be an attack and did not get the original data. The following Eq. (19) describes how to achieve the decryption process:

$$CD = (ug.g.bh - uh.h.bg) \text{ mod } Q \tag{19}$$

Where, $bg = K4\ 1(h+1)\ g\ bh = K4\ mod\ h,\ ug.\ g + uh.\ h = 1$ (16), which indicates original data. This improves data secrecy by performing secure data transmission from source to recipient. The algorithmic procedure for secure data transfer.

Algorithm 3 Combined Linear congruential generator-Digital Signature Algorithm



```
Input: Dataset, Number of classified data $CD1,2,CD3,....CDn$
Output: increase the security of data transmission
Begin
//Key generation
  For data transmission
  Generates the pair of key $(Q,P)$ at a particular session
  end for
// Signcryption
For each data $CD$
Encrypt the data with the public key of the receiver $K \leftarrow CD2 \; mod \; Qr$
Obtain ciphertext '$K$'
Generate the digital signature $\beta s$
Send ciphertext and digital signature to receiver
End for
\\ Signature verification and decryption
The receiver obtains the ciphertext '$K$' and digital signature $S$
 Receiver generates signature $\beta s = h \; (CD|R)$
Verify the signature
 If $(\beta s = \beta s'')$ then
 Signature is valid
 Decrypt the data ad obtain the original plaintext
 else
The signature is not valid
Decryption is not performed
end if
Obtain secure data transaction
End
```

Algorithm 3 describes Combined Digital Signature Algorithm signcryption using the Linear Congruential Generator. The categorised data are first used as an input. The recipient's public key and sender's private key would then allegedly be generated via a combined linear congruential key creation procedure. The receiver is the one who verifies the signature. If the two signatures match, the receiver decrypts the data and obtains the original. In all other circumstances, decryption is not performed. The security and level of data confidentiality are improved by this.

4 Results and analysis

Here, the experimental results obtained using the suggested framework have been compared to those obtained using the prevalent methods. The dataset used in the proposed framework is the “data.gov.in” Dataset. This dataset is collected from publically available sources using the below link. The dataset used in the proposed framework is “Heart Disease Dataset, Obseity Dataset, Womens Dataset and Polycystic ovary syndrome (PCOS)”. This dataset is collected from the publically available sources using

Table 1 Experimental setup

Hardware setup	Processor	Intel i5/core i7
	memory	4 GB
	Operating system:	Windows 10
Software setup	platform	Python
	Flash	A web framework for blockchain
	Postman	Display the information
Simulation criteria	CPU Speed	3. 20 GHz
	System Type	64 bit

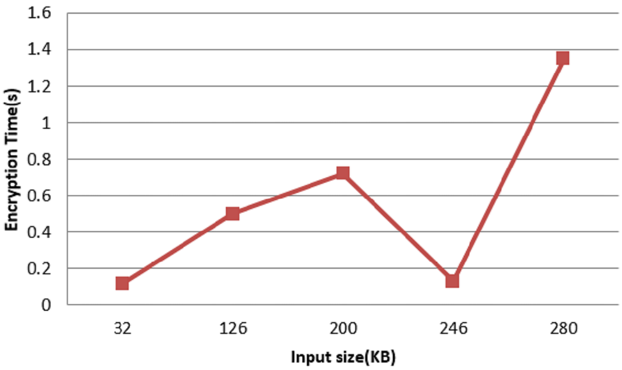


Fig. 6 Encryption time of proposed method

below link. https://www.kaggle.com/ronitf/heart-diseaseuci/discussion/105877, https://www.kaggle.com/datasets/lesumitkumarroy/obesity-data-set, https://www.kaggle.com/prasoonkottarathil/polycystic-ovary-syndrome-pcos.

4.1 Experimental setup

The proposed work is implemented in the working platform of PYTHON. Python is a popular high-level, general-purpose programming language. Thanks to its emphasis on code readability, coders may contribute ideas using its syntax and with less lines of code. Programming language called Python makes it possible to work quickly and integrate systems more successfully. The virtual environment tool produces a standalone Python environment that is entirely distinct from the system-wide Python environment (in the form of a directory). The Following are the stages of a blockchain's execution along with the proposed experimental setup which is shown in Table 1.

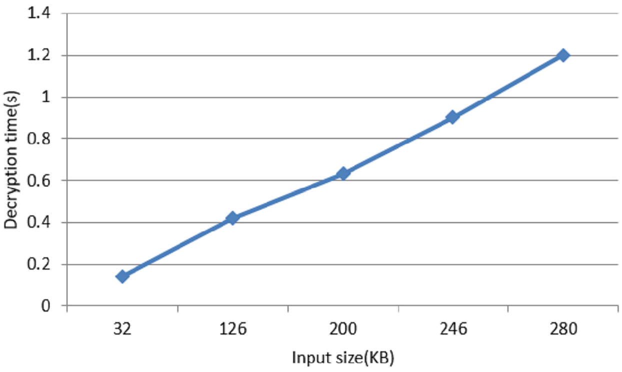


Fig. 7 Performance assessment of proposed DHGECC by means of Decryption time

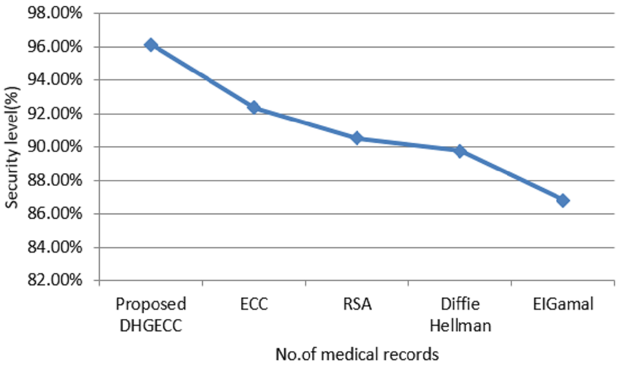


Fig. 8 Security level evaluation of proposed DHGECC technique

In this, the proposed encrypted technique will be compared with existing techniques such as Elliptic Curve Cryptography (ECC), RSA, and Diffie Hellman algorithm, etc. using the result parameters such as Encryption time, Decryption time, security level, etc.

The information investigation addresses cross-approval aftereffects of a DCNN model for each of the 5 exercises. It is addressed the arrived at the midpoint of aftereffects of 5 distinct folds. Standardized disarray framework shows how well the classifier achieves on every motion, and mean upsides of 5 lines of seven measures are addressed in the Fig. 3 where the actions are classified using DCNN. The model perceives Move forward activity with review of 1000, and accuracy, particularity, and F1-score are almost 1.000, and the exactness is 99.99%.

Figure 6 illustrates how long the DHGECC technique took to encrypt the data. The graph is produced to show the relationship between the amount of data and the encryption time, and it shows that as the data size rises, so does the encryption time. The performance of the proposed DHGECC is compared against ECC, RSA, Diffie Hellman, and ELGamaml techniques. The encryption time varies for the other widely used algorithms in a manner similar to this. Compared to the other strategies, which are clear from the graph, the DHGECC method takes less time to encrypt the data.

A contrast of decryption times may be observed clearly in Fig. 7. The decryption time is used to calculate how

Table 2 Encryption decryption time analysis

Algorithm	File size(KB)	Encryption time (s)	Decryption time(s)
Proposed DHGECC	32	0.12	0.14
	126	0.50	0.42
	200	0.72	0.63
	246	0.13	0.90
	280	1.35	1.20
ECC	32	0.13	0.15
	126	0.52	0.43
	200	0.74	0.66
	246	0.11	0.93
	280	1.39	1.23
RSA	32	0.45	0.43
	126	1.03	0.85
	200	1.41	1.13
	246	1.75	1.30
	280	1.83	1.64
Diffie Hellman	32	0.15	0.15
	126	0.46	0.44
	200	0.72	0.63
	246	0.95	0.83
	280	1.12	1.10
EIGamal	32	0.45	0.42
	126	1.02	0.81
	200	1.42	1.28
	246	1.76	0.85
	280	0.95	1.63

long it takes to decode data once it has been encrypted. Less decryption time, along with encryption time, is a sign of high performance. The performance of the existing ECC, RSA, Diffie Hellman, and ELGamaml techniques is compared to the decryption time performance. The DHGECC algorithm requires less time to decode data than the current ECC does. The current decryption times for RSA and Elagamal also differ from one another. Therefore, the DHGECC approach is better than the other widely used methodologies. Subsequently, the acquired security level (SL) for the DHGECC is evaluated. The security level acquired by the DHGECC is connected with the prevalent (blockchain-based medical data exchange), RSA, and ECC in Fig. 8. The assessment shows that the DHGECC approach achieves 96.123% higher security. However, in comparison, the current system has a lesser level of security. Consequently, data security and data encryption techniques are used in conjunction with BC technology. As a result, the proposed structure has performed better in terms of security.

In this experiment, the encryption speeds of symmetric and proposed DHGECC's techniques are compared. We raise the size of the healthcare file from 32 to 280 KB, and it is clear that the proposed DHGECC’s encryption time is quite near to that of symmetric techniques. Table 2 shows that encryption time lowers with smaller file sizes (32 KB), as well. Table 3 compares the memory and security level analysis of different encryption algorithms.

By employing five different file sizes, we analyse the decryption times of proposed DHGECC's and symmetric methods and come to the conclusion that proposed DHGECC's decryption times are negligible compared to symmetric techniques. Additionally, we noticed that because we are utilising a smaller file size (32 KB), the decryption time of proposed DHGECC's is comparable to that of ECC.

Figure 8 shows the Security level evaluation of proposed DHGECC technique.

Figure 9 shows the comparison of memory usage between DHGECC and other existing ECC, RSA, Diffie helman, EIGamal algorithms performance of decryption. It can be seen that DHGECC used the smallest amount of memory while other existing are largest amount of memory.

Figure 10 shows the comparison of memory usage between DHGECC and other existing ECC, RSA, Diffie helman, EIGamal algorithms performance of encryption. It can be seen that DHGECC used the smallest amount of memory while other existing are largest amount of memory.

In data security in healthcare using PCCSCOA-DFSTREEBOG and DHG-ECC with CLCGDSA the parameters are Hashcode generation time, verification time, key generation time. Figure 11 shows the time measure performance. The Hashcode generation time is 324 ms, verification time is 345 ms, key generation time is 1845 ms. The

Table 3 Comparison of memory and security level analysis

Method	Memory Usage on Encryption	Security Level	Memory Usage on Decryption
Proposed DHGECC	1.58*10^8	96	1.58 *10^8
Existing ECC	1.63 *10^8	94	1.63 *10^8
Existing RSA	1.76 *10^8	91	1.76 *10^8
Existing Diffie Hellman	1.88 *10^8	88	1.88 *10^8
Existing ElGamal	1.99 *10^8	85	1.96 *10^8

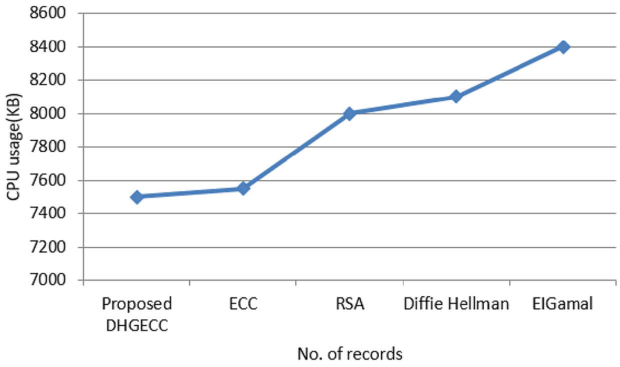


Fig. 9 Memory usage on decryption

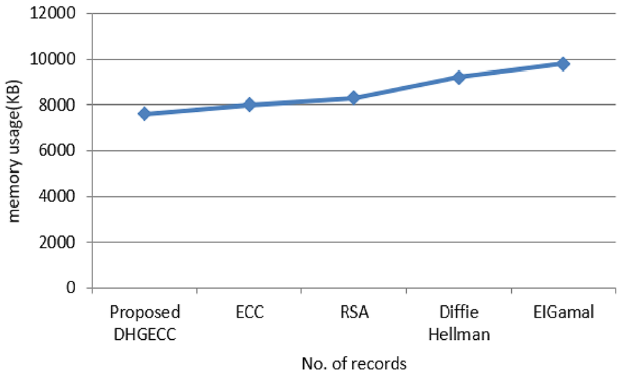


Fig. 10 Memory usage on Encryption

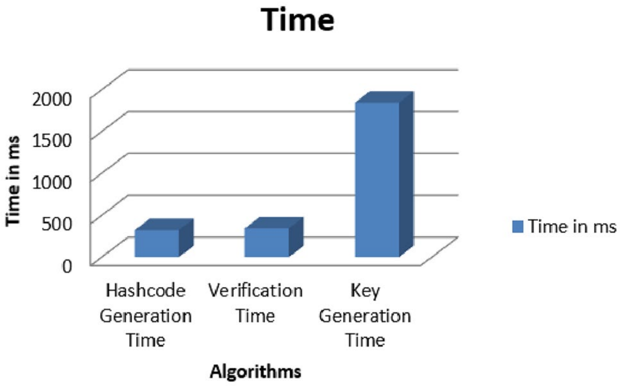


Fig. 11 Performance measure in time

system allow encrypted data based on their role. If not, the process will be declined.

From Fig. 12 described the proposed technique accomplished the performances of correlation coefficient. That is demonstrates the effectual performances of the proposed work in a proficient manner.

Subsequently from all figures under result section demonstrated the proficiency of the proposed work in an effectual manner. Hence, with the accomplishment of performances such as less time complexity of the system with greater more security and memory levels.

5 Conclusion

The importance of applications and IoT hardware is rising in modern society. The effectiveness and productivity of industrial infrastructures are now being increased through analytics and data processing enabled by IoT. Using Diffie Hellman Galois—Elliptic-curve cryptography (DHG-ECC), IoT data will be detected and encrypted. The Pearson Correlation Coefficient based Sand Cat Optimisation Algorithm (PCC-SCOA) will be used to choose the best features. The Digit Folding–Streebog Hashing algorithm will be used to merge and hashcode the chosen best features. The resource requester (a doctor or nurse) uses the Combined Linear Congruential Generator-Digital Signature Algorithm (CLCG-DSA) to send the role request. The following resource requester will contrast the hashed access policy with the blockchain. Although the proposed work is compared in the best manner, the entire study and discussions demonstrate that the suggested work performs better, with more security and accuracy, and takes less time to accomplish. Future work will be enhanced in terms of data load and network issues with the aid of cutting-edge deep learning techniques. The framework that has been proposed should also be used for further IoT application scenarios. Further research will also involve conducting comprehensive pilot studies and real-world implementations to verify the framework's functionality and evaluate its effects on healthcare systems in real-world scenarios. This will assist in locating possible obstacles and areas in need of development.

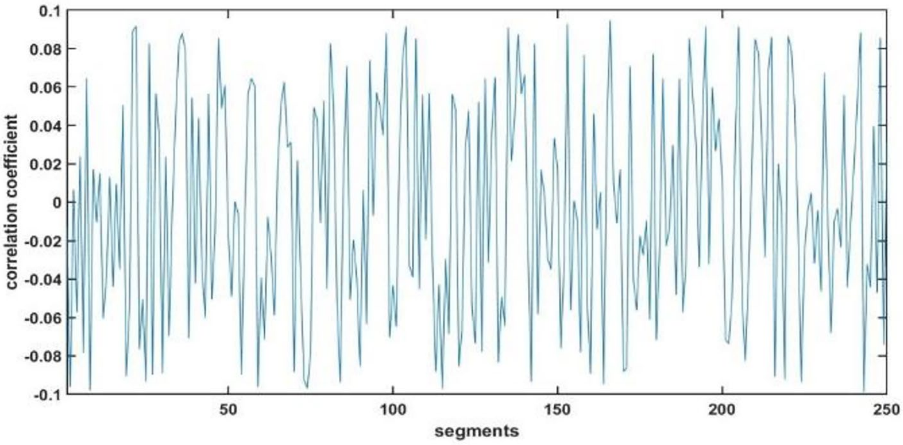


Fig. 12 Perfromance of proposed correlation coefficient

Availability of data and material The authors do not provide supplementary data and material

Declarations

Conflict of Interest The authors declare that they have no potential conflict of interest.

Statement of Animal and Human Rights All applicable institutional and/or national guidelines for the care and use of animals were followed.

Informed Consent For this type of analysis formal consent is not needed.

References

Aazam M, Zeadally S, Harras KA (2020) Health fog for smart healthcare. IEEE Consum Electron Maga 9(2):96–102

Akhter MH, Kazi T, Ixion C, Saadman S, Mohammad MK, Nawal A, Abdulmajeed A, Sami B (2022) Electronic health record monitoring system and data security using blockchain technology. Secur Commun Netw 2022:1–15

Ali F, El-Sappagh S, Islam SR, Kwak D, Ali A, Imran M, Kwak K-S (2020) A smart healthcare monitoring system for heart disease prediction based on ensemble deep learning and feature fusion. Inf Fusion 63:208–222

Ali F, El-Sappagh S, Islam SR, Ali A, Attique M, Imran M, Kwak KS (2021) An intelligent healthcare monitoring framework using wearable sensors and social networking data. Fut Gen Comput Syst 114:23–43

Awais M, Raza M, Ali K, Ali Z, Irfan M, Chughtai O, Khan I, Kim S, Ur Rehman M (2019) An internet of things based bedegress alerting paradigm using wearable sensors in elderly care environment. Sensors 19(11):2498

Chauhan N, Rajendra KD (2022) A secure design of the healthcare IoT system using blockchain technology. In: 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 704–709. IEEE

Gholamhosseini L, Sadoughi F, Ahmadi H, Safaei A (2019) Health internet of things: strengths, weakness, opportunity, and threats. In: 2019 5th International Conference on Web Research (ICWR). 287–296

Griggs KN, Ossipova O, Kohlios CP et al (2018) Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J Med Syst 42(7):130

Haque AKMB, Bhushan B, Dhiman G (2022) Conceptualizing smart city applications: requirements, architecture, security issues, and emerging trends. Expert Syst 39(5):e12753

Hasnida A, Maarten OK, Elizabeth P (2021) Challenges in maintaining medicine quality while aiming for universal health coverage: a qualitative analysis from Indonesia. BMJ Global Health 6(Suppl 3):e003663

Honar Pajooh H, Rashid M, Alam F, Demidenko S (2021) Multi-layer blockchain-based security architecture for internet of things. Sensors. 21(3):772

Jaigirdar FT, Rudolph C, Bain C (2019) Can i trust the data i see? A physician's concern on medical data in iot health architectures. In: Proceedings of the Australasian Computer Science Week Multiconference, pp 1–10

Jiang L, Chen L, Giannetsos T, Luo B, Liang K, Han J (2019) Toward practical privacy-preserving processing over encrypted data in iot: an assistive healthcare use case. IEEE Intern Things J 6(6):10177–10190

Kaur P, Kumar R, Kumar M (2019) A healthcare monitoring system using random forest and internet of things (IoT). Multimed Tools Applm 78(14):19905–19916

Khalaf OI, Muttashar Abdulsahib G (2021) Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks. Peer-to-Peer Netw Appl 14(5):2858–2873

Le NB, Lydia El, Elhoseny M, Pustokhina I, Pustokhin DA, Selim MM, Nguyen GN, Shankar K (2020) Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. Comput Mater Contin 65(1):87–107

Leng J, Yan D, Liu Q, Xu K, Zhao JL, Shi R et al (2019) ManuChain: combining permissioned blockchain with a holistic optimization model as bi-level intelligence for smart manufacturing. IEEE Trans Syst Man Cybern Syst 50(1):182–192

Mahajan HB, Ameer SR, Aparna A, Nilesh U, Sarita DD, Pravin RF, Ahmed A, Bilal A (2023) Integration of Healthcare 40 and blockchain into secure cloud-based electronic health records systems. Appl Nanosci 13(3):2329–2342

Mohana M, Deotare VV, Ninu Preetha NS, Brammya G (2023) An adaptive elliptical curve cryptography-Rivest–Shamir–Adleman-based encryption for IoT healthcare security model with blockchain technology. J Mech Med Biol. https://doi.org/10.1142/S0219519423500689

Nguyen DC, Pathirana PN, Ding M, Seneviratne A (2021) Secure computation offloading in blockchain-based IoT networks with deep reinforcement learning. IEEE Trans Netw Sci Eng 8(4):3192–3208

Ray PP, Dash D, Salah K, Kumar N (2020) Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases. IEEE Syst J 15(1):85–94

Sadiku MNO, Eze KG, Musa SM (2018) Block chain technology in healthcare. Int J Adv Sci Res Eng 4(5):154–159

Saxena S, Bhushan B, Ahad MA (2021) Blockchain based solutions to secure IoT: background, integration trends and a way forward. J Netw Comput Appl 181:103050

Shynu PG, Menon VG, Kumar RL, Kadry S, Nam Y (2021) Blockchain-based secure healthcare application for diabetic-cardio disease prediction in fog computing. IEEE Access 9:45706–45720

Sicari S, Rizzardi A, Coen-Porisini A (2020) 5G in the internet of things era: an overview on security and privacy challenges. Comput Netw 179:107345

Tao H, Bhuiyan MZA, Abdalla AN et al (2018) Secured data collection with hardware-based ciphers for Iot-based healthcare. IEEE Intern Things J 6(1):410–420

Yaqoob I, Salah K, Jayaraman R, Al-Hammadi Y (2022) Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput Appl 34(14):11475–11490

Yun J, Goh Y, Chung JM (2020) DQN-based optimization framework for secure sharded blockchain systems. IEEE Internet Things J 8(2):708–722

Zhu H, Wu CK, Koo CH, Tsang YT, Liu Y, Chi HR, Tsang K-F (2019) Smart healthcare in the era of internet-of-things. IEEE Consum Electron Maga 8(5):26–30

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.