Received 17 July 2024, accepted 15 August 2024, date of publication 27 August 2024, date of current version 5 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3450796

RESEARCH ARTICLE

Blockchain-Powered Deep Learning for Internet of Things With Cloud-Assisted Secure Smart Home Networks

FAHAD F. ALRUWAILI

Department of Computer and Network Engineering, College of Computing and Information Technology, Shaqra University, Sharqa 11961, Saudi Arabia

e-mail: alruwaili@su.edu.sa

ABSTRACT Integrating Internet of Things (IoTs) devices with secure smart home networks assisted by the cloud signifies a cutting-edge and potent tool for contemporary home automation. This allows various appliances and devices in a home remotely controlled by the internet to communicate and share data. The typical smart home system depends on the cloud service or centralized server, which makes them further vulnerable to potential security breaches and single points of failure. As a decentralized nature, Blockchain (BC) distributes the control and storage of data across the network, preventing unauthorized attacks. Integrating BC technology into the protected smart home network boosts the system's dependability, safety, and privacy. In addition, machine learning (ML) and analytics offer behaviour analysis and predictive maintenance for optimized energy consumption. Finally, combining IoT with cloud-assisted security transforms homes into smart, connected ecosystems, offering convenience without integrating confidentiality or dependability. Accordingly, this study presents a BC-based Deep Learning in the Secure Smart Home Network (BPDL-SSHN) methodology in the IoT-cloud platform. In the BPDL-SSHN methodology, BC technology permits secret proficient data from the smart home network. Furthermore, the BPDL-SSHN method follows a series of processes to detect malicious activities such as Binary Fox Optimization Algorithm (BFOA) based feature selection, Attention-based Long Short-Term Memory (ALSTM)-based classification, and Harbor Seal Whiskers Optimization (HSWO)-based hyperparameter tuning. The HSWO method's design helps better the hyperparameter choice of the ALSTM method, significantly enhancing the recognition performance. The comparative outcome of the BPDL-SSHN methodology reported the proficient solution of the smart home network to detect and monitor malicious or harmful activities. The experimental outcome implied that the BPDL-SSHN methodology accomplishes a maximum accuracy performance of 98.91% over other approaches.

INDEX TERMS Internet of Things, blockchain, hyperparameter tuning, deep learning, binary fox optimization algorithm.

I. INTRODUCTION

The modern world arises with smart technologies that can function in smart homes to improve the quality of life [1]. Smart appliances are linked to sharing information, where the Smart devices are connected through the IoT. The average development rate of smart residences and their tools was over 30%, from 500 to 700 million uses annually from 2018 to 2022. Five significant features are connected to smart home safety and confidentiality to enhance the consistency of smart device data removal [2]. Authentication is the first one, which aids in validating the communication format. Authorization is the second one that confirms the access rights. Confidentiality that preserves the data privacy by permitting access to the certified consumer [3]. Integration is the fourth one, which assists in reducing data damage and upholding the data in a precise way. Availability is the last one that offers obtainable access to certified consumers

The associate editor coordinating the review of this manuscript and approving it for publication was Moussa Ayyash.

who are secure from dangers. Therefore, a smart home network is complex to safety attacks due to the many related devices. In these circumstances, a supervised technique for data analysis produced by the IoT network could be moderately beneficial [4].

BC-type methods and united cloud-like computing systems are utilized to resolve these issues. BC design contains a sequence of blocks connected and organized by easy cryptography. BC models are primarily characterized by three key concepts: decentralization, transparency, and immutability [5]. The three parts are effectual, revealing them to various digital currency techniques like embedded systems, mobile transports, and phones. Whereas the BC platform is safe and mysterious, there are a few problems with its current execution. For instance, Sybil's assaults by groups of wrong identities to deploy the group have become difficult [6]. Since regular techniques only aspect at the signs and do not function on examining for numerous precise forms, robust intrusion detection systems (IDSs) have been vital to scrutinize the conditions. RTS-DELM is an ML model employed to evaluate data. This ML platform uses an automatic data flow structure to define data flow and discover attack and intrusion forms. Generating significant and valuable systems to control the frequently developing smart BC-based uses is substantial [7].

ML is a technique that contains computers that demonstrate themselves utilizing an intelligent system. Based on a unique argument, ML is the primary use circumstance of artificial intelligence (AI). The central concept of ML is to resolve challenges without being automated [8] and enhance a genuine method that will obtain data from an input estimate and vary the outputs by utilizing arithmetical analysis. By using ML, one can develop a vast number of data and reach a decision based on realities. Integrating robust security and confidentiality factors in smart home networks is to address the convolutional security threats presented by interrelated devices within the IoT ecosystem [9]. Authorization, integration, authentication, availability, and confidentiality ensure privacy, accessibility, and data integrity for authorized users, which is significant for safeguarding against potential safety challenges and ensuring the reliable operation of smart home environments. By employing BC technology, characterized by transparency, decentralization, and immutability, these threats can be effectually reduced, improving safety measures against outbreaks such as Sybil's assaults and confirming trustworthy data management across several digital platforms [10].

This study presents a BC-based Deep Learning in the Secure Smart Home Network (BPDL-SSHN) methodology in the IoT-cloud platform. In the BPDL-SSHN methodology, BC technology permits secret proficient data from the smart home network. Furthermore, the BPDL-SSHN method follows a series of processes to detect malicious activities such as Binary Fox Optimization Algorithm (BFOA) based feature selection, Attention-based Long Short-Term Memory (ALSTM)-based classification, and Harbor Seal Whiskers Optimization (HSWO)-based hyperparameter tuning. The HSWO method's design helps better the hyperparameter choice of the ALSTM method, significantly enhancing the recognition performance. The comparative outcome of the BPDL-SSHN methodology reported the proficient solution of the smart home network to detect and monitor malicious or harmful activities. The contribution of the BPDL-SSHN method is listed below:

- The proposed BPDL-SSHN technique employs the BFOA model for feature selection, which contributes to the method's capacity to detect the most relevant features. This paves the way for enhanced classification accuracy and mitigated computational complexity.
- The ALSTM-based classification model improves the accuracy of the technique by utilizing attention mechanisms, enabling the approach to concentrate on the most informative features and make accurate classifications, enhancing the overall accomplishment.
- The integration of the HSWO model for hyperparameter tuning contributes to the efficient optimization of method parameters, paving the way to improved robustness and generalization. This enhances the technique's adaptability to diverse datasets and overall accomplishment.
- The novelty of the BPDL-SSHN method is in its novel incorporation of the BFOA for feature selection, ALSTM for classification, and HSWO for hyperparameter tuning. This overall model not only addresses the threats of feature selection, hyperparameter optimization, and classification accuracy but also portrays the adaptability of the technique and robustness in handling various datasets. The novel utilization of nature-inspired optimization models for several phases of the method sets it apart as an overall and efficient outcome for pattern detection and classification tasks, underscoring its potential for wide-ranging ML and data evaluation applications.

II. LITERATURE REVIEW

Almuqren et al. [11] developed a BC-based Secure Smart Home Network employing Gradient-Based Optimization with a Hybrid DL (BSSHN-GBOHDL) technique. This method utilizes BC technology. This model uses data preprocessing, GBO-based hyperparameter tuning, and hybrid DL (HDL) based classification. In [12], a BC-based DL method was introduced by employing smart contract-based improved proof of words (PoWs). Subsequently, a DL model with a Variational Autoencoder (VAE) method for privacy and BiLSTM in intrusion detection was developed. Nguyen et al. [13] examined the security and computational offloading issues concurrently in a multi-user MECCO model with BC. Primarily, a reliable access control method was presented employing BC. Secondarily, the model develops computational offloading issues by collectively improving the offloading solutions, utilizing innovative contracts, and distributing radio bandwidth and computational resources.

In [14], a robust architecture was introduced by employing an isolation forest (IF) method. Afterwards, the database was used for training categorization methods: quadratic discriminant analysis (QDA), KNN, SVM, and linear discriminate analysis (LDA). Additionally, an interplanetary file system (IPFS) was employed for classification. Jadav et al. [15] designed a BC and onion routing (OR) based reliable and protective architecture. An LSTM network is applied for classification. In [16], a trivial authentication method was developed. A particular server queuing architecture and authentication method is also employed. Badshah et al. [17] intended to combine IoT with BC by presenting an intermediate layer of the IoT. Consequently, an intelligent BC-assisted IoT (BIoT) architecture was developed. Additionally, numerous real-time BIoT-specific cases were emphasized and relatively analyzed.

In [18], the honeypot and BC-based intrusion detection and prevention (HB-IDP) technique is developed. Firstly, three-fold authentication was executed using the camellia encrypted algorithm (CEA), which offers secret keys. Signature-based intrusion detection was achieved through the improved IF (IIF) method. Ensemble learning systems, comprising lightweight-CNN (LCNN), general adversarial network (GAN), and multi-layer perceptron (MLP), are implemented for classification. Doe et al. [19] employed an incentive mechanism contract-theoretic approach is proposed. This technique also suggests a discrete incentive customized to the user's revenue-generating capability and contributions to funding network incentives. Reference [20] suggests a BC-based security method comprising gathering discrete datasets and establishing active and redundant miners to collect these sets. The Mayfly Optimizer (MO) method determines the miner count. Afraz et al. [21] present a model using BC-based solutions and selecting an appropriate BC platform. Dansana et al. [22] suggest a multi-step model comprising deep CNN (dCNN). The approach also implemented a Proof-of-Trust (PoT) consensus mechanism and Genetic Algorithm (GA) model-based sidechaining technique.

III. THE PROPOSED MODEL

This study presents a new BPDL-SSHN technique in the IoT-cloud environment. In the BPDL-SSHN technique, BC technology is applied, which enables the data to be collected confidentially in the smart home network. Additionally, the BPDL-SSHN method follows a series of processes to detect malicious activities, such as BFOA-based feature selection, ALSTM-based classification, and HSWO method-based hyperparameter tuning. Fig. 1 depicts the entire process of the BPDL-SSHN method.

A. BC TECHNOLOGY

In the BPDL-SSHN technique, BC technology is applied, which enables the data to be collected confidentially in the smart home network. BC technology allows users to keep records of transaction details and update them once there is a new transaction to ensure consistency [23]. BC provides high accountability and guarantees the transaction authority by keeping a register on the nodes that authenticate the transaction and distributing that register to the overall network. Due to the advances in encryption and internet technologies, it becomes possible for the user to validate the responsibility of the transaction, such that a single point of failure is removed and dependency on an authorized third party can be resolved. The advantage of constructing an intelligent machine is that it can operate and communicate over the BC.

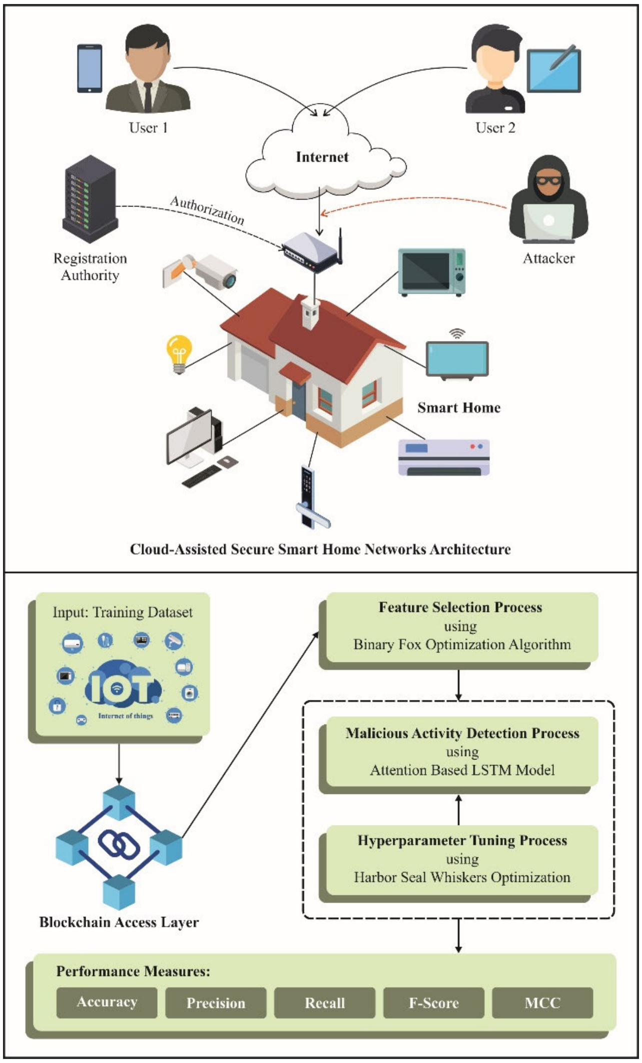
User 1
User 2
Internet
Authorization
Registration Authority
Attacker
Smart Home
Cloud-Assisted Secure Smart Home Networks Architecture
Input: Training Dataset
Internet of things
Feature Selection Process
using
Binary Fox Optimization Algorithm
Malicious Activity Detection Process
using
Attention Based LSTM Model
Hyperparameter Tuning Process
using
Harbor Seal Whiskers Optimization
Blockchain Access Layer
Performance Measures:
Accuracy
Precision
Recall
F-Score
MCC

FIGURE 1. The overall procedure of the BPDL-SSHN method.

Permanent records can be tracked as data once the data transaction occurs through multiple networks managed and owned by various organizations. Inherently, the BC record is transparent. Through network access, anyone can analyze and track each activity. Furthermore, the functionality of ''smart contract'' given by some BC networks, viz., Ethereum, enables the creation of a contract that runs when the condition is met. It provides the control back to the user and is no longer necessary for the strong central authority. Promising technologies such as IoT and BC are widely adopted in the public and industry sectors. The stimulating aspect of BC is that information is entirely decentralized and not stored in a single central point. In addition, BC provides the benefits of cost-effectiveness and traceability for supply chain management. It tracks the movement of quantity, origin, goods, etc.

The network validates that the new transaction is authoritative to guarantee that a legitimate transaction is added to the BC and further prevents the invalidation of prior transactions. When the networked computer has obtained agreement on the authority of the transaction, a new data block is added to BC. The blocks are placed permanently once they are added to the ledger, and transactions included in the block are verified and accessed by each user on the network. Like distributed data, the BC is the structured list that stores information. It is easy to handle as the participant in the network stores and verifies BC. The body part contains transactions. The indexing technique was employed to retrieve the block data. The header comprises the hash value of the prior and present block, a timestamp, and a nonce.

B. FEATURE SELECTION

BFOA can apply the BPDL-SSHN technique for the feature selection process. The hunting performance of foxes stimulates the FOX optimizer procedure [24]. It contains approaches for evaluating the space between the fox and its victim, allowing effective jumps in the optimizer procedure. The method computes a novel location for the fox depending on factors like direction range, jump value, and space to the target. The system mimics the red fox's plan of arbitrarily examining victims in snow climate situations by trusting its capability to get the ultrasound released by the target. By reviewing the sound, the fox guesses the distance to the victim and computes the exact jump wanted to arrest it. The FOX procedure sets a populace of search agents signified by the matrix and estimates their fitness using a benchmark function. It stables exploitation and exploration stages employing a random parameter, and optimum fitness and location values are defined during the iteration. It slowly reduces the search performance depending upon the finest location, allowing the actual exploration and initiation of dissimilar stages. The FOX-optimizer method is applied for the range of significant feature selection.

Eight dissimilar two variations of the FOX optimizer model have been developed and applied to optimize the cost function value for FS. It is intended by employing Eq. (1).

$$CF = -(a \times Acc + b \times F_1 + c \times AS - d \times (CSF/FSD). \tag{1}$$

Here, CF is said to be a cost function estimated by constraint specified in Eq. (2), Where asa, b, c, and d denote the weights hyperparameter for the cost function.

$$a + b + c + d = 1. \tag{2}$$

The search procedure consequences in novel locations for the red fox are in nonstop form. But the nonstop position wants to be changed into dual values. This can be attained by using V- and S-shaped transfer functions to all dimensions. It directs the red fox to transfer to two places. Four sigmoidal (S-shaped) transfer functions are employed to adapt the fundamental ethics of the fox location into prospect values ranging from zero to one.

$$S_1 \rightarrow T\left(X_i^k(u)\right) = \frac{1}{1 + e^{-2X_i^k(u)}} \tag{3}$$

$$S_2 \rightarrow T\left(X_i^k(u)\right) = \frac{1}{1 + e^{-X_i^k(u)}} \tag{4}$$

$$S_3 \rightarrow T\left(X_i^k(u)\right) = 1/(1+e^{(-X_i^k(u)/2)}) \tag{5}$$

$$S_4 \rightarrow T\left(X_i^k(u)\right) = 1/(1+e^{(-X_i^k(u)/3)}) \tag{6}$$

Here, X_i^k designates the location of i^{th} red-fox with u^{th} iteration at k^{th} variable. The constant values are transformed into dual forms depending upon the state in Eq. (7). rand is an arbitrary integer within (0,1).

$$X_i^k(u+1) = \begin{cases} 1: & rand \geq T\left(X_i^k(u)\right) \\ 0: & rand < T\left(X_i^k(u)\right) \end{cases} \tag{7}$$

Likewise, four V-shaped transfer functions are provided below.

$$V_1 \rightarrow T\left(X_i^k(u)\right) = \left| erf(\sqrt{\pi}/2X_i^k(u)) \right| \tag{8}$$

$$V_2 \rightarrow T\left(X_i^k(u)\right) = \left| \tanh\left(X_i^k(u)\right) \right| \tag{9}$$

$$V_3 \rightarrow T\left(X_i^k(u)\right) = \left| X_i^k(u)/\sqrt{1 + X_i^k(u)} \right| \tag{10}$$

$$V_4 \rightarrow T\left(X_i^k(u)\right) = \left| \frac{2\left(\arctan\left(\frac{\pi X_i^k(u)}{2}\right)\right)}{\pi} \right| \tag{11}$$

If the rand value is less, all binary values in the location vector are reversed; otherwise, the fox location does not alter from the latter iteration.

$$X_i^k(u+1) = \begin{cases} X_i^k: & rand \geq T\left(X_i^k(u)\right) \\ (X_i^k)^{-1}: & rand < T\left(X_i^k(u)\right) \end{cases} \tag{12}$$

C. CLASSIFICATION USING ALSTM

At this stage, the ALSLTM-based classification process is utilized. As a specific architecture of RNN, LSTM networks have gained popularity for predicting time-series data [25]. This is indispensable for the LSTM to selectively transfer information, addressing problems like exploding and vanishing gradients during backpropagation. The forget, input and output gates are the three significant gates of LSTM.

At first, the forget gate defines which information must be discarded in the cell state.

$$f_t = \sigma\left(W_f \times [h_{t-1}, x_t] + b_f\right) \tag{13}$$

In Eq. (13), the prior hidden layer output is represented as h_{t-1}, W, and b are the weight matrix and bias, correspondingly, and x_t refers to the existing input, with σ sigmoid activation.

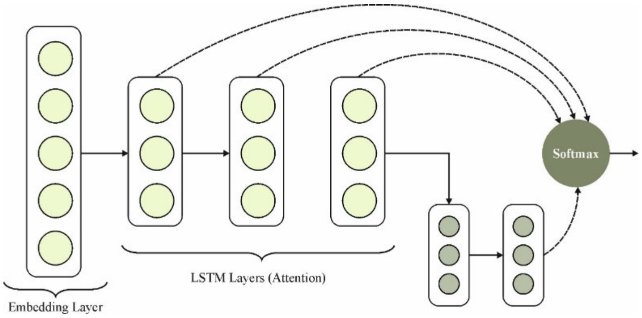

FIGURE 2. Structure of ALSTM.

Then, the input gate adopts the data maintained in the cell state:

$$i_t = \sigma\left(W_i \times [h_{t-1}, x_t] + b_i\right) \tag{14}$$

$$\tilde{C}_{\mathrm{t}} = \tanh\left(W_C \times [h_{t-1}, x_t] + b_C\right) \tag{15}$$

The existing state of a neuron is derived:

$$C_t = f_{t-1}C_{t-1} + i_{t-1}\tilde{C}_t \tag{16}$$

The output gate determines the last output. The sigmoid function assesses that part of the cell layer to allocate to the output:

$$\mathrm{o}_t = \sigma\left(W_{\mathrm{o}} \times [h_{t-1}, x_t] + b_{\mathrm{o}}\right) \tag{17}$$

$$h_t = \mathrm{o}_t \times \tanh(C) \tag{18}$$

The LSTM can detect the pattern over time, which makes it especially valuable for seizure detection in a biomedical context. This model exploits an LSTM layer containing 128 units. The model is fine-tuned for better performance with the categorical-cross entropy loss function and "*Adam*" optimizer, which is suitable for multi-class classification.

The attention mechanism (AM) is a good idea for upgrading the significance of vital data stimulated by the human visual method [26]. When human vision perceives whatever is in the atmosphere, it does not regularly see an act from start to finish but somewhat concentrates on an exact part as required. Depending upon this, the AM selectively concentrates on some of the most significant data, dismisses unwanted data, and increases necessary information. AM is usually employed in earthquake prediction, machine translation, and image captioning. AM performs depend upon the weight allocation, defining the effectual data by allocating greater weights. As an outcome, it has a positive optimizer effect on the traditional techniques. The calculating attention contains three phases. Fig. 2 represents the infrastructure of ALSTM. Initially, the resemblance or association between the Query and every Key is intended as follows:

$$s_t = \tanh\left(W_h h_t + b_h\right) \tag{19}$$

where s_t denotes the score of attention. b_h and W_h refer to the bias and weight of AM, respectively. h_t represents an input vector. During the next phase, the score acquired from the first phase is regularized, and the *softmax* function is used to transform the score of attention as assumed in the formulation:

$$a_t = \frac{\exp(s_t)}{\sum_t \exp(s_t)} \tag{20}$$

As regards the weight constant, the last attention value has been attained by the weighted total value as presented in the formulation:

$$s = \sum_t a_t h_t \tag{21}$$

Generally, AM is utilized after the LSTM model to concentrate on the features affecting output variables, increasing the model's performance.

D. HSWO-BASED HYPERPARAMETER TUNING

Finally, the design of the HSWO technique helps in the optimal hyperparameter selection of the ALSTM model. HSWOA is a biologically inspired optimization method derived from the strong sensing capability of seal whiskers in chasing the target [27]. Unlike humans, most of the mammals have whiskers. Since the base of seal whiskers is densely packed with nerve endings, these wiry, dense hairs are susceptible to each movement. Like a seal, a marine animal can sense and observe the object through whiskers; however, it senses vibration in the water. Typically, mammals have uniform, roundly shaped whiskers. However, most seal species have irregular and wavy-shaped whiskers. The whisker vibrates only in response to hydrodynamic trails. Although they lack a lateral-line system, the Harbor Seal uses their whiskers to track underwater disturbance and find prey.

Whiskers moving together send signals to the nerves carried to the harbour seal's brain, which is stimulated by the water flow. This allows the seal to interpret and process complicated environments. The whisker's elliptical cross-section enables it to differentiate the angle of attack from the water flow.

The zero-attack angle represents the primary axis of an ellipse and is parallel to the incoming flow. When the water flow is coming from different directions, the whiskers will have various characteristic diameters, which leads to drag pressure on the whiskers. Drag forces will be conveyed to cheek tension at the bottom of the whisker since there are no nerves within the whiskers, which generates sensory signals for the harbour seal.

1) EXPLORATION MODE

At a certain sensing velocity, the harbour seal explores the search range to attack the prey using whiskers. While tracing underwater vibration, the seals hold their whiskers up and away from their faces. The prey movement stirs up the water. The seal's whisker picks up the hydrodynamic trails the prey leaves, which follow the prey's trails. This enables us to define the prey's direction, proximity, and size. The angular frequency, the oscillating sphere diameter, and the displacement amplitude are s, d, and ω, correspondingly formulated by:

$$v_i = \frac{M}{2\pi} \frac{\left(2x_i^2 - D^2\right)}{(x_i^2 + D^2)^{5/2}} \tag{22}$$

$$Ms = 2\pi\omega s d^3 \sin(\omega t) \tag{23}$$

where the distance between seals and prey is represented as D, x_i refers to the seal's location. The time harbour seals take to sense the underwater disturbance of prey is defined as t.

2) EXPLOITATION MODE

After the update, the seals exploit the potential location of the prey in this mode. The updated sensing velocity is formulated by:

$$v_i^{k+1} = Lr_1 v_i^k + bQr_2\left(GP_{best} - x_i^k\right) + aQr_3\left(LP_{best,i} - x_i^k\right) \tag{24}$$

$$L = ab^* \frac{1}{\sqrt{b^2\sin^2 Q + a^2\cos^2 Q}} \tag{25}$$

$$a = 0.14\sin(0.92n + 1.5\pi) + 1 \tag{26}$$

$$b = 0.067\sin(0.91n + \pi) - 0.0041n + 0.64 \tag{27}$$

Here , a and b are the length of the major and minor axes of the ellipse, L denotes the ellipse diameter, r_1, r_2, and r_3 are randomly generated integers, the count of cross sections of one whisker refers to n, and the flowing water attack angle is Q.

The updated location of the seal is

$$x_i^{k+1} = x_i^k + v_i^{k+1} \tag{28}$$

The HSWO method develops a fitness function (FF) for greater classification efficiency. It defines the positive integer to represent the higher outcomes of the solution candidate. In this study, the decline of the classifier error rate is considered the FF.

$$\begin{aligned} fitness\,(x_i) &= ClassifierErrorRate\,(x_i) \\ &= \frac{No.\ of\ misclassified\ instances}{Total\ No.\ of\ instances} \times 100 \end{aligned} \tag{29}$$

IV. RESULT ANALYSIS

This section examines the performance validation of the BPDL-SSHN technique using the NSL-KDD dataset [28]. The dataset includes 126238 samples with two class labels, as represented in Table 1.

TABLE 1. Details on database.

Classes	No. of Samples
Normal	65495
Attack	60743
Total Instances	126238

Fig. 3 displays the confusion matrices produced by the BPDL-SSHN approach under 80:20 and 70:30 of TRPH/TSPH. The outcomes specify the effective recognition of the normal and attack samples with all classes.

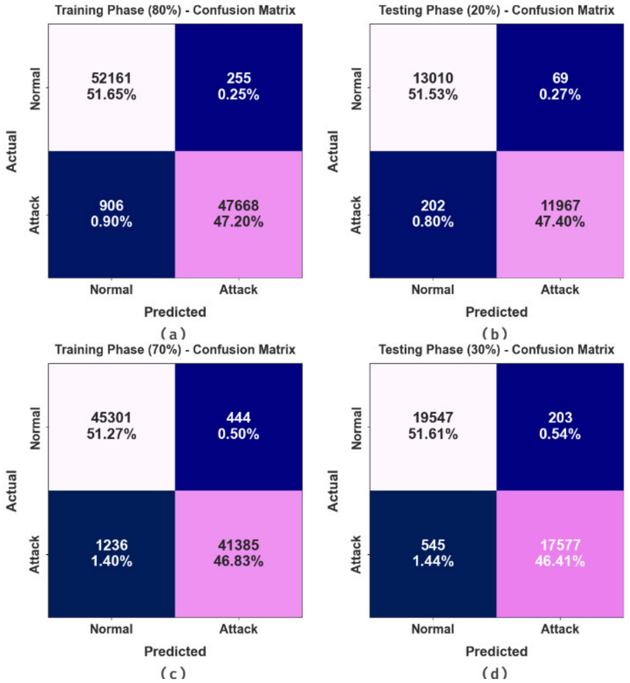

FIGURE 3. Confusion matrices of (a-b) 80:20 of TRPH/TSPH and (c-d) 70:30 of TRPH/TSPH.

Table 2 shows the overall detection analysis of the BPDL-SSHN approach under 80:20 of TRPH/TSPH.

TABLE 2. Detection outcome of BPDL-SSHN technique under 80:20 of TRPH/TSPH.

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	MCC
TRPH (80%)					
Normal	99.51	98.29	99.51	98.90	97.70
Attack	98.13	99.47	98.13	98.80	97.70
Average	98.82	98.88	98.82	98.85	97.70
TSPH (20%)					
Normal	99.47	98.47	99.47	98.97	97.86
Attack	98.34	99.43	98.34	98.88	97.86
Average	98.91	98.95	98.91	98.92	97.86

In Fig. 4, the training results of the BPDL-SSHN technique are stated under 80% of TRPH. These outcomes showcase that the BPDL-SSHN method offers capable detection of normal and attack classes. With normal class, the BPDL-SSHN technique obtains an increased $accu_y$ of 99.51%, $prec_n$ of 98.88%, $reca_l$ of 98.82%, F_{score} of 98.85%, and MCC of 97.70%. Meanwhile, based on attack class, the BPDL-SSHN method gets improved $accu_y$ of 98.13%, $prec_n$ of 99.47%, $reca_l$ of 98.13%, F_{score} of 98.80%, and MCC of 97.70%.

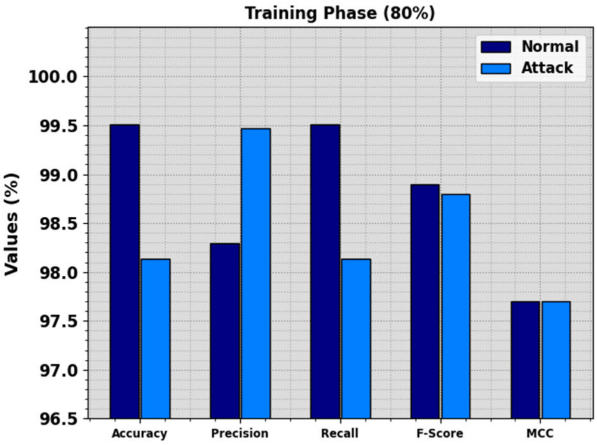

FIGURE 4. Detection outcome of BPDL-SSHN technique under 80% of TRPH.

In Fig. 5, the testing outcomes of the BPDL-SSHN method can be described on 20% of TSPH. These findings highlight that the BPDL-SSHN method achieves efficient detection of normal and attack classes. According to normal class, the BPDL-SSHN technique achieves raised $accu_y$ of 99.47%, $prec_n$ of 98.47%, $reca_l$ of 99.47%, F_{score} of 98.97%, and MCC of 97.86%. Besides, with attack class, the BPDL-SSHN technique gains increased $accu_y$ of 98.34%, $prec_n$ of 99.43%, $reca_l$ of 98.34%, F_{score} of 98.88%, and MCC of 97.86%.

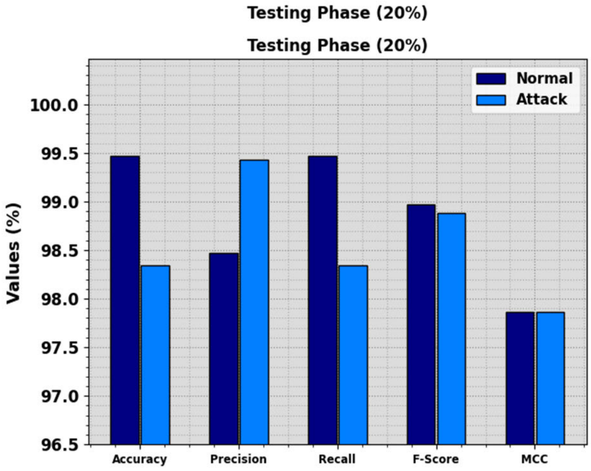

FIGURE 5. Detection outcome of BPDL-SSHN technique under 20% of TSPH.

Table 3 reports the overall detection analysis of the BPDL-SSHN technique at 70:30 TRPH/TSPH. In Fig. 6, the training outcomes of the BPDL-SSHN technique can be determined under 70% of TRPH. These results show that the BPDL-SSHN method effectively identifies normal and attack classes. Based on normal class, the BPDL-SSHN method acquires a higher $accu_y$ of 99.03%, $prec_n$ of 97.34%, $reca_l$ of 99.03%, F_{score} of 98.18%, and MCC of 96.21%. Also, based on the attack class, the BPDL-SSHN technique attains raised $accu_y$ of 97.10%, $prec_n$ of 98.94%, $reca_l$ of 97.10%, F_{score} of 98.01%, and MCC of 96.21%.

TABLE 3. Detection outcome of BPDL-SSHN technique under 70:30 of TRPH/TSPH.

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	MCC
70% of TRPH					
Normal	99.03	97.34	99.03	98.18	96.21
Attack	97.10	98.94	97.10	98.01	96.21
Average	98.06	98.14	98.06	98.10	96.21
30% of TSPH					
Normal	98.97	97.29	98.97	98.12	96.06
Attack	96.99	98.86	96.99	97.92	96.06
Average	97.98	98.07	97.98	98.02	96.06

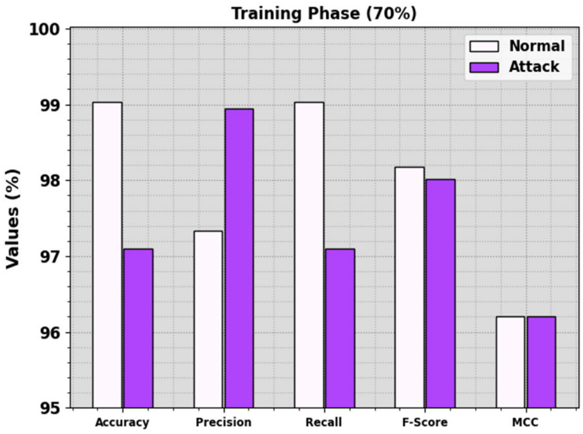

FIGURE 6. Detection outcome of BPDL-SSHN technique under 70% of TRPH.

In Fig. 7, the testing analysis of the BPDL-SSHN technique is informed with 30% of TSPH. The acquired outcomes indicate that the BPDL-SSHN technique automatically recognizes normal and attack classes. According to normal class, the BPDL-SSHN technique obtains improved $accu_y$ of 98.97%, $prec_n$ of 97.29%, $reca_l$ of 98.97%, F_{score} of 98.12%, and MCC of 96.06%. In the meantime, with attack class, the

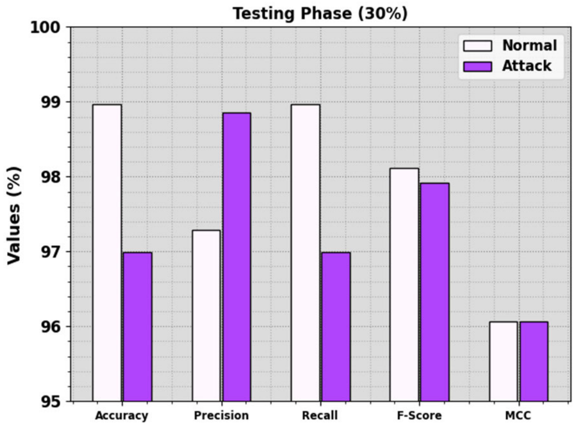

FIGURE 7. Detection outcome of BPDL-SSHN model under 30% of TSPH.

BPDL-SSHN approach gets an increased $accu_y$ of 96.99%, $prec_n$ of 98.86%, $reca_l$ of 96.99%, F_{score} of 97.92%, and MCC of 96.06%.

The $accu_y$ curves for training (TR) and validation (VL) displayed in Fig. 8 for the BPDL-SSHN method on 80:20 of TRPH/TSPH provides valued insights into its effectiveness with diverse epochs. Mainly, it can be a reliable improvement in both TR and TS $accu_y$ with increased epochs, representing the model's proficiency in learning and recognizing patterns in the data of TR and TS. The upward trend in TS $accu_y$ emphasizes the model's flexibility to the TR dataset and ability to produce correct predictions on unnoticed data, underscoring capabilities of robust generalization.

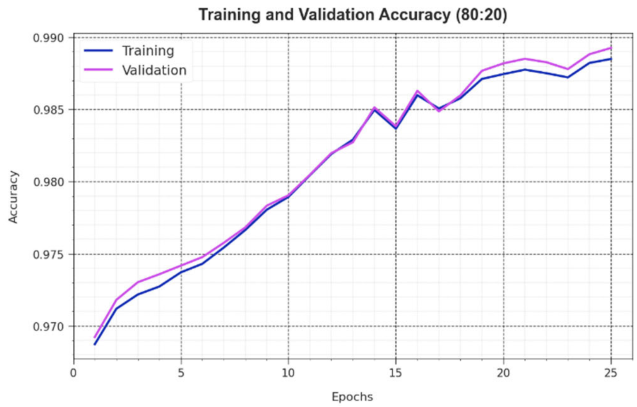

FIGURE 8. $Accu_y$ **curve of BPDL-SSHN technique under 80:20 of TRPH/TSPH.**

Fig. 9 illustrates an extensive overview of the TR and TS loss values for the BPDL-SSHN method under 80:20 of TRPH/TSPH through numerous epochs. The TR loss constantly diminishes as the model refines its weights to decrease classification errors under both datasets. The loss curves show the model's alignment with the TR data, emphasizing its ability to capture patterns successfully. The continued refinement of parameters in the BPDL-SSHN approach is significant and is targeted at lessening discrepancies between predictions and actual TR labels.

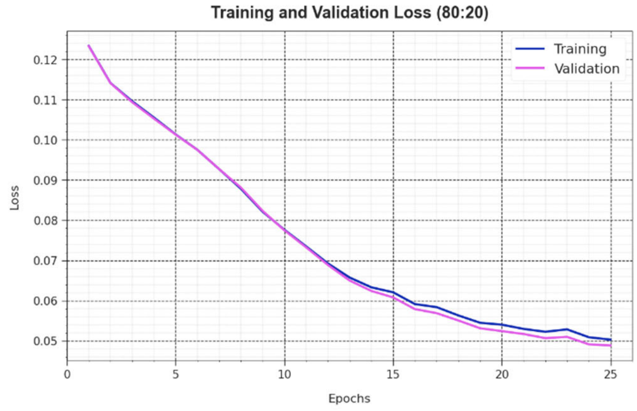

FIGURE 9. **Loss curve of BPDL-SSHN technique under 80:20 of TRPH/TSPH.**

Fig. 10 illustrates the classifier analysis of the BPDL-SSHN method with 80:20 and 70:30. Figs. 10a-10c represents the PR analysis of the BPDL-SSHN method. These accomplished findings indicated that the BPDL-SSHN method offers higher values of PR. Additionally, it is perceptible that the BPDL-SSHN technique can obtain higher PR values for each class. Lastly, Figs. 10b-10d shows the ROC analysis of the BPDL-SSHN technique. This figure defined that the BPDL-SSHN technique provides increased ROC values. Also, the BPDL-SSHN technique can extend enriched ROC values in all classes.

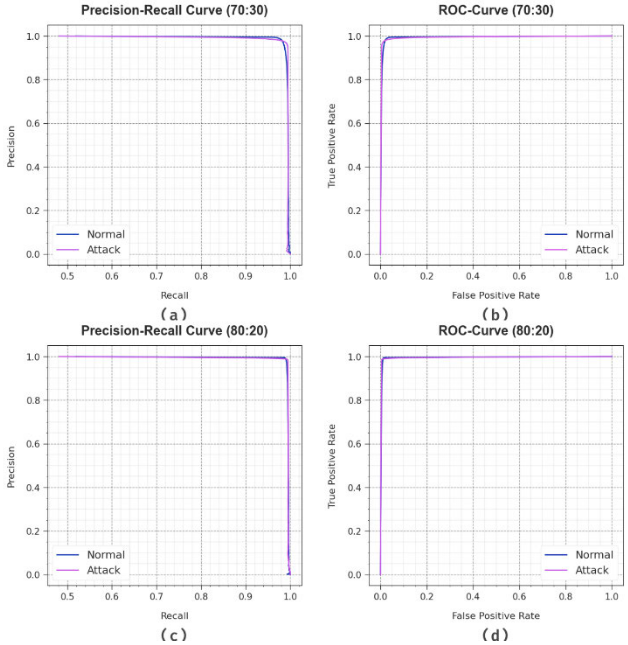

FIGURE 10. **(a-b) PR and ROC curves of 70:30 and (c-d) PR and ROC curves of 80:20.**

In Table 4 and Fig. 11, the performance of the BPDL-SSHN method can be compared with other models [11]. The simulated outcomes exhibit that the ANN-based IDS and GAN models obtain poor performance. At the same time, the DELM, RTS-DELM, SYD, and DNN models perform moderately well. Meanwhile, the BSSHN-GBOHDL

TABLE 4. **Comparison analysis of BPDL-SSHN approach with other methods.**

Methods	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
BPDL-SSHN	98.91	98.95	98.91	98.92
BSSHN- GBOHDL	98.29	98.34	98.29	98.31
ANN Based IDS	81.43	80.74	81.67	82.26
GAN	86.09	87.48	87.68	88.46
DELM	93.52	94.75	94.28	93.80
RTS-DELM	94.85	95.20	94.73	94.36
SYD	94.83	96.11	96.41	97.55
DNN	94.51	94.16	95.21	95.94

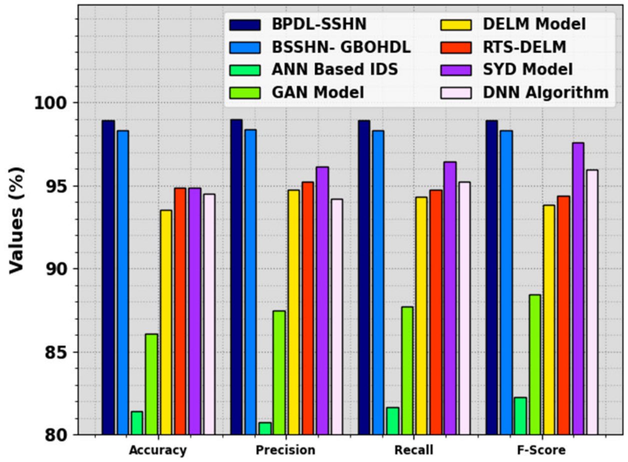

FIGURE 11. Comparative outcome of BPDL-SSHN technique with other methods.

model reaches near-optimal performance. However, the BPDL-SSHN technique results in superior performance with maximum results with $accu_y$ of 98.91%, $prec_n$ of 98.95%, $reca_l$ of 98.91%, and F_{score} of 98.92%.

Table 5 and Fig. 12 compare the BPDL-SSHN technique's computation time (CT) results with recent techniques. These results show that the BPDL-SSHN technique gains better performance with a minimal CT of 4.10s. On the other hand, the BSSHN-GBOHDL, ANN-based IDS, GAN, DELM, RTS-DELM, SYD, and DNN methods acquire increased CT outcomes. These accomplished outcomes depicted the superior solution of the BPDL-SSHN approach.

TABLE 5. CT analysis of BPDL-SSHN technique with other methods.

Methods	CT (Sec)
BPDL-SSHN	4.10
BSSHN- GBOHDL	7.85
ANN-Based IDS	18.05
GAN	18.58
DELM	13.63
RTS-DELM	9.51
SYD	11.78
DNN	9.74

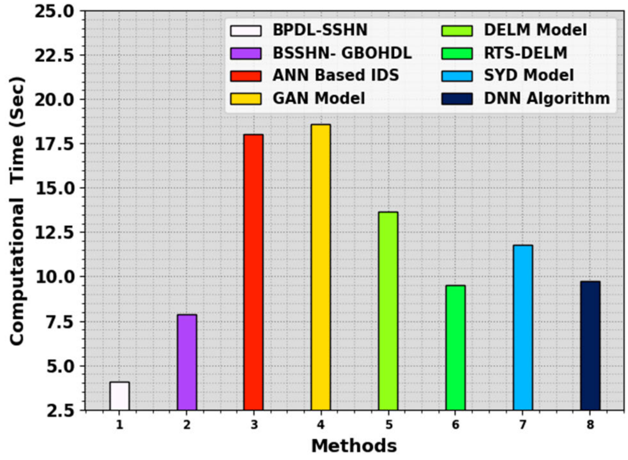

FIGURE 12. Comparative outcome of BPDL-SSHN method with recent models.

V. CONCLUSION

This study introduced a novel BPDL-SSHN technique in the IoT-cloud environment. In the BPDL-SSHN technique, BC technology is applied, which enables the data to be collected confidentially in the smart home network. Additionally, the BPDL-SSHN method follows a series of processes to detect malicious activities, such as HSWO method-based hyperparameter tuning, ALSTM-based classification, and BFOA-based feature selection. The design of the HSWO technique helps in the optimal hyperparameter selection of the ALSTM network, significantly enhancing the detection performance. The comparative analysis of the BPDL-SSHN technique reported the proficient performance of the smart home network in monitoring and detecting harmful or malicious activities. The experimental findings stated that the BPDL-SSHN method achieves better results than other techniques. The limitations of the BPDL-SSHN method include scalability and adaptability to diverse atmospheres, which remain a potential threat. Future research could focus on scalability, real-time recognition, and privacy augmentation to widen its applicability in varied smart home contexts.

ACKNOWLEDGMENT

The author would like to thank the Deanship of Scientific Research at Shaqra University for supporting this research.

REFERENCES

[1] J. B. Awotunde, T. Gaber, L. V. N. Prasad, S. O. Folorunso, and V. L. Lalitha, "Privacy and security enhancement of smart cities using hybrid deep learning-enabled blockchain," *Scalable Comput., Pract. Exper.*, vol. 24, no. 3, pp. 561–584, Sep. 2023.

[2] A. T. Kouanou, C. T. Tchapga, M. S. Ekonde, V. Monthe, B. A. Mezatio, J. Manga, G. R. Simo, and Y. Muhozam, "Securing data in an Internet of Things network using blockchain technology: Smart home case," *Social Netw. Comput. Sci.*, vol. 3, no. 2, p. 167, Mar. 2022.

[3] A. Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan, and P. Tiwari, "Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT," *Digit. Commun. Netw.*, vol. 9, no. 2, pp. 411–421, Apr. 2023.

[4] M. Picone, S. Cirani, and L. Veltri, "Blockchain security and privacy for the Internet of Things," *Sensors*, vol. 21, no. 3, p. 892, Jan. 2021.

[5] S. M. Nagarajan, P. Anandhan, V. Muthukumaran, K. Uma, and U. Kumaran, "Security framework for IoT and deep belief network-based healthcare system using blockchain technology," *Int. J. Electron. Bus.*, vol. 17, no. 3, pp. 226–243, 2022.

[6] A. Ali, B. A. S. Al-rimy, F. S. Alsubaei, A. A. Almazroi, and A. A. Almazroi, "HealthLock: Blockchain-based privacy preservation using homomorphic encryption in Internet of Things healthcare applications," *Sensors*, vol. 23, no. 15, p. 6762, Jul. 2023.

[7] N. Butt, A. Shahid, K. N. Qureshi, S. Haider, A. O. Ibrahim, F. Binzagr, and N. Arshad, "Intelligent deep learning for anomaly-based intrusion detection in IoT smart home networks," *Mathematics*, vol. 10, no. 23, p. 4598, Dec. 2022.

[8] J. Cai, W. Liang, X. Li, K. Li, Z. Gui, and M. K. Khan, "GTx-Chain:A secure IoT smart blockchain architecture based on graph neural network," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 21502–21514, Dec. 2023, doi: 10.1109/JIOT.2023.3296469.

[9] L. Guo, "Application of blockchain based on deep learning algorithm in enterprise Internet of Things system," *Mobile Inf. Syst.*, vol. 2022, no. 1, Aug. 2022, Art. no. 9943452, doi: 10.1155/2022/9943452.

[10] M. Navaneethan and S. Janakiraman, "An optimized deep learning model to ensure data integrity and security in IoT based e-commerce block chain application," *J. Intell. Fuzzy Syst.*, vol. 44, no. 5, pp. 8697–8709, May 2023, doi: 10.3233/JIFS-220743.

[11] L. Almuqren, K. Mahmood, S. S. Aljameel, A. S. Salama, G. P. Mohammed, and A. A. Alneil, "Blockchain-assisted secure smart home network using gradient-based optimizer with hybrid deep learning model," *IEEE Access*, vol. 11, pp. 86999–87008, 2023, doi: 10.1109/ACCESS.2023.3303087.

[12] M. A. Almaiah, A. Ali, F. Hajjej, M. F. Pasha, and M. A. Alohali, "A lightweight hybrid deep learning privacy preserving model for FC-based industrial Internet of Medical Things," *Sensors*, vol. 22, no. 6, p. 2112, Mar. 2022.

[13] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Secure computation offloading in blockchain based IoT networks with deep reinforcement learning," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 3192–3208, Oct. 2021.

[14] K. Shah, N. K. Jadav, S. Tanwar, A. Singh, C. Pleşcan, F. Alqahtani, and A. Tolba, "AI and blockchain-assisted secure data-exchange framework for smart home systems," *Mathematics*, vol. 11, no. 19, p. 4062, Sep. 2023.

[15] N. K. Jadav, R. Gupta, M. D. Alshehri, H. Mankodiya, S. Tanwar, and N. Kumar, "Deep learning and onion routing-based collaborative intelligence framework for smart homes underlying 6G networks," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 3, pp. 3401–3412, Sep. 2022.

[16] B. M. Yakubu, M. I. Khan, A. Khan, F. Jabeen, and G. Jeon, "Blockchain-based DDoS attack mitigation protocol for device-to-device interaction in smart home," *Digit. Commun. Netw.*, vol. 9, no. 2, pp. 383–392, Apr. 2023.

[17] A. Badshah, M. Waqas, F. Muhammad, G. Abbas, and Z. H. Abbas, "A novel framework for smart systems using blockchain-enabled Internet of Things," *IT Prof.*, vol. 24, no. 3, pp. 73–80, May 2022.

[18] E. Ntizikira, L. Wang, J. Chen, and K. Saleem, "Honey-block: Edge assisted ensemble learning model for intrusion detection and prevention using defense mechanism in IoT," *Comput. Commun.*, vol. 214, pp. 1–17, Jan. 2024, doi: 10.1016/j.comcom.2023.11.023.

[19] D. M. Doe, J. Li, N. Dusit, Z. Gao, J. Li, and Z. Han, "Promoting the sustainability of blockchain in web 3.0 and the Metaverse through diversified incentive mechanism design," *IEEE Open J. Comput. Soc.*, vol. 4, pp. 171–184, 2023, doi: 10.1109/OJCS.2023.3260829.

[20] D. Dansana, P. K. Behera, S. G. K. Patro, Q. N. Naveed, A. Lasisi, and A. W. Wodajo, "BSMACRN: Design of an efficient blockchain-based security model for improving attack-resilience of cognitive radio ad-hoc networks," *IEEE Access*, vol. 12, pp. 10047–10058, 2024, doi: 10.1109/ACCESS.2024.3350739.

[21] N. Afraz, F. Wilhelmi, H. Ahmadi, and M. Ruffini, "Blockchain and smart contracts for telecommunications: Requirements vs. cost analysis," *IEEE Access*, vol. 11, pp. 95653–95666, 2023, doi: 10.1109/ACCESS.2023.3309423.

[22] D. Dansana, P. K. Behera, A. A. Darem, Z. Ashraf, A. T. Zamani, M. N. Ahmed, G. K. Patro, and M. Shameem, "BDDTPA: Blockchain-driven deep traffic pattern analysis for enhanced security in cognitive radio ad-hoc networks," *IEEE Access*, vol. 11, pp. 98202–98216, 2023, doi: 10.1109/ACCESS.2023.3312291.

[23] S. Singh, I.-H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of Things smart home architecture based on cloud computing and blockchain technology," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 4, Apr. 2019, Art. no. 155014771984415.

[24] R. Sharma, G. K. Mahanti, G. Panda, A. Rath, S. Dash, S. Mallik, and Z. Zhao, "Comparative performance analysis of binary variants of FOX optimization algorithm with half-quadratic ensemble ranking method for thyroid cancer detection," *Sci. Rep.*, vol. 13, no. 1, p. 19598, Nov. 2023.

[25] S. U. Khan, S. U. Jan, and I. Koo, "Robust epileptic seizure detection using long short-term memory and feature fusion of compressed time–frequency EEG images," *Sensors*, vol. 23, no. 23, p. 9572, Dec. 2023.

[26] P. Kavianpour, M. Kavianpour, E. Jahani, and A. Ramezani, "A CNN-BiLSTM model with attention mechanism for earthquake prediction," *J. Supercomput.*, vol. 79, no. 17, pp. 19194–19226, Nov. 2023, doi: 10.1007/s11227-023-05369-y.

[27] H. Zaher, H. Al-Wahsh, M. H. Eid, R. S. A. Gad, N. Abdel-Rahim, and I. M. Abdelqawee, "A novel harbor seal whiskers optimization algorithm," *Alexandria Eng. J.*, vol. 80, pp. 88–109, Oct. 2023.

[28] Accessed: Feb. 23, 2024. [Online]. Available: https://www.unb.ca/cic/datasets/nsl.htm