Wireless Personal Communications (2023) 130:1549–1574
https://doi.org/10.1007/s11277-023-10344-0

Design and Development of Consensus Activation Function Enabled Neural Network-Based Smart Healthcare Using BIoT

Ilyas Benkhaddra[1] · Abhishek Kumar[2] · Mohamed Ali Setitra[3] · Lei Hang[1]

Accepted: 25 February 2023 / Published online: 20 March 2023

Abstract
In the healthcare region, Internet of Things (IoT) plays a major role in various fields and is developed as a common technique. An enormous amount of data is collected from various sensing equipment owing to the increasing demand for IoT. There occur a few challenges in the designing and developing of analyzing the huge amount of data resource limitations, absence of suitable training data, centralized architecture, privacy, and security. These issues are resolved by incorporating blockchain technology, they provide a decentralized mechanism and also ensure safe transmission of data. Blockchain technology majorly assists the caretaker to reveal the encrypted genetic codes by ensuring the security level for secure data transfer and enabling the secure transmission of patient electronic health records. The smart doctor has the accessibility to decrypt the data which is in encrypted form and after verifying the condition of the patient, the report is securely transmitted to the hospital cloud with the same encryption process. Only the relevant features are selected and are delivered to the optimized neural network with the consensus activation function. The neural network classifier performance is enhanced by the utilization of smart echolocation optimization in the developed method. The consensus activation function majorly helps to capture only the significant features for further training the model and which improves the classification accuracy. The trained model is compared with the test data to predict the disease affected the patient in the n number of hospitals.

Keywords Optimization · Neural network · Consensus activation function · Smart healthcare · Blockchain · IoT

✉ Ilyas Benkhaddra
benkhaddra.ilyas@hotmail.com

[1] School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China

[2] Department of Computer Science and Engineering, Chandigarh University, Mohali, Punjab, India

[3] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

1 Introduction

IoT has developed as a critical technology in today's society, and the usage of IoT in various applications had led to the uncontrollable network traffic [1]. The sensing layer, is concerned with sensors, the Network layer, is concerned with communications within gateways and IoT devices, Application layer, is concerned with processing the data and interaction between users and service providers [2, 3]. Blockchain is the emerging technology that might be applied to IoT healthcare systems to improve privacy and security [4, 5]. Many developers have been inspired by blockchain architecture to create privacy-preserving e-Health modules [6]. Because of blockchain's immutability, e-health data is protected to ensure data integrity and privacy [7–11]. Because of its decentralized structure, blockchain could be utilized to establish a certain level of security without the need for a third party [5, 12]. To a large extent, blockchain technologies meet the security requirements of the Internet of Things. The important properties of blockchain include integrity, decentralization, and anonymity, which boost the integrity of IoT applications while correspondingly improving IoT protection [13, 14]. In addition, blockchain technology is being employed to provide various cryptographic functions at the network's edge [15]. To protect the Cloud-IoT environment, decentralized scheme is being developed.

Authentication, encryption, and data retrieval are all important aspects of the DeBlock-Sec method [16]. The potentiality relies in encrypting the data before storing at the cloud servers such that when the security mechanism fails, the attackers can only perceive the data in its encrypted form. Moreover, for maintaining the data security, the encrypted data is managed at the source and decryption for the authorized users is based on the secret keys [1]. Encryption is another strong data security method since it ensures data secrecy and integrity. Sensitive data might be vulnerable to numerous types of attacks if there isn't an appropriate security mechanism in place. To accomplish protected communication in an IoT network, data privacy and access controls are required [17–19]. EHR data sources can be stored in a decentralized and safe manner at local blockchain nodes. Data confidentiality can be obtained using encryption methods, data integrity can be achieved by blockchain hash values, and data availability can be achieved more easily than in current healthcaremethods [5, 20]. In addition, to attain security, a better efficient hash value encrypted approach is required. As a result, a novel DL-based safe blockchain method for IoT-based healthcare diagnosing systems is urgently needed [6].

Several cryptographic primitives have been widely used to offer data security, including Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), Rivest Shamir Adleman (RSA), and so on [21]. To ensure data security, symmetric encryption such as AES (Advanced Encryption Standard) is utilized. For decryption and encryption, symmetric encryption algorithms may utilize a single key.For decryption reasons, the encrypted key must be provided to the miner or validator [3]. Access control techniques and Attribute-based encryption have also received a lot of exposure [22]. The attribute-based algorithms generate signatures, access policies, and ciphertext based on the qualities of numerous users. Location, passwords, User ID, and other attributes are examples of available attributes.A brief signature scheme and hash algorithms are used to verify data integrity [16, 23, 24]. Identity-Based Encryption (IBE) is a lightweight encryption system that enables a large number of users, simple key management, and adaptable key applications. For electronic contracts, it provides privacy protection, digital signatures, and identity identification [25]. Homomorphic encryption [26], which permits calculations on encrypted data, is a capable field. Homomorphic encryption, on the other hand, is still in its early stages of

development. IBE has been shown to reduce the difficulty in computation when compared with different Asymmetric encryptiontechniques [3].

In this research, the major contributions to developing the smart healthcare and improving the medical quality of service are as follows,

- The constancy and reliability essential level for the distributed healthcare monitoring system is achieved by designing the optimized neural network for ensuring accurate and quality medical services to the patients.
- By the utilization of the consensus activation function-based optimized neural network, the performance of classification is greatly improved. The consensus-based activation function eliminates the sensitivity related to identifying the contradictory examples with minor concerns and also the unwanted input signals are also completely reduced for an individual sample.
- The smart echolocation optimization-based CAF enabled neural network identifies the hyperparameters of the classifier and only the relevant features are selected from the provided dataset to attain better performance.

The structure of the paper from Sect. 2 is organized as follows. The review of the various research-based on smart healthcare is exposed in Sect. 2 with their merits, demerits, and the evolved challenges. Section 3 showed the system model of distributed Healthcare system, Sect. 4 reveals the patient monitoring system using Artificial Intelligence. Section 5 reveals the result and discussion of the CAF-NN-based Smart healthcare using BIoT. Consequently, Sect. 6 concludes the section with the achievements.

2 Motivation

Smart healthcare using IoT and Blockchain in various research are reviewed in this section with the evolved challenges in addition to the merits and demerits of the existing dominant methods.

2.1 Literature Review

Ray et al. [5] presented a Blockchain-IoT health record for ensuring the safe transmission of data and the developed method provides an encryption/decryption technique with the dual-layer structure of blockchain. This developed systemimproves the Electronic Health Records facility with the absence of the minor party and achieves privacy, flexibility, security, and transparency. The developed system does not apply to large-scale systems and is only suited for small-scalesystems.

Veeramakali et al. [6] developed an effective Optimal deep learning-basedsecure blockchain (ODLSB) with the three major steps safe transmission, hash value encryption, and medical analysis. The Hash value Encryption-Neighborhood Indexing Sequence reveals the best compression method for the blockchain hash values that also saves the spacing and file size. When the size of data increases then there is a probability of occurrence of a collision.

Pavithran et al. [3] introduced an IoT-enabled blockchain system for ensuring the privacy of health records transmission by the utilization of Hierarchical Identity-based Encryption. The developed encryption technique need not share the generated secret keys

to various nodes for ensuring privacy. The consolidated management of data is the major difficult task in the presented method.

Agyekum et al. [1] presented a secure identity-dependent proxy re-encryption data sharing scheme that ensures flexible authorization on the provided encrypted data and also follows the decentralization method for data sharing. In the semi-trusted disseminated environment, providing security is a risky factor in case of a collision attack.

Vishwakarmaand and Das [14] offered a secureauthentication and communication system for IoT applications with the hybridized technique of the Elliptical Curve Signature Algorithm and the Advanced Encryption Standard method. This technique improves the security of IoT-dependent applications and reduces the occurrence of numerous attacks with a lesser amount of storage overhead and calculation although not suited for an open environment.

Saurabh Shukla et al. [15] developed an intelligent Fog C-based blockchain model which increases the facilities of the cloud network and also reduces the challenge of verification, authentication, and identification. The detection rate of the developed method is highly improved for identifying the malicious attacker node in the presence of credibility however there is a limitation in scalability.

Narayanan et al. [16] presented a Decentralized Blockchain dependent Authentication protocol for providing authentication ina distributed environment. The accessing of devices and unlicensed usage are prevented with numerous identifications for a high-security level. The newly developed Decentralized Blockchain-based Authentication protocol reduces the searching time although a certain attack is not identified.

Liu et al. [19] established a Blockchain-dependent distributed access control system integrated with the mixed linear and non-linear spatiotemporal chaotic methods for encrypting the IoT information and then uploaded to the cloud. The fine-grained access control and the dynamic method are utilized to solve the issue of access control but there occurs a low rate of confirmation and throughput.

2.2 Challenges

Several challenges that arise during the research of smart healthcare and securing the storage of protection are provided as follows:

- To ensure the security and safety of the IoT-based systems, various systems and technologies are combined. The gathered data is ever the target of attackers since they play an integral role in various systems. Thus, the protection of unauthorized changes and access is an even bigger challenge [3].
- Authentication and further basic security are considered in most recent research ona unified party or server. In general, there is the possibility to break all the hypersensitive information and increase security susceptibility by cooperating as a single server. Thus, there is a lack of security [16].
- The centralized server that is the integration of IoT and blockchain with the cloud server meets numerous challenges, like the occurrence of errors in packets, the behavior of a malicious node, smart contracts weaker codes, and unlicensed IoT information. In the prevalent mechanism, the reliability of securing the IoT-based medical data is the major anxiety feature [15].
- The information is transferred through the cloud computing technique for various gadgets and users in cloud-based IoT settings. Under this situation, the various number of

users are supported and the cloud should be accessible. Inappropriately, the most prevalent research mostly concentrates on a specific number of users [16].

- The performance might be slow and the consumption of energy is high due to the encryption as well as the processing of enormous data in the IoT devices. For that purpose, the modeled algorithms should be rapid and lightweight to combine into the IoT background [16].

3 System Model of Distributed Healthcare System

Patients are increasingly receiving care from various health care locations and providers as well as it becoming more complicated in addition systematized. The medical service quality is improved by the monitoring units and the distributed electronic health organization even in inaccessible areas [27]. The new developing patient-centered model creates the medical care from clinics and hospitals to the patient's location concerning the improvement of the healthcare facility method. The constancy and reliability essential level for the distributed healthcare monitoring system is achieved by designing the optimized neural network for ensuring accurate and quality medical services to the patients.

Let us assume the IoT sensor nodes as

$$\mathrm{I}_j = \left\{\mathrm{I}_{1j}, \mathrm{I}_{2j}, \ldots \mathrm{I}_{ij}, \ldots, \mathrm{I}_{mj}\right\} \tag{1}$$

where m be the total number of sensor nodes embedded in a patient, j denotes the patient present in the provided data, and the sensors embedded in the jth patient are represented as I_j. The data collection is assisted by the IoT-WBAN sensors in the IoT sensor layer in Fig. 1.

In the sensor layer, the IoT WBAN sensors like EEG sensors, ECG sensors, Blood pressure sensors, and Motion sensors collect patient information. The EEG sensors collect information about the patient's abnormal or normal brain activity as waves by placing the sensors in the head region. The ECG sensors are generally wet sensors clipped to the region of the limb and chest of the patient that detect the electrical signals related to the heartbeat. The blood pressure sensor records the blood pressure of the patient and the pressure of the blood is measured in terms of systolic, main arterial pressure, and diastolic. Consequently, the motion sensors are utilized to capture the movement of the patient.

The recorded data is communicated between the devices and stored in the hospital server which is fed forwarded to the Cloud computing layer for data filtering and device-to-device data communication. In the process of data filtering, the unnecessary, irrelevant, and even sensitive data are eliminated to highlight the information required for the user. The device-to-device data communication can share the recorded information in the absence of network organization like the Base station and the many other access points. For device-to-device communication, the data is communicated and stored in the hospital cloud server through the energy-efficient communication path selected for data communication. The communication path selection depends on the network parameters, such as energy, network lifetime, and communication distance. Before the storage of collected data, the data should be initially encrypted.

The 'n' number of hospital patient health records is classified by the optimized Neural Network classifier with the utilization of a Decision support system. The accurate decision is made by the process of DSS including Arrhythmia classification, Diabetes monitoring, BP Estimation, Heart rate monitoring, and other disease identification. This classified

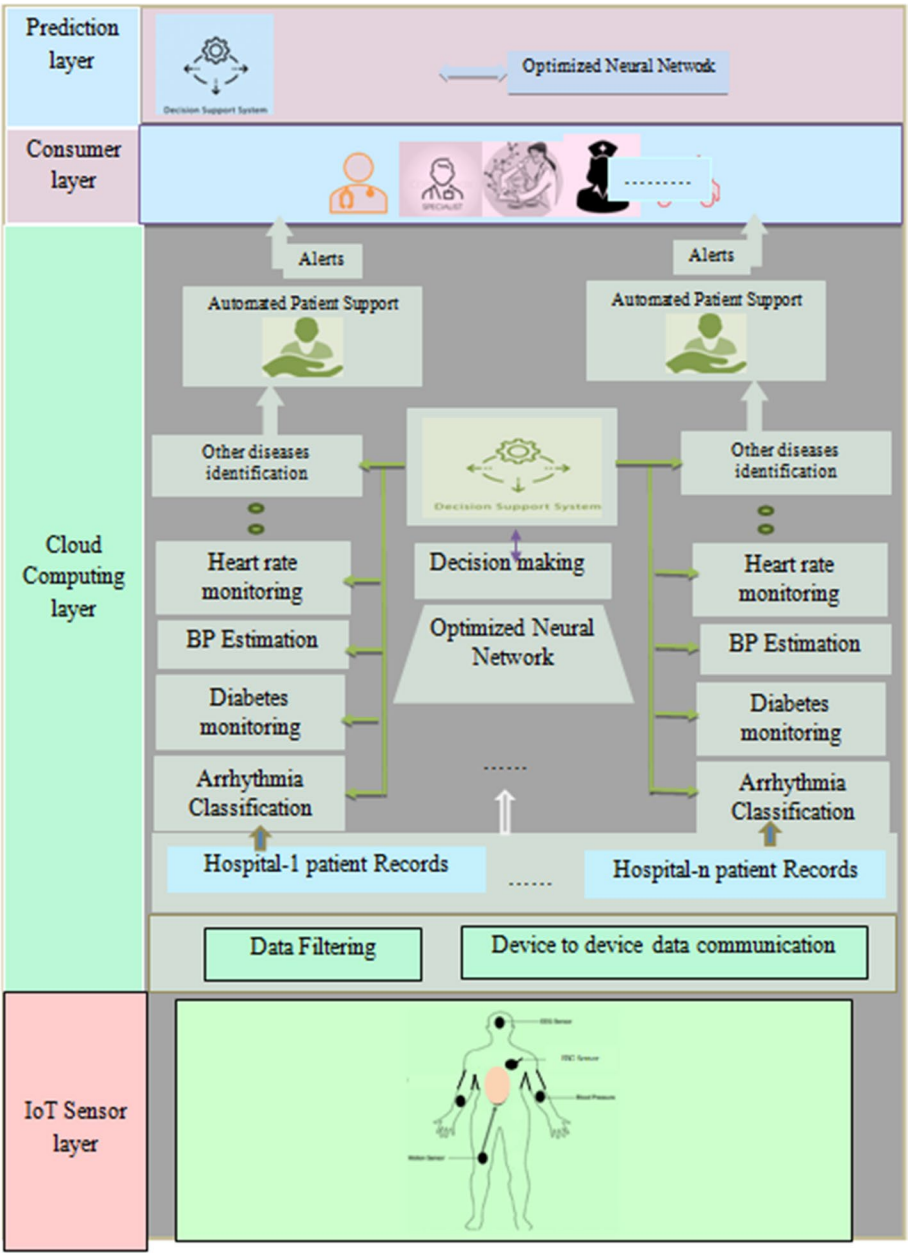

Fig. 1 The architecture of IoT-based Smart healthcare system

information is collected by the automated patient support, which assists decide the patient's health condition by making discussions with various medical-related support systems. If they identified any critical issue about the verified cases, then they generate alert signals to the attendee present in the consumer layer. The attendee may be the doctor, specialist,

lab supporter, Nurse, ambulance, and so on for taking care of the disease-affected patient. In the end, the decision support system is incorporated in the prediction layer, where the disease prediction is done, which s intimated to the entities in the consumer layer based on the risk of the disease.

The cloud system offers several advantages although there exist certain drawbacks in place of security issues such as data loss, User Account Hijacking, Changing Service providers, Lack of skill, Denial of Service attack, Interference of hackers, and Insecure APIs. The data loss in other words the data leakage problem is faced in various cloud-based systems due to the lack of reliable guidance. Then when the account with sensitive information is hijacked by the attacker, they have the entire permission for the illegal activities. The Denial of service type attack is the most emerging issue when the system is encountered with severe traffic. These issues are resolved by using the newly emerging blockchain technology to enhance the security and privacy of the stored information in addition to the decentralized structure, which applies only to legitimate users.

4 Proposed Patient Monitoring System Using Artificial Intelligence

The smart healthcare using IoT and Blockchain is demonstrated in Fig. 2. Numerous patient health records in 'n' several hospitals are securely transmitted to the smart doctor using the blockchain network. These medical health records are collected from the Pima Indians Diabetes dataset [28] and then the details are completely secured through the encryption process. In the encryption of medical records, the data they contain is changed to a code that can only be decrypted with a decryption key. Once the data is encrypted using the Advanced Encryption Standard, it is unreadable to anyone who doesn't have the decryption key. These encrypted data are fed forward to the blockchain network for enhancing security, thus in healthcare, Blockchain has a wide range of applications and functions.

Blockchain technology majorly assists the caretaker to reveal the encrypted genetic codes by ensuring the security level for secure data transfer and enabling the secure transmission of patient electronic health records. The smart doctor has the accessibility to decrypt the data which is in encrypted form and after verifying the condition of the patient, the report is securely transmitted to the hospital cloud with the same encryption process. The decrypted format of the report is further provided as input to the feature extraction process and then the extracted features are delivered to the optimized neural network (Fig. 3) with the consensus activation function. The neural network classifier performance is enhanced by the utilization of smart echolocation optimization in the developed method. The consensus activation function majorly helps to capture only the significant features for further training the model and which improves the classification accuracy. The trained model is compared with the test data to predict the disease affected the patient in the n number of hospitals.

4.1 Secured Data Occurs in the Blockchain Storage

Blockchain technology is appropriate to the process of security sharing in addition to the secure storage of the patient medical health records. Blockchain is the most successful emerging technology, thus various research institutes mainly concentrate on blockchain technology and the applications of blockchain storage are greatly improved. Thus, the blockchain majorly assists to make the decentralized mechanism and the issue of reduced work efficiency is resolved.

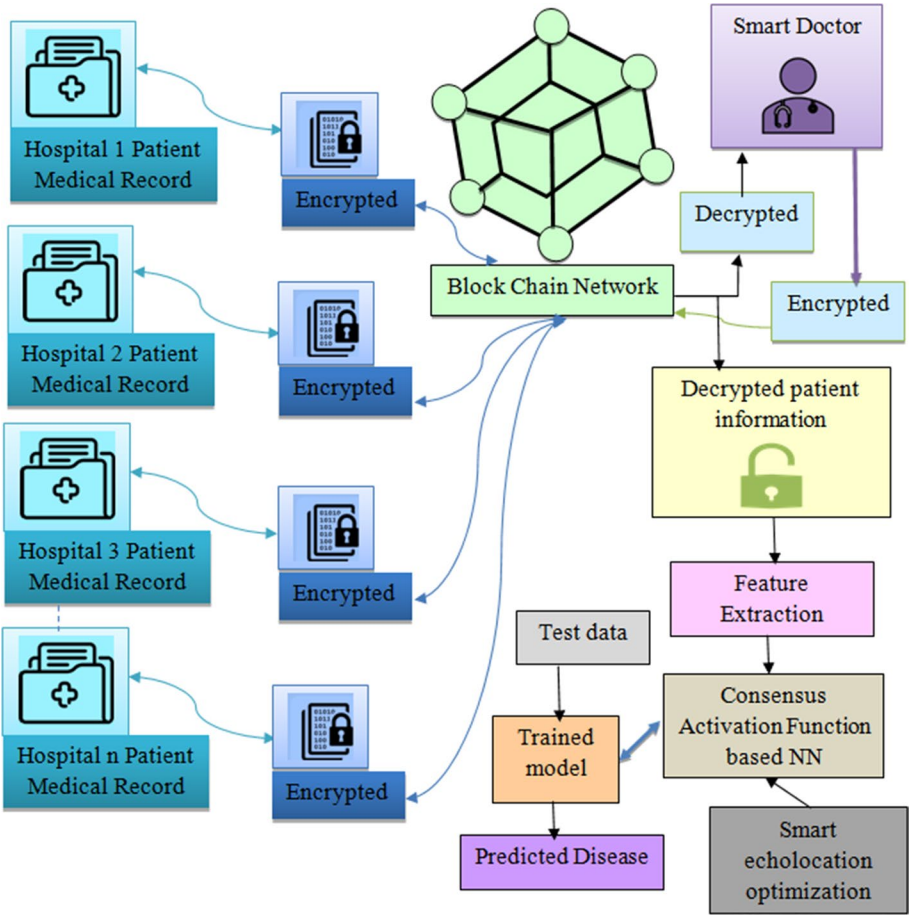

Fig. 2 Consensus activation function-NN based Smart healthcare using IoT and Blockchain

4.1.1 Data Collection

From the Pima Indians Diabetes dataset [28], the data is collected to improve the quality of medical services, the data is collected using the Sensor attached to the patient like the ECG sensor, EEG sensor, Blood Pressure sensor, and motion sensor from the IoT sensor layer. The recorded data is communicated between the devices and stored in the hospital server which is fed forwarded to the Cloud computing layer for data filtering and device-to-device data communication. In the process of data filtering, the unnecessary, irrelevant, and even sensitive data are eliminated to highlight the information required for the user.

4.1.2 Data Communication

The main aim of data communication is to transfer the significant data from one point (sender) to another point (receiver) over a complex network. The device-to-device data communication can share the recorded information in the absence of network organization

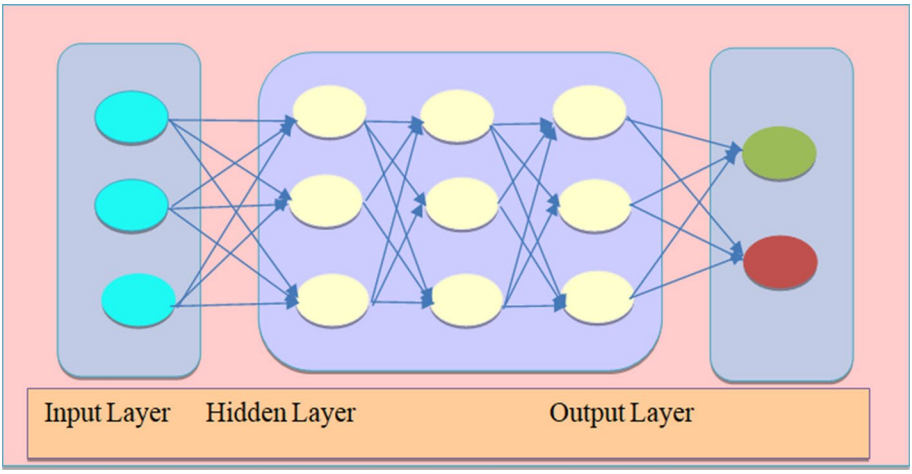

Fig. 3 The architecture of Neural Network

like the Base station and the many other access points. For device-to-device communication, the data is communicated and stored in the hospital cloud server through the energy-efficient communication path selected for data communication. The communication path selection depends on the network parameters, such as energy, network lifetime, and communication distance. Before the storage of collected data, the data should be initially encrypted.

4.1.3 Storage in Blockchain-Provides Occurs Only to Legitimate Users

The most recent developing techniques are blockchain and cloud computing due to providing unreachable facilities to various organizations. Owing to the emerging cutting-edge method and the assuring techniques, Blockchain has become a developing technology in the different fields that ensure improved privacy and security. It reduces the probability of every single operation which protects the system from fraud transactions and also provides accessible exposure for various needs. Blockchain keeps data in an assured database with a well-encrypted technique such as hashes and encryption. However, cloud computing stores the data via the internet and they are easily accessible by other users.

Here, the standard encryption technique is preferred to protect the uploaded documents in the cloud server. Then the smart doctor has the accessibility to decrypt the data which is in encrypted form and after verifying the condition of the patient, the report is securely transmitted to the hospital cloud with the same encryption process.

4.2 Decision Support System Using Optimized Neural Network in the Prediction Layer

To improve the accuracy of the optimized neural network classifier, the relevant features are selected from the input Pima Indian Diabetes Dataset. In the provided dataset, 8 different features are involved and only the required four features are selected. The selected features for the classification are the blood pressure readings of the patient, motion sensor attached patient details, EEG signals, and the ECG signals of the patient.

By the utilization of the consensus activation function-based optimized neural network, the performance of classification is greatly improved. The consensus-based activation function eliminates the sensitivity related to identifying the contradictory examples with minor concerns and also the unwanted input signals are also completely reduced for an individual sample. The optimized neural network with the activation function [29] is represented as,

$$Output = f\left(\sum (weight * input) + bias\right) \tag{2}$$

The neural network can adapt to the varying provided input and they produce optimal output which is most accurate to the input. The weights in the neural network are tuned by the smart echolocation optimization enabled with a consensus activation function. The developed CAF-NN-based smart healthcare using Blockchain-enabled IoT achieves better performance in both the encryption as well as the classification with an improved accuracy.

The parameters involved in the developed optimized neural network classifier are identified by the smart echolocation optimization by generating various solutions and analyzing the optimal fitness value for tuning the classifier is revealed in the following section.

4.3 Proposed smart Echolocation Optimization

The smart echolocation optimization involves the characteristic behavior of Bonelli's Eagle [30] and the flying foxes [31]. Bonelli's eagle is intelligent and expert in the hunting mechanism, they initially search around the search space flying in a swirling shaped manner, once the prey gets targeted then they move forward towards the prey by bending downwards vertically. Similarly, the classifier parameters are identified by initializing the process of solution generation and then the fitness of the generated solutions is estimated to optimally tune the parameters relating to obtaining the better performance. The alone performance of the Bonelli's Eagle is enhanced by integrating the additional behavior of echolocation of the flying foxes that must improve the convergence rate at the very initial stage. Thus, the behavior of the flying fox is updated to the modernizing phase of the developed smart echolocation optimization to attain optimal performance.

4.3.1 Inspiration

The Bonelli's eagle is the most famous bird for capturing the prey in the area of the northern hemisphere and this species is easily spread towards the sphere due to the interesting facts.Bonelli's eagle is usually light golden brown or dark brown with white marks on its wings. Bonelli's eagle prefers to fly at high speed over the sky in an encircling manner while discovering the prey and they utilize their strapping feet as well as the honed fingernails to get hold of the prey which survive on the ground. The most preferred prey for Bonelli's eagle are marmots, rabbits, deeps, squirrels, hares, and so on. Bonelli's eagle found their nests on large mountains and they mostly prefer at the top position of the hills. The terrains can be as high as 200 km^2 for the Bonelli's eagle and the female Bonelli's eagle produce up to 4 eggs and the incubation period is generally 6 weeks. The male Bonelli's eagle has a more dominant character than the female one during the solo-hunting and they easily shift back to the normal situation quickly as well as cleverly.

4.3.2 Mathematical Model of Smart Echolocation Optimization

Each stage of attacking the prey involves the behavior of Bonelli's eagle with the four different optimistic methods as Solution Generation, Extended discovery, Limited discovery, extended manipulation, and Limited manipulation.

4.3.2.1 Solution Generation The initial step of optimization depends on the generation of solutions for the developed populations which are expressed in Eq. (3) which is initialized based on the upper and lower bound. In each iteration, the obtained best solution is considered the optimal solution.

$$S = \begin{bmatrix} s_{1,1} & \cdots & s_{1,n} & s_{1,D-1} & s_{1,D} \\ s_{2,1} & \cdots & s_{2,n} & \cdots & s_{2,D} \\ \cdots & \cdots & s_{l,n} & \cdots & \cdots \\ \cdots & \vdots & \vdots & \vdots & \vdots \\ s_{\mathrm{P}-1,1} & \cdots & s_{\mathrm{P}-1,n} & \cdots & s_{\mathrm{P}-1,D} \\ s_{\mathrm{P},1} & \cdots & s_{\mathrm{P},n} & s_{\mathrm{P},D-1} & s_{\mathrm{P},D} \end{bmatrix} \tag{3}$$

where the present candidate solutions are represented as S and the random generation of these solutions are utilizing Eq. (4) as follows,

$$S_{\mathrm{ln}} = rand \times \left(J_n - \mathrm{K}_n\right) + \mathrm{K}_n, \quad l = 1, 2, ..., \mathrm{P} \quad n = 1, 2, \ldots, D \tag{4}$$

where the decision values are denoted as S_l of the lth solution, the total population of the generated solutions is denoted as P, and the problem dimension size is represented as D. The lower bound of n is represented as K_n, the upper bound of n is denoted as J_n, and the random number is denoted as *rand*.

The extended steps involved in the developed smart echolocation optimization are transferred to limited steps responsible for various activities and depend on the condition of t *and* T. If $\mathrm{T} \leq \left(\frac{2}{3}\right) * t$, then the extended stage will be executed or else, the limited stage is exciting.

4.3.2.2 Extended Discovery $\left(S_1\right)$ In this stage, the area of the prey is identified as $\left(S_1\right)$ and chooses the optimal attacking area by the high shoot up with a vertical bend down towards the ground. The Bonelli's eagle flies high to identify the location of the discovery space to capture the prey, which is technically expressed as follows,

$$S_1(\mathrm{T}+1) = S_{best}(\mathrm{T}) \times \left(1 - \frac{\mathrm{T}}{t}\right) + \left(S_V(\mathrm{T}) - S_{best}(\mathrm{T}) * rand\right) \tag{5}$$

where the subsequent iteration T^{th} solution is denoted as $S_1(\mathrm{T}+1)$ that is produced by the initial extended discovery method S_1. Up until Tth iteration, the optimal solution is represented as $S_{best}(\mathrm{T})$, this identifies the suitable location of the prey. The extended search of the Bonelli's eagle is controlled by the $\left(\frac{1-\mathrm{T}}{t}\right)$ over the various number of repetitions. At the end of Tth iterations, the mean value of the location for the present solutions is calculated using Eq. (6) and is expressed as $S_v(\mathrm{T})$. The random value is denoted as *rand* and the value is between 0 and 1.The present, as well as the maximum number of iterations, are denoted as T and t individually.

$$S_V(\mathrm{T}) = \frac{1}{\mathrm{P}} \sum_{l=1}^{\mathrm{P}} S_l(\mathrm{T}), \quad \forall n = 1, 2, \ldots, D \tag{6}$$

where the problem size is denoted as E based on the dimension and where the size of the population is described as P.

4.3.2.3 Limited Discovery In the second stage of limited discovery $\left(S_2\right)$, after the identification of the location of the prey the Bonelli's eagle encircles in the air to attack the target prey, make the area, and then get hold of the target prey. This behavior is similar to contour flight to some extent and begins to glide to attack the prey on the ground. During the preparation for attacking the prey, the Bonelli's eagle discovers the target prey in a limited area. This way of behaving is mathematically expressed as,

$$S_2(\mathrm{T}+1) = S_{best}(\mathrm{T}) \times Levy(\mathrm{E}) + S_G(\mathrm{T}) + (v-u)^* rand \tag{7}$$

where the solution created for the following iteration T for the second limited discovery stage $\left(S_2\right)$ is denoted as $S_2(\mathrm{T}+1)$. The levy flying behavior of Bonelli's eagle is represented as $Levy(\mathrm{E})$ based on the space of dimension E and which is estimated using the Eq. (6). The random solution within the range of [1 P] at the iteration of l. The distribution function of levy flight is also estimated using Eq. (8) as follows.

$$Levy(\mathrm{E}) = b \times \frac{q \times \sigma}{|v|^{\frac{1}{\alpha}}} \tag{8}$$

where the constant values are denoted as b which are fixed to different random numbers as $0.01, q, and\ v$ in the range of $0\ and\ 1$. Whereas, the value of σ is estimated using the Eq. (9) are as follows.

$$\sigma = \left(\frac{\Gamma(1+\alpha) \times sine\frac{(\pi\alpha)}{2}}{\Gamma\left(\frac{1+\alpha}{2}\right) \times \alpha \times 2^{\frac{(\alpha-1)}{2}}} \right) \tag{9}$$

where the constant value is represented as α which is constant at the value of 1.5. Using Eq. (7), the generated swirling shape in the discovery phase is utilizing the value of $u\ and\ v$

$$v = c \times \cos(\theta) \tag{10}$$

$$u = c \times \sin(\theta) \tag{11}$$

where,

$$c = c_1 + W \times \mathrm{E}_1 \tag{12}$$

$$\theta = -\beta \times \mathrm{E}_1 + \theta_1 \tag{13}$$

$$\theta_1 = \frac{3 \times \pi}{2} \tag{14}$$

The total number of discovering phase cycles is fixed by assuming the value of c_1 is in the range of 1 and 20, the small value of W is fixed to 0.00565, and the integer number

is denoted as E_1 towards the discovering phase which ranges from 1 to the length of the discovering space.The small value β is assumed in the range of 0.005.

4.3.2.4 Extended Manipulation After the identification of the particular location of the prey in the extended manipulation phase S_3, the Bonelli's eagle is ready for the landing stage and gets hold of the prey. In the process of preliminary attack, the Bonelli's eagle moves forward vertically to identify the location of prey. This flow of attack is generally referred to as the slow descent attack and tries to get close to the target prey known as low flight. This flow of behavior is described in Eq. (15) as follows,

$$S_3(\mathrm{T}+1) = \left(S_{best}(\mathrm{T}) - S_V(\mathrm{T})\right) \times \gamma - rand + ((J - \mathrm{K}) \times rand + \mathrm{K}) \times \delta \tag{15}$$

The solution of the third iteration of T is represented as $S_3(\mathrm{T}+1)$ which is produced by the third extended manipulation method S_3. Up until the third iteration, the optimal solution is described as $S_{best}(\mathrm{T})$. Then the average value of the present solution at T^{th} iteration is estimated using the Eq. (6). The random number is in the range of 0 and 1 which is denoted as *rand*.

4.3.2.5 Limited Manipulation In the fourth limited exploitation $\left(S_4\right)$ phase, the Bonelli's eagle moves nearer to the prey, then the attacking is done depending on the stochastic movements of the Bonelli's eagle toward the land which is defined as walking and taking hold of prey. Consequently, the Bonelli's eagle attack the prey at the final stage of the extended and the limited discovery as well as the manipulation stage which is mathematically expressed in Eq. (16) as follows.

$$S_4(\mathrm{T}+1) = \mathrm{M} \times S_{best}(\mathrm{T}) - \left(Q_1 \times S(\mathrm{T}) \times rand\right) - Q_2 \times Levy(\mathrm{E}) + rand \times Q_1 \tag{16}$$

where the solution of the fourth iteration of T is represented as $S_4(\mathrm{T}+1)$ which is produced by the third extended manipulation method S_4. Equation (17) is used to calculate the quality function M to determine the equilibrium of the discovering strategies. The different movements of the Bonelli's eagle which is utilized to attack the prey are denoted as Q_1 during the escaping stage. The flight slope of Bonelli's eagle is represented by Q_2 ranges from 2 to 0 during the escaping strategy of prey from the initial location to the final location using the Eq. (19) and where the Tth iteration present solution is denoted as $S(\mathrm{T})$.

$$\mathrm{M}(\mathrm{T}) = \mathrm{T}^{\frac{2\times rand-1}{(1-t)^2}} \tag{17}$$

$$Q_1 = 2 \times rand - 1 \tag{18}$$

$$Q_2 = 2 \times \left(1 - \frac{\mathrm{T}}{t}\right) \tag{19}$$

where at the Tth iteration, the value of the quality function is denoted as M(T), the random value is denoted as *rand* in the range of 0 and 1, and the maximum number of iterations, as well as the present iteration, are represented as *t and* T.

4.3.2.6 Modernizing Phase In this modernizing phase, the convergence rate of Bonelli's eagle is improved by integrating the flying behavior in terms of the high frequency and

velocity of the flying foxes in the extended discovery, Limited discovery, and limited manipulation phase. Thus, the updated flying fox equation is formulated in Eq. (20),

$$S_{l,flying\,fox}(\tau+1) = S_l\tau\left[1+g_l\right] + h_l\tau - g_l S^* \tag{20}$$

where the frequency of the flying foxes is denoted as g and the velocity is represented as h in the renovated stage. Integration of both the flying fox character and the Bonelli's eagle character improves the convergence rate of the developed optimization, then the equation is expressed as,

$$S_l(\mathrm{T}+1) = \frac{1}{2}\left[S_{l,flying\,fox}(\tau+1) + S_{1,Bonelli's\,eagle}(\mathrm{T}+1)\right] \tag{21}$$

Thus, the Eq. (5) in the extended discovery phase is substituted in Eq. (21) as follows,

$$S_l(\mathrm{T}+1) = \frac{1}{2}\left[\left(S_l\tau\left[1+g_l\right] + h_l\tau - g_l S^*\right) + \left(S_{best}(\mathrm{T}) \times \left(1-\frac{\mathrm{T}}{t}\right) + \left(S_V(\mathrm{T}) - S_{best}(\mathrm{T}) * rand\right)\right)\right] \tag{22}$$

where $S_l\tau$ represents the current new solution in the flying fox behavior, thus the $S_l\tau$ can be written as $S_{best}(\tau)$. Then the Eq. (22) becomes as,

$$S_l(\mathrm{T}+1) = \frac{1}{2}\left[\left(S_{best}\tau\left[1+g_l\right] + h_l\tau - g_l S^*\right) + \left(S_{best}(\mathrm{T}) \times \left(1-\frac{\mathrm{T}}{t}\right) + \left(S_V(\mathrm{T}) - S_{best}(\mathrm{T}) * rand\right)\right)\right] \tag{23}$$

$$S_l(\mathrm{T}+1) = \frac{1}{2}\left[\left(S_{best}\tau\left(g_l\right) + \tau\left(S_{best} + h_l\right) - g_l S^*\right) + S_{best}(\mathrm{T})\left[1-\frac{\mathrm{T}}{t} - rand\right] + S_v(\mathrm{T})\right] \tag{24}$$

Similarly, Eq. (7) in the limited discovery phase becomes,

$$S_l(\mathrm{T}+1) = \frac{1}{2}\left[\left(S_{best}\tau\left[1+g_l\right] + h_l\tau - g_l S^*\right) + \left(S_{best}(\mathrm{T}) \times Levy(\mathrm{E}) + S_G(\mathrm{T}) + (v-u)^* rand\right)\right] \tag{25}$$

$$S_l(\mathrm{T}+1) = \frac{1}{2}\left[\left(S_{best}g_l + \tau\left(S_{best} + h_l\right) - g_l S^*\right) + \left(S_{best}(\mathrm{T}) \times Levy(\mathrm{E}) + S_G(\mathrm{T}) + (v-u)^* rand\right)\right] \tag{26}$$

When integrating the flying fox behavior in Eq. (16) in the limited manipulation phase becomes as,

$$\begin{aligned} S_l(\mathrm{T}+1) = \frac{1}{2}\Big[&\left(S_{best}\tau\left[1+g_l\right] + h_l\tau - g_l S^*\right) + \left(\mathrm{M} \times S_{best}(\mathrm{T})\right. \\ &\left. -\left(Q_1 \times S(\mathrm{T}) \times rand\right) - Q_2 \times Levy(\mathrm{E}) + rand \times Q_1\right)\Big] \end{aligned} \tag{27}$$

$$\begin{aligned} S_l(\mathrm{T}+1) = \frac{1}{2}\Big[&\left(S_{best}g_l + \tau\left(S_{best} + h_l\right) - g_l S^*\right) \\ &+\left(\mathrm{M} \times S_{best}(\mathrm{T}) - Q_2 \times Levy(\mathrm{E}) + rand \times Q_1(1 - S(\mathrm{T}))\right)\Big] \end{aligned} \tag{28}$$

where the Eqs. (24), (26), and (28) are the modernized phase of the developed smart echolocation optimization in which the convergence rate is quickly improved.

The pseudocode ofthe developed Smart echolocation optimization is described in algorithm 1 as follows,

S. No	Algorithm 1. Smart echolocation optimization-based pseudocode
1.	Input: $'S'$ $\left(S = S_1, S_2, \ldots S_{\mathrm{P}}\right)$;
2.	Output: $S_l\left(\mathrm{T}+1\right)$;
3.	Solution generation
4.	Population P initialization of the Bonelli's eagle
5.	Parameter initialization of the Bonelli's eagle $\left(i.e., \gamma, \delta, and\ so\ on\right)$
6.	Estimate fitness value
7.	$S_{best}\left(\mathrm{T}\right)$ =Determine according to fitness value
8.	For $l = 1, 2, ..\mathrm{P}$
9.	Renovate $S_v\left(\mathrm{T}\right)$
10.	if $\mathrm{T} \le \left(\frac{2}{3}\right) * t$
11.	Extended discovery
12.	Renovate the solution using $S_1\left(\mathrm{T}+1\right) = S_{best}\left(\mathrm{T}\right) \times \left(1 - \frac{\mathrm{T}}{t}\right) + \left(S_V\left(\mathrm{T}\right) - S_{best}\left(\mathrm{T}\right) * rand\right)$
13.	else if
14.	Limited discovery
15.	if $rand \le 0.5$
16.	Extended manipulation
17.	Renovate the solution using $S_3\left(\mathrm{T}+1\right) = \left(S_{best}\left(\mathrm{T}\right) - S_V\left(\mathrm{T}\right)\right) \times \gamma - rand + \left(\left(J - \mathrm{K}\right) \times rand + \mathrm{K}\right) \times \delta$
18.	else if
19.	Limited manipulation
20.	Modernizing phase
21.	Modernizing the extended discovery phase
22.	$S_l\left(\mathrm{T}+1\right) = \frac{1}{2}\left[\left(S_{best}\tau\left(g_l\right) + \tau\left(S_{best} + h_l\right) - g_l S^*\right) + S_{best}\left(\mathrm{T}\right)\left[1 - \frac{\mathrm{T}}{t} - rand\right] + S_v\left(\mathrm{T}\right)\right]$
23.	Modernizing the Limited discovery phase
24.	$S_l\left(\mathrm{T}+1\right) = \frac{1}{2}\left[\left(S_{best} g_l + \tau\left(S_{best} + h_l\right) - g_l S^*\right) + \left(S_{best}\left(\mathrm{T}\right) \times Levy\left(\mathrm{E}\right) + S_G\left(\mathrm{T}\right) + \left(v - u\right)^* rand\right)\right]$
25.	Modernizing the Limited manipulation phase
26.	$S_l\left(\mathrm{T}+1\right) = \frac{1}{2}\left[\left(S_{best} g_l + \tau\left(S_{best} + h_l\right) - g_l S^*\right) + \left(\mathrm{M} \times S_{best}\left(\mathrm{T}\right) - Q_2 \times Levy\left(\mathrm{E}\right) + rand \times Q_1\left(1 - S\left(\mathrm{T}\right)\right)\right)\right]$
27.	End while

5 Results and Discussion

The Consensus Activation Function (CAF) enabled Neural Network (NN)-based Smart Healthcare (SH) Using Blockchain IOT with the better performance is verified in this section. The performance of the developed method is verified by considering the performance measures as Accuracy, Sensitivity, and Specificity. In this section, the developed method reveals better performance when associated with other existing dominant methods.

5.1 Preliminary Setup

The CAF-NN-based SH using BIoT is executed in the Windows 10 operating system with the MATLAB tool in 8 GB RAM to depict the effectiveness of the developed method for enhancing the quality of medical service.

5.2 Performance Measures

The performance of the established model is recognized by considering the performance measures are as follows,

5.2.1 Accuracy

The developed CAF-NN-based SH using BIoT classifier accuracy is detected by the ratio of true prediction of positive values and true prediction of negative values with the entiresamples.

$$Acc = \frac{True\ prediction\ of\ positive\ values\ and\ negative\ values}{Entire\ samples} \tag{29}$$

5.2.2 Sensitivity

The developed CAF-NN-based SH using BIoT classifier accuracy is detected by the ratio of correct prediction of values to the fraction of the sum of correct and wrong predictions.

$$Sen = \frac{Correct\ prediction\ of\ values}{Sum\ of\ correct\ and\ wrong\ predictions} \tag{30}$$

5.2.3 Specificity

The developed CAF-NN-based SH using BIoT classifier accuracy is detected by the ratio of accurate prediction of real false values to the fraction of predicting the addition of real false and wrong positive.

$$Speci = \frac{Accurate\ prediction\ of\ real\ false\ values}{Addition\ of\ real\ false\ and\ wrong\ positive\ predictions} \tag{31}$$

5.3 Dataset

The Pima Indian Diabetes dataset source is collected from the UCI machine learning repository with 8 attributes, one binary class, and 768 instances. In the dataset, the diastolic blood pressure rate in mm Hg, Diabetes pedigree function, Number of times pregnant,Body

mass index Kgm-2,Plasma glucose concentration,2-Hour serum insulin (mu U/ml), Age in years, and Triceps skinfold thickness (mm).

5.4 Comparative Methods

The Consensus Activation Function-Neural Network-based Smart Healthcare using Blockchain Internet of Things (CAF-NN based SH using BIoT) classifier is evaluated with the various existing methods such as Internet of Things enabled Blockchain Smart Healthcare using K-Nearest Neighbors (IoT Enabled Blockchain SH using KNN) [32], Internet of Things-enabled Blockchain Smart Healthcare using Support Vector Machine (IoT Enabled Blockchain SH using SVM) [33], Blockchain Internet of Things Health Records (BIoTHR) [5], Fog cloud computing-based blockchain (Fog C-based blockchain) [15], Secure Communication and Authentication Blockchain-enabled Internet of Things (SCAB-IoTA) [14], Neural Network-based Smart Healthcare using Blockchain Internet of Things (NN based SH using BIoT) [34], Bat optimization-Neural Network-based Smart Healthcare using Blockchain Internet of Things (BO-NN based SH using BIoT) [31], Aquila optimization-Neural Network-based Smart Healthcare using Blockchain Internet of Things (AO-NN based SH using BIoT) [30].

5.4.1 Comparative Analysis

The CAF-NN-based SH using BIoT classifier is compared to the various existing methods for the secure transmission and storage of medical health records. Whereas the data collected from the Pima Indian Diabetes Dataset and the performance of the optimized method are analyzed by the training percentage. The efficiency of the developed method depends on the various performance measures such as accuracy, sensitivity, and specificity depending on the various nodes as 50, 100, and 200.

5.4.1.1 Comparison Based on 50 Nodes The accuracy of the developed method and the compared existing methods are exposed in Fig. 4a). The developed CAF-NN-based SH using BIoT classifier achieves an 8.854% accuracy improvement in the training percentage 50 than the NN-based SH using BIoT classifier in predicting the disease of the patient and also the quality of service. Thus, the developed method has a 91.962% accuracy at the training percentage of 80 in the analysis of considering 50 nodes.

The sensitivity of the developed method and the compared existing methods are exposed in Fig. 4b). The developed CAF-NN-based SH using BIoT classifier achieves a 4.458% sensitivity improvement in the training percentage 60 than the BO-NN-based SH using BIoTclassifier in predicting the disease of the patient and also the quality of service. Thus, the developed method has a 95.398% sensitivity at the training percentage of 80 in the analysis of considering 50 nodes.

The specificity of the developed method and the compared existing methods are exposed in Fig. 4c). The developed CAF-NN-based SH using BIoT classifier achieves 1.772% specificity improvement in the training percentage 70 than the AO-NN-based SH using BIoT classifier in predicting the disease of the patient and also the quality of service. Thus, the developed method has a 90.246% specificity at the training percentage of 80 in the analysis of considering 50 nodes.

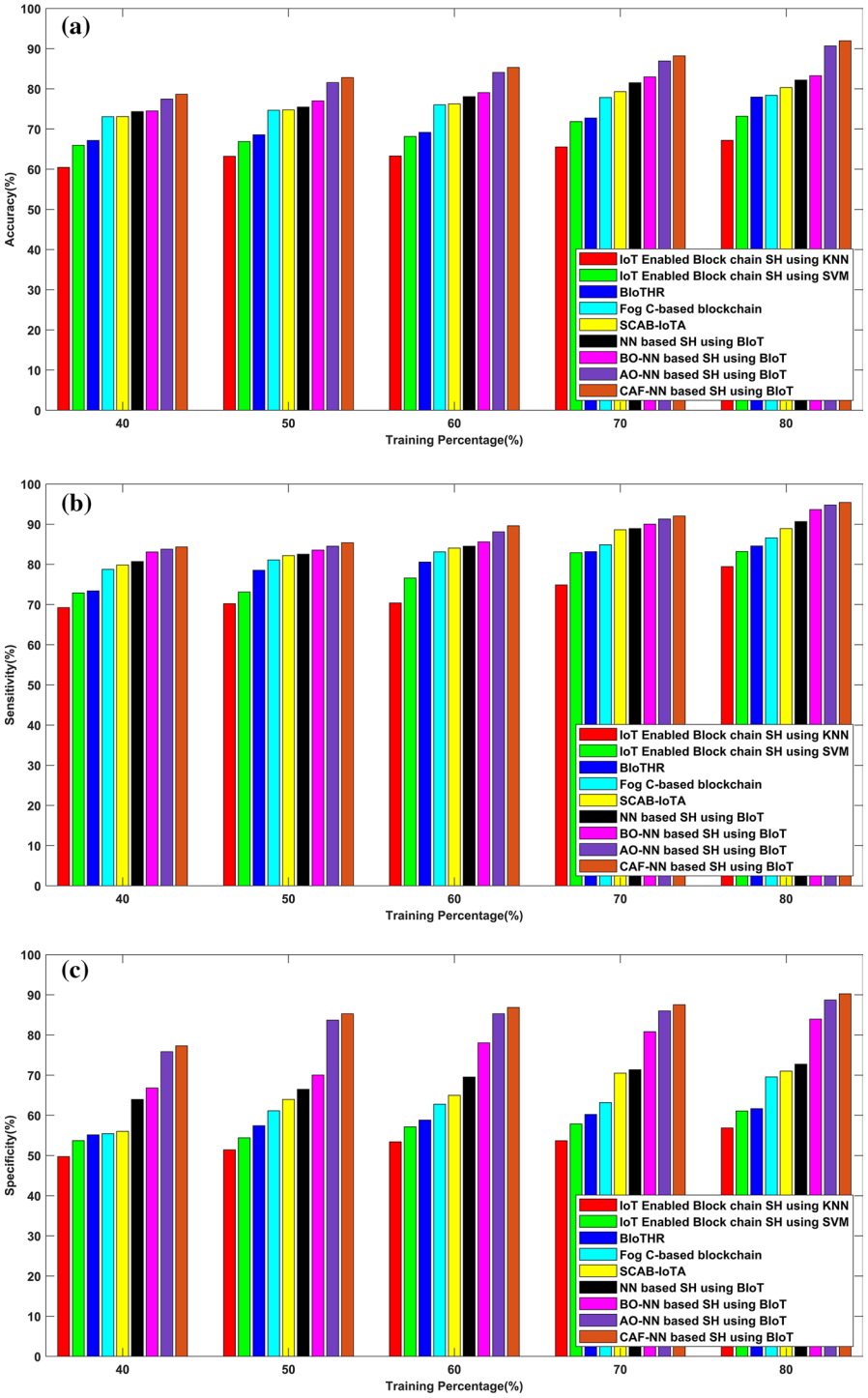

Fig. 4 Comparability analysis based on training percentage with **a** accuracy **b** sensitivity, and **c** specificity

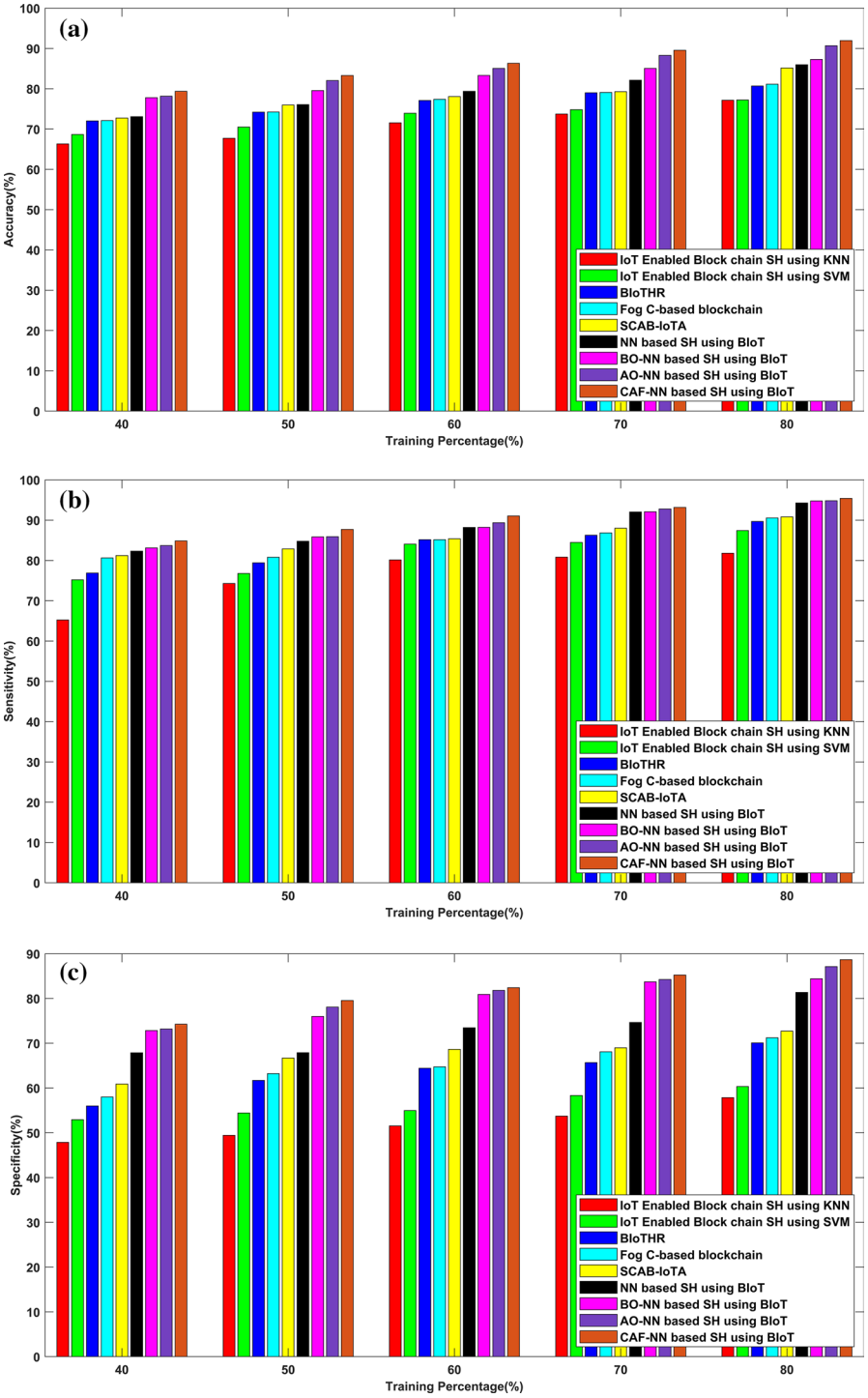

Fig. 5 Comparison of model achievements (training percentage vs. metrics) with 100 nodes, **a** accuracy, **b** sensitivity, and **c** specificity

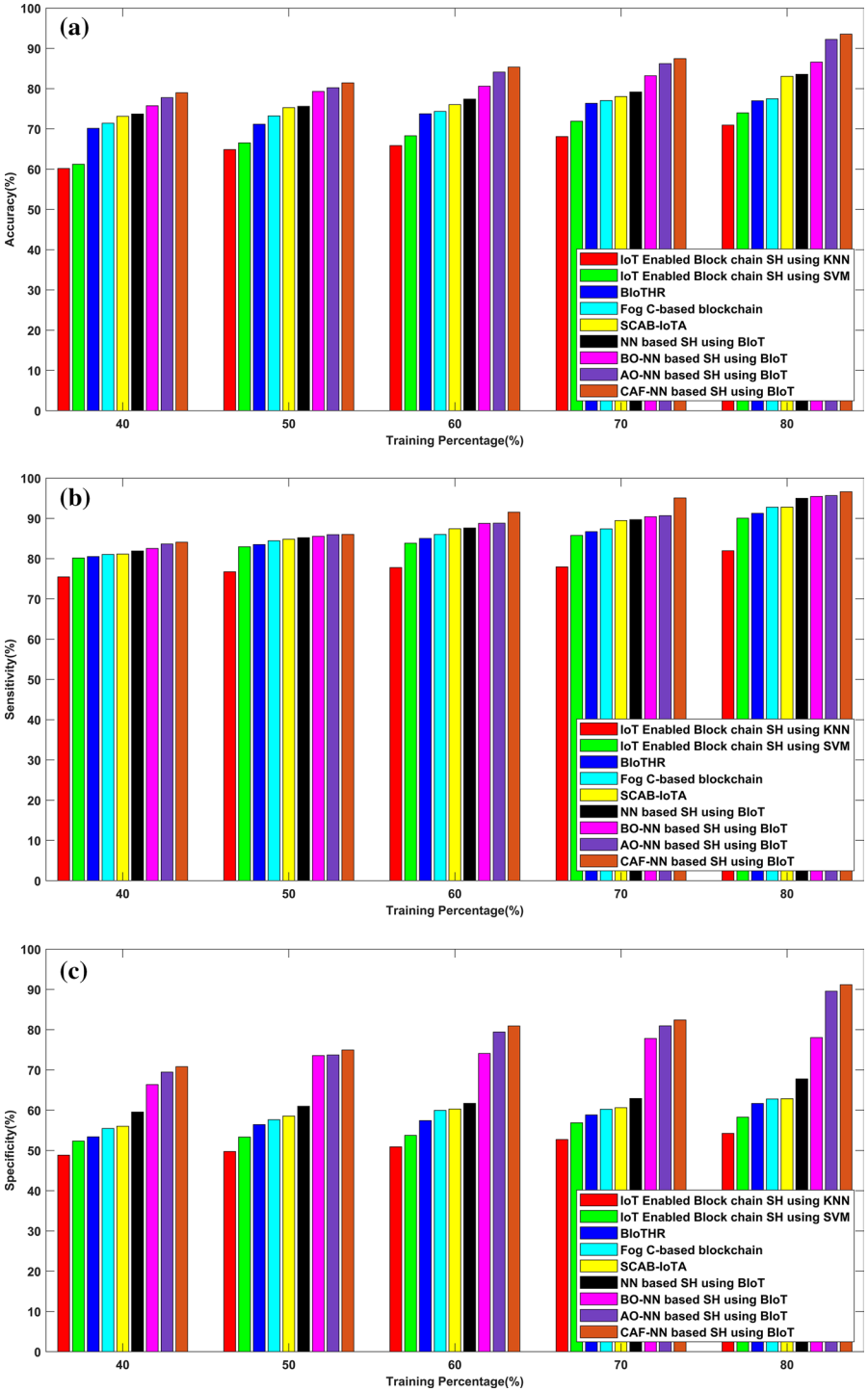

Fig. 6 Comparison of model achievements (training percentage vs. metrics) with 200 nodes, **a** accuracy, **b** sensitivity, and **c** specificity

5.4.1.2 Network with 100 Nodes and Performance Evaluation The analysis of methods when network is simulated with 100 nodes is shown in Fig. 5. The developed CAF-NN-based SH achieves 8.666% accuracy improvement at 50% training comparative with NN-SH in predicting the disease of the patient (Fig. 5a). Thus, the developed model attained 91.962% accuracy at 80% training with 100 nodes in the simulation area.

The sensitivity analysis is presented in Fig. 5b). The CAF-NN-based SH achieves a 3.141% sensitivity improvement at the training percentage 60 than the BO-NN- SH using BIoT classifier in predicting the disease of the patient and also the quality of service. Thus, the developed method acquires 95.410% sensitivity at the training percentage of 80 with 100 nodes.

The specificity of the developed method and the compared existing methods are exposed in Fig. 5c). The developed CAF-NN-based SH using BIoT classifier achieves a 1.152% specificity improvement in the training percentage 70 than the AO-NN-based SH using BIoT classifier in predicting the disease of the patient and also the quality of service. Thus, the developed method has an 88.674% specificity at the training percentage of 80 in the analysis of considering 100 nodes.

5.4.1.3 Network with 200 Nodes and Achievements of the Classification Model The performance with the network of 200 nodes is demonstrated in Fig. 6a). The developed CAF-NN-based SH using BIoT classifier achieves a 7.144% accuracy improvement in the training percentage 50 than the NN-based SH using BIoT classifier in predicting the disease of the patient and also the quality of service. Thus, the developed method attains 93.535% accuracy at the training percentage of 80 with 200 nodes.

The sensitivity of the developed method and the compared existing methods are exposed in Fig. 6b). The CAF-NN-based SH in BIoT shows 3.042% improvement comparing with BO-NN-based SH at 60% training. Thus, the developed method attained 96.615% sensitivity at 80% with 200 nodes in network.

The specificity of the methods is shown in Fig. 6c). The developed CAF-NN-based SH using BIoT classifier achieves a 1.773% specificity improvement in the training percentage 70 than the AO-NN-based SH using BIoT classifier in predicting the disease of the patient and also the quality of service. Thus, the developed method attained 91.143% specificity at 80% of training with 200 nodes in the network.

5.5 Comparative Discussion

The CAF-NN model achieves better performance in securing the data in secure transmission as well as the quality of service when compared to the previously developed methods related to blockchain and IoT. The improved performance of the CAF-NN model in disease identification in the BIoT applications is demonstrated in the Table 1.

Table 1 Achievements of the CAF-NN model in BIoT applications

Methods	Pima Indians diabetes dataset								
	Training percentage 80								
	50 nodes			100 nodes			200 nodes		
	Accuracy %	Sensitivity %	Specificity %	Accuracy %	Sensitivity %	Specificity %	Accuracy %	Sensitivity %	Specificity %
IoT Enabled Blockchain SH using KNN	67.176	79.442	56.860	77.154	81.799	57.870	70.943	81.944	54.236
IoT Enabled Blockchain SH using SVM	73.171	83.190	61.093	77.221	87.424	60.347	73.992	90.040	58.271
BIoTHR	77.950	84.583	61.652	80.697	89.698	70.096	76.991	91.272	61.652
Fog C-based blockchain	78.392	86.601	69.557	81.128	90.544	71.235	77.496	92.774	62.769
SCAB-IoTA	80.299	88.899	70.985	85.157	90.814	72.730	83.063	92.808	62.841
NN based SH using BIoT	82.188	90.663	72.749	85.974	94.258	81.367	83.560	94.999	67.758
BO-NN based SH using BIoT	83.262	93.632	83.937	87.292	94.769	84.433	86.588	95.449	78.045
AO-NN based SH using BIoT	90.673	94.776	88.682	90.673	94.834	87.137	92.224	95.644	89.563
CAF-NN based SH using BIoT	91.962	95.398	90.246	91.962	95.410	88.674	93.535	96.615	91.143

6 Conclusion

In this research, the CAF-NN based SH using BIoT enhance the quality of medical services and the secure transmission of data in the network system. Initially, the health details of the patient are gathered from the various affixed IoT senor layers, then the collected data proceeded to the device-to-device data communication. The communication path selection depends on the network parameters, such as energy, network lifetime, and communication distance. Before the storage of collected data, the data should be initially encrypted. Blockchain has become a developing technology in the different fields that ensure improved privacy and security. It reduces the probability of every single operation which protects the system from fraud transactions and also provides accessible exposure for various needs. Blockchain keeps data in an assured database with a well-encrypted technique such as hashes and encryption. The consensus-based activation function eliminates the sensitivity related to identifying the contradictory examples with minor concerns and also the unwanted input signals are also completely reduced for an individual sample. The parameters of the developed optimized neural network classifier are identified by the smart echolocation optimization by generating various solutions and analyzing the optimal fitness value for tuning the classifier.

Author contributions Benkhaddra Ilyas conceived the presented idea and designed the analysis. Also, he carried out the experiment and wrote the manuscript with support from Abhishek Kumar, Setitra Mohamed Ali and Hang Lei. Abhishek Kumar co-supervised the whole work and supervision done by Lei Hang. All authors discussed the results and contributed to the final manuscript. All authors read and approved the final manuscript.

Declarations

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

References

1. Agyekum, K. O. B. O., Xia, Q., Sifah, E. B., Cobblah, C. N. A., Xia, H., Gao, J. (2021). A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain. *IEEE Systems Journal*.
2. Gu, L., Wang, J., & Sun, B. (2014). Trust management mechanism for Internet of Things. *China Communications, 11*(2), 148–156.
3. Pavithran, D., Al-Karaki, J. N., & Shaalan, K. (2021). Edge-based blockchain architecture for event-driven iot using hierarchical identity based encryption. *Information Processing & Management, 58*(3), 102528.
4. Mishra, P., Puthal, D., Tiwary, M., & Mohanty, S. P. (2019). Software defined IoT systems: Properties, state of the art, and future research. *IEEE Wireless Communication Magazine, 26*(6), 64–71.
5. Ray, P. P., Chowhan, B., Kumar, N., & Almogren, A. (2021). Biothr: Electronic health record servicing scheme in IoT-blockchain ecosystem. *IEEE Internet of Things Journal, 8*(13), 10857–10872.
6. Veeramakali, T., Siva, R., Sivakumar, B., Senthil Mahesh, P. C., & Krishnaraj, N. (2021). An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. *The Journal of Supercomputing, 77*(9), 9576–9596.
7. Puthal, D., & Mohanty, S. P. (2019). Proof of authentication: IoT-friendly blockchains. *IEEE Potentials Mag., 38*(1), 26–29.
8. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, C. (2018). To blockchain or not to blockchain: That is the question. *IT Professional, 20*(2), 62–74.

9. Li, J., Ji, Y., Choo, K.-K.R., & Hogrefe, D. (2019). CL-CPPA: Certificate-less conditional privacy-preserving authentication protocol for the Internet of Vehicles. *IEEE Internet of Things Journal, 6*(6), 10332–10343.
10. Ilyas, B., Kumar, A., Setitra, M. A., Bensalem, Z. A., Lei, H. (2023) Prevention of DDoS attacks using an optimized deep learning approach in blockchain technology. *Transactions On Emerging Telecommunication and Technologies*.
11. Ilyas, B., Kumar, A., Bensalem, Z. E. A., Hang, L. (2023). Secure transmission of secret data using optimization based embedding techniques in Blockchain. *Expert Systems with Applications*, 211.
12. Roy, S. S., Puthal, D., Sharma, S., Mohanty, S. P., & Zomaya, A. Y. (2018). Building a sustainable Internet of Things: Energy-efficient routing using low-power sensors will meet the need. *IEEE Consumer Electronics Magazine, 7*(2), 42–49.
13. Lau, C. H., Alan, K.-H. Y., Yan, F. (2018). Blockchain-based authentication in IoT networks. In *Proceedings of 2018 IEEE conference on dependable and secure computing, DSC*, IEEE, pp. 1–8.
14. Vishwakarma, L., & Das, D. (2021). SCAB-IoTA: Secure communication and authentication for IoT applications using blockchain. *Journal of Parallel and Distributed Computing, 154*, 94–105.
15. Shukla, S., Thakur, S., Hussain, S., Breslin, J. G., & Jameel, S. M. (2021). Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model. *Internet of Things, 15*, 100422.
16. Narayanan, U., Paul, V., & Joseph, S. (2022). Decentralized blockchain based authentication for secure data sharing in Cloud-IoT. *Journal of Ambient Intelligence and Humanized Computing, 13*(2), 769–787.
17. Pal, S., Rabehaja, T., Hill, A., Hitchens, M., & Varadharajan, V. (2019). On the integration of blockchain to the internet of things for enabling access right delegation. *IEEE Internet of Things Journal, 7*(4), 2630–2639.
18. Xia, Q., Sifah, E. B., Agyekum, K.O.-B.O., Xia, H., Acheampong, K. N., Smahi, A., Gao, J., Du, X., & Guizani, M. (2019). Secured fine-grained selective access to outsourced cloud data in IoT environments. *IEEE Internet of Things Journal, 6*(6), 10749–10762.
19. Liu, Y., Zhang, J., & Zhan, J. (2021). Privacy protection for fog computing and the internet of things data based on blockchain. *Cluster Computing, 24*(2), 1331–1345.
20. Al-Jaroodi, J., & Mohamed, N. (2019). Blockchain in industries: A survey. *IEEE Access, 7*, 36500–36515.
21. Guan, Z., et al. (2017). Achieving efficient and secure data acquisition for cloud-supported internet of things in smart grid. *IEEE Internet of Things Journal, 4*(6), 1934–1944. https://doi.org/10.1109/JIOT.2017.2690522
22. Cui, H., et al. (2018). Achieving scalable access control over encrypted data for edge computing networks. *IEEE Access, 6*, 30049–30059.
23. Efficient and privacy-preserving online fingerprint authentication scheme over outsourced data. *IEEE Transactions on Cloud Computing*, *6*(1):1–11.
24. Integrity verification for digital Holy Quran verses using cryptographic hash function and compression. *Journal of King Saud University-Computer and Information Sciences 32*(1), 24–34.
25. Research on application of blockchain and identity-based cryptography. *IOP Conference Series Earth and Environmental Science, 252*(4).
26. Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, 169–178.
27. Rajavel, R., Ravichandran, S. K., Harimoorthy, K., Nagappan, P., & Gobichettipalayam, K. R. (2022). IoT-based smart healthcare video surveillance system using edge computing. *Journal of Ambient Intelligence and Humanized Computing, 13*(6), 1–13.
28. Pima Indians Diabetes dataset. https://www.kaggle.com/datasets/uciml/pima-indians-diabetes-database/discussion.
29. Benardos, P. G., & Vosniakos, G.-C. (2007). Optimizing feedforward artificial neural network architecture. *Engineering Applications of Artificial Intelligence, 20*(3), 365–382.
30. Abualigah, L., Yousri, D., Abd Elaziz, M., Ewees, A. A., Al-Qaness, M. A., & Gandomi, A. H. (2021). Aquila optimizer: A novel meta-heuristic optimization algorithm. *Computers & Industrial Engineering, 157*, 107250.
31. Yang, X.S., & Gandomi, A. H. (2012). Bat algorithm: A novel approach for global engineering optimization. *Engineering Computations*.

32. Thilakarathne, N. N., Kagita, M. K., Lanka, D., Ahmad, H. (2020). Smart grid: a survey of architectural elements, machine learning and deep learning applications and future directions. arXiv preprint arXiv:2010.08094.
33. Jeong, S., Shen, J. H., Ahn, B. (2021). A study on smart healthcare monitoring using IoT based on blockchain. *Wireless Communications and Mobile Computing*.
34. Awan, K. A., Din, I. U., Almogren, A., Almajed, H., Mohiuddin, I., & Guizani, M. (2020). NeuroTrust—artificial-neural-network-based intelligent trust management mechanism for large-scale internet of medical things. *IEEE Internet of Things Journal, 8*(21), 15672–15682.

Ilyas Benkhaddra received the State Engineer Diploma in Telecommunication from the Polytechnic School, Algiers, Algeria, in 2010, and the Mastery Degree in Electrical, Electronic Engineering, and Industrial Computing Sciences, and the Master degree in Radiocommunication and Reliable Electronic Systems from the University of Lorraine, Metz, France, in 2016 and 2017, respectively. He is currently a Ph.D. of the School of Information and software engineering at the University of Electronic Science and Technology of China (UESTC). His current research interests include chaos-based cryptography, reliable embedded systems based on MPSOC and NOC, IoT, and blockchain technology.

Abhishek Kumar is Doctorate in computer science from University of Madras and done M.tech in Computer Sci. & Engineering from Government engineering college Ajmer, Rajasthan Technical University, Kota India. He has total Academic teaching experience of more than 7 years with more than 80 publications in reputed, peer reviewed National and International Journals, books & Conferences. He has guided more than 20 M.Tech Projects and Thesis and guiding 2 PhD Scholar. His research area includes- Artificial intelligence, Image processing, Computer Vision, Data Mining, Machine Learning. He has been Session chair and keynote Speaker of many International conferences, webinars in India and Abroad. He has been the reviewer for IEEE and Inderscience Journal. He has authored/Co-Authored 6 books published internationally and edited 16 books (Published & ongoing with Elsevier, Wiley, IGI GLOBAL Springer, Apple Academic Press, De-Grueter and CRC etc. He has been member of various National and International professional societies in the field of engineering & research like Senior Member of IEEE, IAENG (International Association of Engineers), Associate Member of IRED (Institute of Research Engineers and Doctors), He has got Sir CV Raman National award for 2018 in young researcher and faculty Category from IJRP Group. He is Editor of Special issue in the Journal Computer materials and continua [SCI and SCOPUS.IF- 4.98] and Intelligent Automation and Soft Computing [SCI, SCOPUS, IF-1.276] Cognitive Neuro dynamics, Springer [SCI, SCOPUS, IF-3.925].

Mohamed Ali Setitra received the State Engineer Diploma in computer science and Master's degree in Networking and Distributed Systems from the University of Science and Technology Houari Boumediene (USTHB), Algiers, Algeria, in 2004 and 2016, respectively. He worked as responsible for Cybersecurity (forensic, threats intelligence, regulation), and his Master's research was on predicting DDoS attacks employed on Distributed Systems. He is currently pursuing his Ph.D. degree in Cybersecurity with the School of Computer Science and Engineering at the University of Electronic Science and Technology of China (UESTC), Chengdu/China. His research interests include improving the detection of Distributed Denial of Service (DDoS) attacks in Emerging Software Defined Networks (SDN) environments.

Lei Hang received the Ph.D. degree in computer science from the University of Electronic Science and Technology of China, China, in 1997. After graduation, he conducted research in the _elds of real-time embedded operating system, operating system security, and program verification, as a Professor with the Department of Computer Science, University of Electronic Science and Technology of China. He is currently a professor (doctoral supervisor) with the School of Information and Software Engineering, University of Electronic Science and Technology of China. His research interests include big data analytics, machine learning, and program verification