Journal of Intelligent Systems and Internet of Things
Vol. 15, No. 02, PP. 01-13, 2025
DOI: https://doi.org/10.54216/JISIoT.150201

Blockchain-Enabled Multi-Head Attention Based Deep Learning Model for Intrusion Detection System in Smart Networks

Ehab Bahaudien Ashary[1,*]
[1]Electrical and Computer Engineering Department, Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia
Email: eashary@kau.edu.sa

Abstract

Intrusion Detection Systems (IDS) are increasingly being integrated into smart homes for effective pervasive sensing and resource management, thanks to advancements in sensor technologies and the development of Information and Communication Technology (ICT). Securing IDSs in smart homes is significant for safeguarding crucial data and ensure the integrity of related devices. Implementing strong cybersecurity, measures, including regular software updates, encrypted communication protocols, and secure authentication mechanisms, is critical to safeguard potential risks. As the smart home network constantly increasing, developers, users, and manufacturers must work together to maintain and prioritize stringent security standards, alleviating the risks closely related to connected devices and preserving the safety and privacy of the consumer. Blockchain (BC) technology can increase the security of IDS in smart homes by giving a tamper-resistant and decentralized framework to manage data transactions and device interactions. By leveraging blockchain, smart home networks can establish a more secure and resilient infrastructure, which provides consumers with high confidence in the security and privacy of the interconnected devices. This study introduces a Blockchain and Multi-Head Attention-Based Deep Learning for Intrusion Detection System in Smart Networks (BCMHDL-IDSSN) technique in Smart Home Networks. The BCMHDL-IDSSN method aims to enhance security in the smart home networks. In the BCMHDL-IDSSN technique, BC technology is used to achieve security. Besides, the BCMHDL-IDSSN technique involves the design of a multi-head attention bidirectional gated recurrent unit (MHA-BiGRU) method for the detection of malicious activities. Finally, an enhanced pigeon-inspired optimization (EPIO) model is applied for the optimal hyperactive parameter choice of the MHA-BiGRU model. A detailed investigation was applied to validate the performance of the BCMHDL-IDSSN method. The simulation values emphasized that the BCMHDL-IDSSN method gains high efficiency over other techniques.

Received: September 14, 2024 Revised: November 10, 2024 Accepted: January 03, 2025

Keywords: Blockchain; Bidirectional Gated Recurrent Unit; Consumer Electronic Devices; Smart Home; Pigeon Inspired Optimization

1. Introduction

Intrusion detection is performed to make our day-to-day lives easy. There are various consumer electronic devices for particular applications namely wearable devices, medical devices, devices for entertainment and business, and so on. While these devices offer advanced proficiencies and services to consumers, they also give new challenges [1]. Especially, security and privacy complexities of these devices are especially significant. Numerous IDSs have wireless connections that increase their vulnerability to safety attacks [2]. In recent times, the IoT has become a division of consumer electronics wherein devices are linked to the Internet. This internet connectivity can be more improve these products' privacy and security difficulties due to the existence of malicious users and attackers through the internet [3]. Smart homes are linked to the Internet, permitting users to control various smart gadgets that assist significant purposes in the home for the consumer and their family. IoT is the basis of smart home networks, interconnecting different smart devices like wearable devices, smart computers, and smartphones. By making their homes more open and protected, the survival of people may be safer and easier. Smart homes provide

beneficial resources like monitoring behaviors and security analysis that have interesting users and system developers for carrying out wide-ranging research [4]. Blockchain (BC) technology is a major developing technology for resolving the aforementioned complexities.

As a distributed ledger technology, BC can store data continuously in an unassailable, distributed, and decentralized database [5]. As an alternative to relying on a centralized system, BC provisions trust among contributors dependent on the agreed-upon consensus methods. The decentralized aspect of BC technology assists diverse abilities of IDS, beginning from data storage constantly to preserving transparency. Therefore, if data is included in the BC network via block, it will not altered [6]. BC provides a high level of security for cybersecurity and safe data exchange through its cryptographic features. With the help of smart contracts, it automatically obtained activities, while a few predetermined conditions have been satisfied. In cybersecurity, consensus methods could be employed to decide on a few phases [7]. Additionally, BC technology helps to safely implement transactions of cybersecurity and accomplish an effective and protective supply chain management system; there is no requirement for an intermediate or additional delay. Accordingly, BC technology assists end users of cybersecurity in having superior experiences.

Since traditional techniques employ a signature-based algorithm for identifying unique measures, a wide-ranging Intrusion Detection System (IDS) is critical to solve the fundamental problem [8]. However, the most significant latest technologies, called the Deep Extreme Learning Machine (DELM) could be employed to estimate data flows for spot intrusions and attack patterns. Consequently, it is essential to deal with smart BC-assisted applications by emerging robust and adaptable techniques for processing massive quantities of information [9]. Machine learning (ML) comprises machines for behaving training, and reasoning without human involvement. This is named as an Artificial Intelligence (AI) model. The simple objective of ML is to make an efficient method for obtaining data from the input, creating a prediction, and changing the output by applying statistical analysis [10]. ML processes a considerable quantity of information and makes the decision directed by indication.

This study introduces a Blockchain and Multi-Head Attention-Based Deep Learning for Intrusion Detection System in Smart Networks (BCMHDL-IDSSN) technique in Smart Home Networks. The BCMHDL-IDSSN method aims to enhance security in the smart home networks. In the BCMHDL-IDSSN technique, BC technology is used to achieve security. Besides, the BCMHDL-IDSSN technique involves the design of a multi-head attention bidirectional gated recurrent unit (MHA-BiGRU) model for the detection of malicious activities. Finally, an enhanced pigeon-inspired optimization (EPIO) model is applied for the optimal hyperparameter choice of the MHA-BiGRU model. A detailed set of experiments was applied to validate the performance of the BCMHDL-IDSSN method.

2. Literature Works

Qashlan et al. [11] introduced a technique aimed at offering a privacy-preserving data collection method employing the ML. The utilization of difference privacy was also developed; a robust notation in privacy-preserving techniques for offering the proper assurances regards how much data is leaked employing a privacy inexpensive. This method employs the R′enyi differential privacy (RDP) ML method and is dependent upon a form of the stochastic gradient descent process. Khayyat et al. [12] provided an innovative BC-assisted Shark Smell Optimizer with the Hopfield Chaotic Neural Network (SSO-HCNN) method. The introduced SSO-HCNN model uses a composite Chaotic Map (CM). Moreover, the SSO technique was presented. In addition, the diffusion stage employs HCNN for making a self-diffusion chaotic matrix while the random image executes an XOR operation through the keys for acquiring the cipher images. In [13], a BC-based AKA method was incorporated with the explainable artificial intelligence (XAI) method. Particularly, the contributing individuals interact with one another in a protective way to share the data employing a BC-based AKA method. Alternatively, a SHapley Additive exPlanations (SHAP) technique was exploited for interpreting the noticeable features that integrate the majority of the decisions.

In [14], a novel two-level privacy-preserving model was developed in this study. This method closely integrated federated learning (FL) with partly homomorphic encryption. This selection for partly homomorphic encryption was dependent upon its higher balance among model effectiveness and computational efficiency. Combining partially homomorphic encryption enhances FL privacy assurance, presenting a more protectable layer. In [15], an innovative technique that confirms safe and apparent communication in IDS was developed. The study also presented a multi-criterion decision-making method named TOPSIS. Moreover, this developed method utilizes a BC model for incessant monitoring and tracking of devices, safeguarding liability, and surveillance of their previous communications. In [16], an adaptive optimum lightweight CNN (AOLCNN) system was implemented. BC was integrated to improve the transparency, privacy, and security of IoT systems. The integrated key store model entirely targeted for Android smartphones must be employed in the developed application of security-based web services. The NIST Curve P-256 was deployed for producing the key pairs and verifying with the help of the elliptical curve digital signature algorithm (ECDSA).

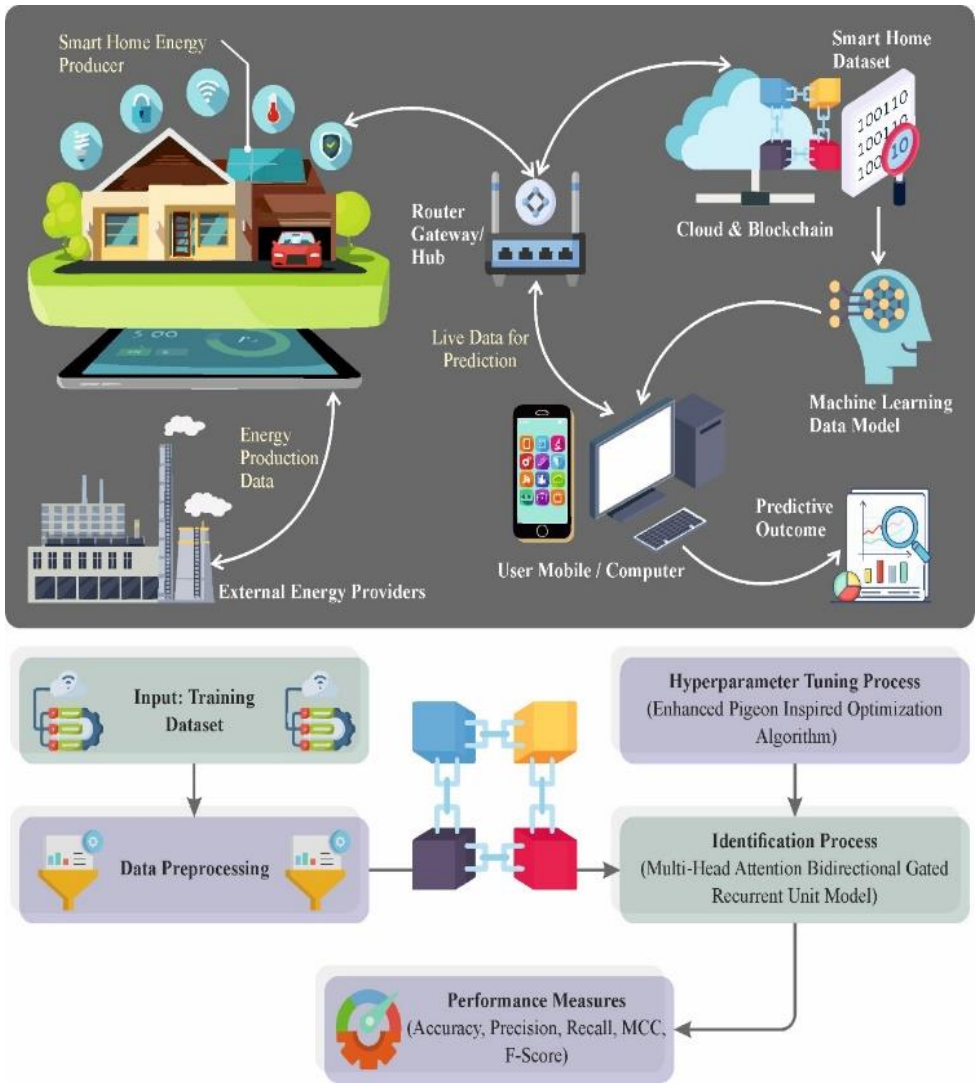

Figure 1. Overall flow of BCMHDL-IDSSN technique

Singh et al. [17] projected BC and FL-assisted Secure Architecture where BC-based IoT cloud infrastructure could be employed for security and privacy. The FL method was deployed for accessing the ML applications such as the medical field. Additionally, an ML system is acquired without transmitting personal information to the cloud. Xie et al. [18] examine a verifiable FL method assisting secure data collection without employing the bilinear groups (FLVA) model. Mainly, to resolve the problem of private key leakage in the gradient collection process on data of electronic products, a three-party key negotiation algorithm was proposed. The private gradients have been transferred and combined with ciphertext formats that ensure the privacy of the electronic product gradient.

3. The Proposed Method

In this work, a BCMHDL-IDSSN technique is presented for smart home networks. The BCMHDL-IDSSN method aims to enhance security in the smart home networks. The MHA-BiGRU-based malicious activity recognition and EPIO-based tuning are the two major processes. Fig. 1 shows the workflow of the BCMHDL-IDSSN methodology.

A. Blockchain

In the proposed context, the BC layer generates the transaction by the utility layer and user [19]. As a revolutionary technology, BC can revolutionize various sectors and industries. It is a decentralized database that verifies and records transactions, which replaces manual processes with automatic ones making it more secure, easier, and faster for the business to perform transactions without third parties. BC facilitates transactions in different industries, such as healthcare, the public sector, finance, etc. During the BC transaction, every block is chained to the prior block, generating public and permanent records of each transaction's details. This enables transparent and secure transactions since the block comprises a unique hash and timestamp that can be validated by the network.

BC helps to provide new opportunities for individuals and businesses, reduce fraud, and enhance efficiency by creating transparent and secure records of each transaction. The hash generator takes any size of input and produces a fixed size of output. The cryptographic hash function is the popular type of hash function utilized in security applications for protecting information from tampering. The cryptographic hash function is a one-way function that implies that it is not possible to obtain the original input and reverse the function. This makes it ideal to store information securely, as any attempt to modify the information leads to diverse hash values. SHA-1 and SHA-256 are the two most popular cryptographic hash functions. This function is utilized by several applications and websites to defend information.

The BC layer is performed by the Firebase BC platform to host the data. As a cloud-assisted platform, firebase provides different services and tools for application development. It provides various features including cloud storage, real-time database, hosting, and authentication. The application must be configured with the Firebase project to apply this feature in mobile or web applications. The configured data is restored in the JavaScript object, widely called a firebaseConfig object. The firebaseConfig object has various characteristics, namely authDomain, apiKey, projectId, databaseURL, storageBucket, measurementId, and appId. This property holds unique value to a certain Firebase project. The Firebase SDK for establishing the connection between the Firebase services and the app utilizes this value.

B. Malicious Activity Recognition using MHA-BiGRU

The BCMHDL-IDSSN technique involves the design of the MHA-BiGRU model for the detection of malicious activities that exist in IDS. Cho et al. introduced a simple GRU mechanism together with the tremendous growth of LSTM, particularly text classification, and the training time is long, the increased number of samples, the internal computation difficulty is higher, and the parameters are many [20]. The GRU mechanism preserves the new LSTM effects, using a better convergence model, simple structure, fewer parameters, plus a GRU model. It includes a reset and update gates. The gate of reset describes what amount previous hidden layer (HL) data is ignored. The more ignored the data is, the smaller the reset gate value will be. The update gate defines how much prior output HL affects the existing layer. The stronger the influence is, the larger the value is.

In the following ways, the GRU mechanism is updated:

$$r_t = \sigma(W_r * [h_{t-1}, x_t]) \tag{1}$$

$$z_t = \sigma(W_z * [h_{t-1}, x]) \tag{2}$$

$$\tilde{h}_t = \tanh(W_{\tilde{h}} * [r_t * h_{t-1}, x_t]) \tag{3}$$

$$h_t = (1 - z_t) * h_{\mathrm{t-1}} + z_t * \tilde{h}_t \tag{4}$$

In the equations, Z_t represents the update gate at moment $\tilde{h}_t$, r_t is the reset gate at moment t, h_t denotes the candidate activation at t moment, h_{t-1} embodies the HL at $(t-1)$ moment and h_{t-1} indicates the active state at t moment. The gate of reset r is described by the data received from the prior candidate state; the gate of update z can be defined by the prior data that the existing should be forgotten and the novel data is accepted.

GRU is a variant of unidirectional NN architecture, which is often output from the back. However, the output of the present moment has relationships with the before and after moment in classifying the text sentiment. At each moment, the input is used to provide dual GRUs in opposite directions, and these unidirectional GRUs define the output.

The present HL state of BiGRU is defined by combining the output $\overleftarrow{h}_{t-1}$ of the forward HL at the x_i and $(t-1)$ moment and the backward HL $\overleftarrow{h}_{t-1}$. The HL state $\vec{h}_{t-1}$ of Bi-GRU at t time is attained by weighting the HL forward and the HL $\overleftarrow{h}_{t-1}$ reverse:

$$\vec{h}_t = GRU(x_t, \vec{h}_{t-1}) \tag{5}$$

$$\overleftarrow{h}_t = GRU(x_t, \overleftarrow{h}_{t-1}) \tag{6}$$

$$h_t = w_t \vec{h}_t + v_t \overleftarrow{h}_t + b_t \tag{7}$$

The $GRU()$ function specifies the non-linear conversion to the input word vector, then it is encoded into the HL state. w_t and v_t are the weights respective to the $\vec{h}_t$ HL forward and the $\overleftarrow{h}_t$ HL reverse, at time t, b_t refers to the offset value respective to the HL at t moment.

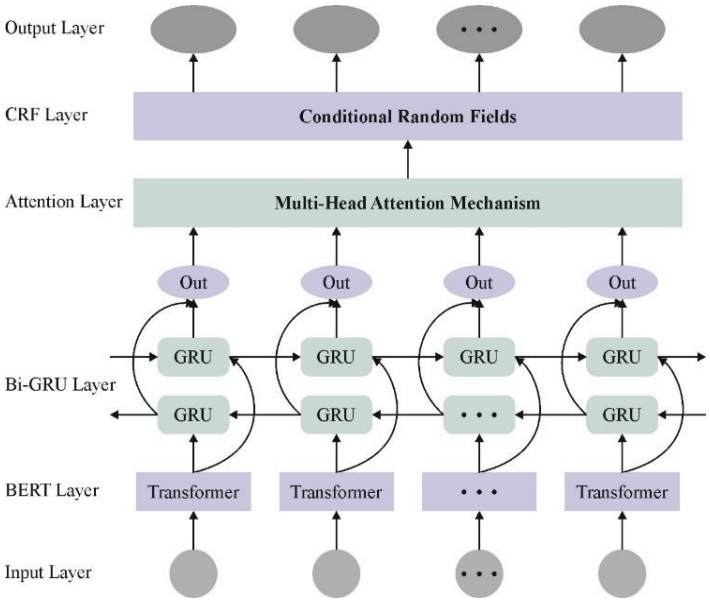

Figure 2. Architecture of MHA-BiGRU

The attention device initiated from the attention of human-visual that pretends when individuals detect data, they will mostly concentrate on exact fragments of the data [21]. Presently, attention is effectively functional for numerous tasks like text classification, image detection, machine translation, etc. The authors projected the multi-head attention (MA) mechanism. It obtains the important data of the series from numerous features, i.e., it can able to absorb deeper text feature data. The technique takes a BI-GRU layer output as vectors X_B, and the sequence of text input is $X = (x_1, x_2, \dots, x_t)$, whereas x_i denotes the i^{th} vector of word, and d refers to the dimensionality of the problem, $X \in \mathbb{R}^{n \times d}$. The MA layer input is $[X_B, X_B, X_B, X, X]$, $Q = K = V = X_B, Q \in \mathbb{R}^{n \times d_k}, K \in \mathbb{R}^{m \times d_k}, V \in \mathbb{R}^{m \times d_v}$ $Whereas$ Q, K, and V pass over 3 independent linear transformations that are exposed in Eqs. (8) - (10). Fig. 2 portrays the infrastructure of MHA-BiGRU.

$$Q = QW_i^Q \tag{8}$$

$$K = KW_i^K \tag{9}$$

$$V = VW_i^y \tag{10}$$

Permit the values of Q, K, and V into Scaled Dot-Product Attention, and do again that process h times, whereas h denotes the sum of heads of MA.

$$head_i = Attention(Q, K, V) \tag{11}$$

$$Attention\ (Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{cl_k}}\right)V \tag{12}$$

Lastly, every attention value () is merged as the last output of the MA layer, as revealed in Eq. (13).

$$MultiHead(O, K, V) = ConcaT(head_1, \dots, head_h) \tag{13}$$

C. Hyperparameter Tuning using EPIO Algorithm

Lastly, the EPIO technique is applied for the optimal hyperparameter choice of the MHA-BiGRU model. The PIO algorithm pretends to be the dual operative method employed in the method dependent upon the dissimilar navigational tools utilized by pigeons on their travel such as Landmark Operator and Map and Compass Operator [22].

$$V_i(t) = V_i(t-1) \times e^{-Rt} + rand \times \left(X_g - X_i(t-1)\right) \tag{14}$$

$$X_i(t) = X_i(t-1) + V_i(t) \tag{15}$$

Here, $rand$ denotes the randomly generated numbers between 0 and 1; R signifies the factor of map and compass that range among 0 and 1; X_g signifies the existing global finest location; t signifies the generation amount. In the dual-dimension space, the speed of the i^{th} pigeons has been defined by its preceding speed and the existing location that is compared to the present finest location of pigeons. Likewise, the ith pigeon location is based on its preceding location as well as its existing speed. By equating every pigeon's location, the individuals with the finest fitness value are nominated as the existing global best location, X_g.

$$Np(t) = \frac{Np(t-1)}{2} \tag{16}$$

$$X_c(t) = \frac{\Sigma X_i(t) \times fitness\big(X_i(t)\big)}{Np(t) \times \Sigma fitness\big(X_i(t)\big)} \tag{17}$$

$$X_i(t) = X_i(t-1) + rand \times \big(X_c(t) - X_i(t-1)\big) \tag{18}$$

Whereas, fitness () signifies the fitness of all pigeons, representing the excellence of the solution after estimation; $rand$ denotes the randomly generated number amid $zero$ and one; $X_c(t)$ refers to the vital location of every pigeon in generation t; Np indicates the number of pigeons residual in all groups that total half of the original population. In this estimation stage, the navigational position of the pigeon is dependent upon the midpoint location of higher individuals. At this stage, pigeons do not have the delay from their distinct speed. As an outcome, it can rapidly meet the optimum values.

The algorithm of PIO displays faster convergence because it has its specific disadvantages. If the early population is heavily spread or does not lie nearer the exact global optimal, then the algorithm may change incorrectly, converging to local goals. Furthermore, the PIO technique removes halved of the pigeons with lesser fitness in all iterations, leading to a condensed populace range after some iterations. So the space of solution converts restricted and upsurges the probability of dropping into local goals. To find out these restrictions, a chaos and reverse tactic is presented at the time of initialization, which will improve the arbitrariness of the produced first solution and extend the attention of the solution area. Moreover, a variable named failure count (FC) is presented in this iteration procedure. If the value of FC beats a pre-defined threshold of MFC, then a Cauchy perturbation redistribution tactic has been utilized to annoy the global finest solution, thus averting early convergence.

Chaos movement is impelled by its characteristic outlines, which can navigate every path within a definite array without reiteration or crossing. By employing chaos movement, an expanded early pigeon can be produced, efficiently averting early convergence at the time of optimization. The dual general models for making chaotic variables are Tent Map and Logistic. When compared to the Logistic method, the Tent Map delivers a larger convergence and quicker iteration velocity that is definite as

$$X_{n+1} = \mu \times (1 - 2 \times |X_n - 0.5|) n = 0,1,2,\dots,N \tag{19}$$

Whereas, $0 < X_0 < 1$ is produced utilizing the function of $rand$. By choosing $\mu = 1$, the mapping leftovers in the fully chaotic condition, $X_n \in (0,1)$. Applying this technique, randomly generate numbers amid [0,1]. Next, dependent upon the solution space $[S_{\min}/S_{\max}]$ of the issue and the dimension D, the equivalent individual initialize Eq. (19) can be changed as

$$S_{i,j} = S_{\min,j} + X_n \times \big(S_{\max,j} - S_{\min,j}\big) j = 1,2,\dots,D \tag{20}$$

Here, $S_{i,j}$ signifies the jth dimension of $the\ ith$ individual in the population; $S_{\min}$ and $S_{\max}$ denote the lower and upper limits, correspondingly. While utilizing the chaos model improves the assortment of the early populace, there stays a definite amount of arbitrariness, and the convergence of the solution space may not be optimum. So, an inverse tactic has been executed to develop the initialize procedure additionally, to transport the preliminary values nearer to the global optimal. So, an elite collection tactic is used dependent on the existing and inverse solution to produce an early pigeon nearer to the global optimal. The backward point explanation is:

During this D-dimensional area, $S = (X_1, X_2, \dots, X_D)$ is employed to signify a fact in space. Here, $X_1, X_2, \dots, X_D \in R$ and $X_i \in [a_i, b_i] \forall i \in \{1,2,\dots,D\}$. The reverse point $\hat{S} = (\hat{X}_1, \hat{X}_2, \dots, \hat{X}_D)$ relates to every space point that stated as

$$\hat{X}_i = a_i + b_i - X_i \tag{21}$$

For the early population produced over chaotic movement, the reverse point $\hat{S}$ equivalent to every individual S has been calculated. Then, these reverse points were replaced in the FF, $f(\Delta)$ to compute the fitness value of every individual. A lesser value of fitness specifies a greater solution. If $f(\hat{S}) \leq f(S)$ is lesser than S, then the individuals are substituted by the reverse point S, or else, the original individual stays unmoved. The early solution has been

improved by iterative equating the fitness value with their equivalent symmetric points and uniting the similar with the elite choice tactic.

D. Cauchy Perturbation Redistribution Strategy

In this stage, the population inclines to travel near the midpoint of the superior individual at the time of landmark operator, resulting in great converge velocity. Nevertheless, the distance among pigeons reduces and maximum entities collect within a definite array, so their speeds decline and the model acquires fixed local goals. To overwhelm this restraint, a Cauchy perturbation redistribution tactic has been presented to interrupt the global finest solution, compelling the entities to endure progressing and outflow from the global bests.

The function of Cauchy likelihood density has been expressed below

$$f(x; x_0, \gamma) = \frac{1}{\pi\gamma[1 + \left(\frac{x - x_0}{\gamma}\right)^2]} = \frac{1}{\pi}\left[\frac{\gamma}{(x - x_0)^2 + \gamma^2}\right] \quad (22)$$

Additionally, the function of Cauchy distribution is definite as

$$F_t(x) = \frac{1}{2} + \frac{1}{\pi}\arctan\left(\frac{x}{t}\right) \quad (23)$$

Here, x_0 signifies the position parameter; γ embodies the scale parameter. Dissimilar values of x_0 and γ resemble diverse functions of probability density. In this paper, the values of $\gamma = 1$ and $x_0 = 0$ are selected to attain considerably dissimilar function values in a smaller array of independent parameters. Next, the Cauchy perturbation is employed for the global optimal solutions.

$$X_g = X_g + C(x_0, \gamma) \times (ub - lb) \quad (24)$$

Whereas $C(x_0, \gamma)$ epitomizes randomly generated values; X_g signifies the global best solution; lb and ub signify the lower and upper limitations of the optimizer issue, correspondingly. The process includes numerous stages after gaining the novel X_g. As an initial stage, it must be verified if the perturbed co-ordinate of this aspect decreases within the definite limits. If it beats the limits, the coordinates must be the same. Or else, if it lies in the limits, the fitness must be equated with the global finest solution of the original. If the solution of perturbed is superior, then the original finest global solution is upgraded, and then the value of FC is changed to 0. Lastly, dependent upon the fitness position, the underperforming half of the population has been reorganized, uniting near the recently upgraded global finest location.

The EPIO approach originates an FF to reach higher classification competence. It delineates a positive number to illustrate the greater candidate solutions. Here, the declining of the classifier error is considered as the FF,

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{N\ of\ misclassified\ samples}{Total\ No.of\ samples} * 100 \quad (25)$$

4. Result Analysis and Discussion

The performance analysis of the BCMHDL-IDSSN approach is inspected in the Kaggle dataset [23]. It includes 126238 samples with two class labels as portrayed in Table 1.

Table 1: Dataset description

Class	No. of Instances
Normal	65495
Attack	60743
Total No. of Instances	126238

Fig. 3 exemplifies the confusion matrices made by the BCMHDL-IDSSN technique at 80:20 and 70:30 TRAS/TESS. The outputs pointed out that the BCMHDL-IDSSN method has active recognition of the attack and normal samples at all class labels.

Table 2 and Fig. 4 portray a wide-ranging classifier outcome of the BCMHDL-IDSSN technique on 80:20TRAS/TESS data. These experimentation outcomes highlighted that the BCMHDL-IDSSN technique appropriately detected the normal and attack samples. With 80%TRAS, the BCMHDL-IDSSN system gives an average $accu_y$ of 98.95%, $prec_n$ of 98.98%, $reca_l$ of 98.95%, F_{score} of 98.97%, and MCC of 97.93%. Moreover, with 20%TESS, the BCMHDL-IDSSN approach provides an average $accu_y$ of 99.06%, $prec_n$ of 99.08%, $reca_l$ of 99.06%, F_{score} of 99.07%, and MCC of 98.14%.

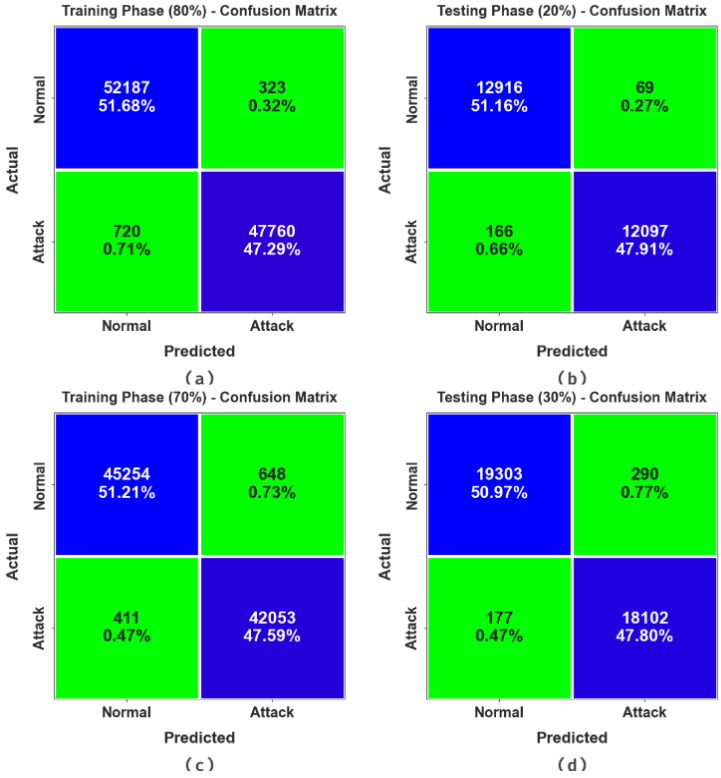

Figure 3. Confusion matrices of (a-c) TRAS of 80:70 and (b-d) TESS of 20:30

Table 2: Classifier outcomes of BCMHDL-IDSSN technique at 80:20TRAS/TESS

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	MCC
TRAS (80%)					
Normal	99.38	98.64	99.38	99.01	97.93
Attack	98.51	99.33	98.51	98.92	97.93
Average	98.95	98.98	98.95	98.97	97.93
TESS (20%)					
Normal	99.47	98.73	99.47	99.10	98.14
Attack	98.65	99.43	98.65	99.04	98.14
Average	99.06	99.08	99.06	99.07	98.14

Table 3 and Fig. 5 examine a comprehensive classifier result of the BCMHDL-IDSSN method at 70:30TRAS/TESS data. These experimentation outcome values emphasized that the BCMHDL-IDSSN method appropriately recognized the normal and attack samples. According to 70%TRAS, the BCMHDL-IDSSN

algorithm attained an average $accu_y$ of 98.81%, $prec_n$ of 98.79%, $reca_l$ of 98.81%, F_{score} of 98.80%, and MCC of 97.60%. Meanwhile, depending on 30%TESS, the BCMHDL-IDSSN system gets an average $accu_y$ of 98.78%, $prec_n$ of 98.76%, $reca_l$ of 98.786%, F_{score} of 98.77%, and MCC of 97.53%.

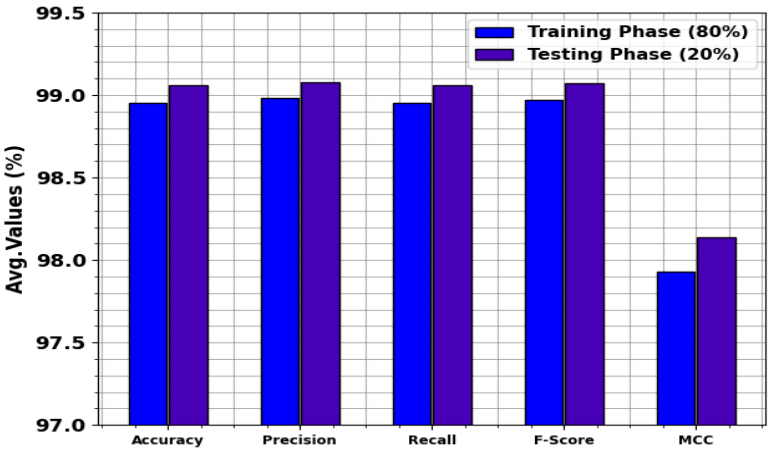

Figure 4. Average of BCMHDL-IDSSN method at 80:20TRAS/TESS

Table 3: Classifier result of BCMHDL-IDSSN system at 70:30TRAS/TESS

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	MCC
TRAS (70%)					
Normal	98.59	99.10	98.59	98.84	97.60
Attack	99.03	98.48	99.03	98.76	97.60
Average	98.81	98.79	98.81	98.80	97.60
TESS (30%)					
Normal	98.52	99.09	98.52	98.80	97.53
Attack	99.03	98.42	99.03	98.73	97.53
Average	98.78	98.76	98.78	98.77	97.53

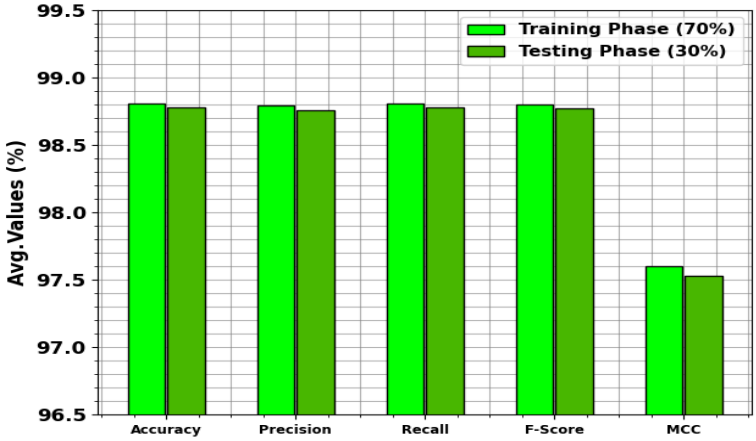

Figure 5. Average of BCMHDL-IDSSN method on 70:30TRAS/TESS

The effectiveness of the BCMHDL-IDSSN method with 80:20TRAS/TESS is illustrated in Fig. 6 under training $accu_y$ (TRAA) and validation $accu_y$ (VALA) curves. The figure displays the performance of the BCMHDL-IDSSN method above numerous epochs, presenting its learning procedure and generalizability. Essentially, the figure displays a continuous enhancement in the TRAA/VALA with development in epoch counts. It confirms the adaptive factor of the BCMHDL-IDSSN technique in the pattern detection on TRA/TES datasets. The boosted tendencies in VALA define the ability of the BCMHDL-IDSSN technique and additionally exceed in offering precise classification on unidentified data, underscoring strong generalizability.

Fig. 7 depicts an overall representation of the training loss (TRLA) and validation loss (VALL) results of the BCMHDL-IDSSN system at 80:20TRAS/TESS above distinct epochs. The increasing minimization in TRLA emphasizes the BCMHDL-IDSSN algorithm improving the weights and reducing the classification error at TRA/TES datasets. The figure identifies the BCMHDL-IDSSN model related to the TRA data, underscoring its superiority in comprehending designs. In addition, the BCMHDL-IDSSN technique steadily improves its parameters in decreasing the discrepancies amongst the forecast and actual TRA classes.

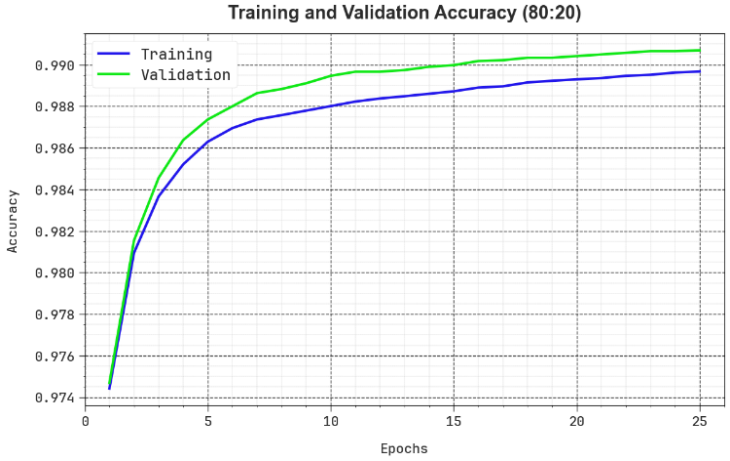

Figure 6. $Accu_y$ Curve of BCMHDL-IDSSN technique at 80:20TRAS/TESS

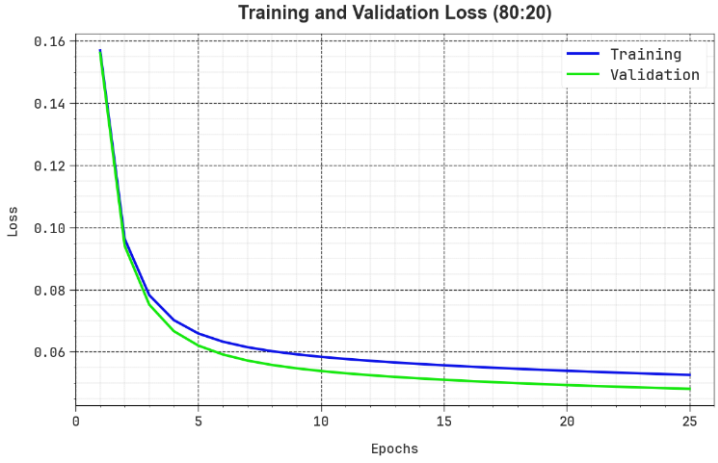

Figure 7. Loss of BCMHDL-IDSSN method at 80:20TRAS/TESS

Fig. 8 examines the classifier outcomes of the BCMHDL-IDSSN system at 80:20 and 70:30. Figs. 8a-8c displays the PR result of the BCMHDL-IDSSN methodology. These experimentation results specified that the BCMHDL-IDSSN system offer maximum values of PR. Similarly, it must be perceptible that the BCMHDL-IDSSN algorithm could gain greater values of PR at each class. In conclusion, Figs. 8b-8d exemplifies the ROC result of the BCMHDL-IDSSN technique. This figure defined that the BCMHDL-IDSSN system gets boosted ROC values. In addition, it is obvious that the BCMHDL-IDSSN technique extends superior ROC values with every class

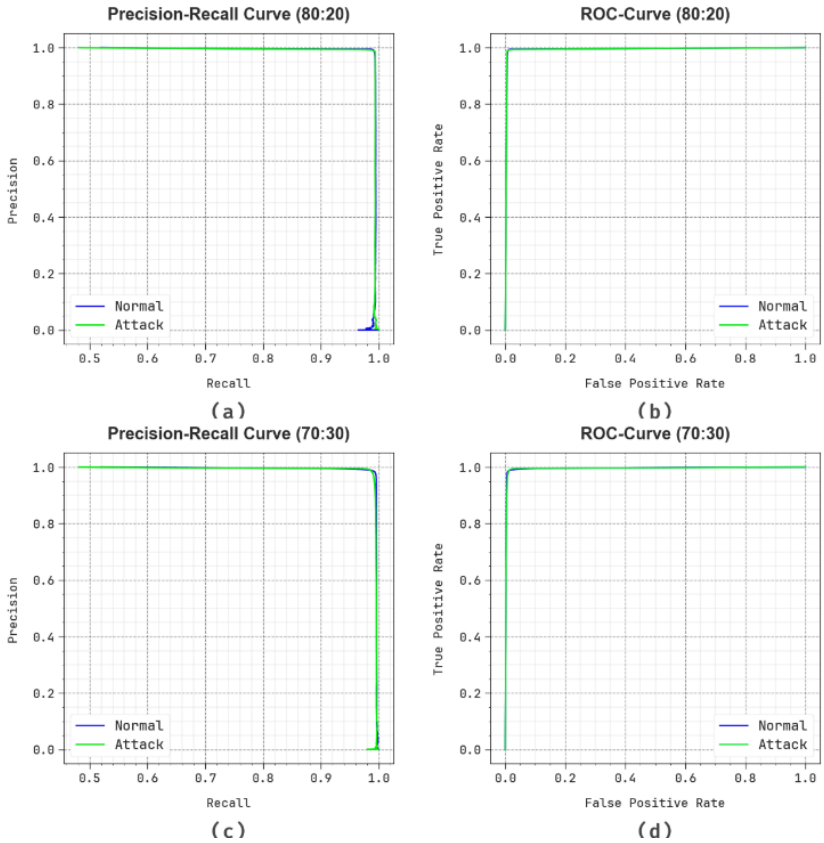

Figure 8. (a-c) PR curve on 80:20 and 70:30 and (b-d) ROC curve on 80:20 and 70:30

Table 4: Comparative outcome of BCMHDL-IDSSN technique with recent algorithms

Methods	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
BCMHDL-IDSSN	99.06	99.08	99.06	99.07
BC-RTHADL	98.98	98.97	98.98	98.98
BSSHN- GBOHDL	98.30	98.35	98.30	98.33
ANN Based IDS	81.44	80.76	81.68	82.28
DELM	93.53	94.76	94.30	93.82
RTS-DELM	94.86	95.21	94.74	94.38
SYD	94.85	96.13	96.43	97.57
DNN	94.52	94.17	95.22	95.96

Table 4 reports an overall comparative result of the BCMHDL-IDSSN technique [24]. These simulated results emphasized that the BCMHDL-IDSSN technique reaches better performance. Based on $accu_y$, the BCMHDL-IDSSN technique obtains an increased $accu_y$ of 99.06% whereas the BC-RTHADL, BSSHN-GBOHDL, ANN-based IDS, DELM, RTS-DELM, SYD, and ANN systems attain diminished $accu_y$ of 98.98%, 98.30%, 81.44%, 93.53%, 94.86%, 94.85%, and 94.52%, correspondingly. Also, based on $prec_n$, the BCMHDL-IDSSN algorithm gets an improved $prec_n$ of 99.08% but, the BC-RTHADL, BSSHN-GBOHDL, ANN-based IDS, DELM, RTS-DELM, SYD, and ANN systems attain minimized $prec_n$ of 98.97%, 98.35%, 80.76%, 94.76%, 95.21%, 96.13%,

and 94.17%. Moreover, with $reca_l$, the BCMHDL-IDSSN approach gets an improved $reca_l$ of 99.06% although, the BC-RTHADL, BSSHN-GBOHDL, ANN-based IDS, DELM, RTS-DELM, SYD, and ANN approach gains minimized $reca_l$ of 98.98%, 98.30%, 81.68%, 94.30%, 94.74%, 96.43%, and 95.22%.

Table 5: CT outcome of BCMHDL-IDSSN technique with recent other methods

Methods	CT (Sec)
BCMHDL-IDSSN	1.98
BC-RTHADL	3.60
BSSHN- GBOHDL	7.86
ANN Based IDS	18.07
DELM	13.65
RTS-DELM	9.53
SYD	11.79
DNN	9.76

Table 5 report an overall comparative computational time (CT) outcome of the BCMHDL-IDSSN method. These simulated outcome values denote that the BCMHDL-IDSSN system gets better performance. As specified with CT, the BCMHDL-IDSSN algorithm acquires minimum CT of 1.98s however, the BC-RTHADL, BSSHN-GBOHDL, ANN-based IDS, DELM, RTS-DELM, SYD, and ANN algorithms provides superior CT of 3.60s, 7.86s, 18.07s, 13.65s, 9.53s, 11.79s, and 9.76s, respectively.

5. Conclusion

In this study, a BCMHDL-IDSSN approach is introduced for smart homes. The BCMHDL-IDSSN method aims to enhance security in the smart home networks. The MHA-BiGRU-based malicious activity recognition and EPIO-based tuning process are the two major processes. In the BCMHDL-IDSSN technique, BC technology is used to achieve security. Besides, the BCMHDL-IDSSN technique involves the design of the MHA-BiGRU technique for the recognition of malicious activities. Finally, the EPIO approach is exploited for the optimum hyperparameter selection of the MHA-BiGRU methodology. A complete set of experiments was applied to validate the performance of the BCMHDL-IDSSN algorithm. The simulation values emphasized that the BCMHDL-IDSSN algorithm gains high efficiency over other techniques.

Funding: "The author gratefully acknowledges technical support provided by the Faculty of Engineering, King Abdulaziz University, Jeddah, Saudi Arabia"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] R. Kairaldeen, N. F. Abdullah, A. Abu-Samah, and R. Nordin, "Data integrity time optimization of a blockchain IoT smart home network using different consensus and hash algorithms," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–23, Nov. 2021.

[2] H. Abdulqadder, D. Zou, and I. T. Aziz, "The DAG blockchain: A secure edge assisted honeypot for attack detection and multi-controller based load balancing in SDN 5G," *Future Generation Computer Systems*, vol. 141, pp. 339–354, Apr. 2023.

[3] T. M. Ghazal, M. K. Hasan, S. N. H. S. Abdullah, K. A. A. Bakar, and H. Al Hamadi, "Private blockchain-based encryption framework using computational intelligence approach," *Egyptian Informatics Journal*, vol. 23, no. 4, pp. 69–75, Dec. 2022.

[4] S. F. Khan, S. S. Priya, M. Soni, I. Keshta, and I. R. Khan, *A Blockchain-Based AI Approach Towards Smart Home Organization Security*, CRC Press, 2024, pp. 589–596.

[5] L. Almuqren et al., “Blockchain-assisted secure smart home network using gradient-based optimizer with hybrid deep learning model,” *IEEE Access*, 2023.

[6] Y. Ren et al., “Multiple cloud storage mechanism based on blockchain in smart homes,” *Future Generation Computer Systems*, vol. 115, pp. 304–313, Feb. 2021.

[7] R. Kumar et al., “A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network,” *Journal of Parallel and Distributed Computing*, vol. 164, pp. 55–68, Jun. 2022.

[8] M. Baza et al., “Privacy-preserving blockchain-assisted private-parking scheme with efficient matching,” *Computers and Electrical Engineering*, vol. 103, Oct. 2022, Art. no. 108340.

[9] W. Meng et al., “Towards blockchain-enabled single character frequency-based exclusive signature matching in IoT-assisted smart cities,” *Journal of Parallel and Distributed Computing*, vol. 144, pp. 268–277, Oct. 2020.

[10] N. Butt et al., “Intelligent deep learning for anomaly-based intrusion detection in IoT smart home networks,” *Mathematics*, vol. 10, no. 23, p. 4598, Dec. 2022.

[11] A. Qashlan, P. Nanda, and M. Mohanty, “Differential privacy model for blockchain-based smart home architecture,” *Future Generation Computer Systems*, vol. 150, pp. 49–63, 2024.

[12] M. M. Khayyat, S. Abdel-Khalek, and R. F. Mansour, “Blockchain-enabled optimal Hopfield chaotic neural network-based secure encryption technique for industrial Internet of Things environment,” *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 11377–11389, 2022.

[13] R. Kumar et al., “Blockchain-based authentication and explainable AI for securing consumer IoT applications,” *IEEE Transactions on Consumer Electronics*, 2023.

[14] E. Rabieinejad, A. Yazdinejad, A. Dehghantanha, and G. Srivastava, “Two-level privacy-preserving framework: Federated learning for attack detection in the consumer Internet of Things,” *IEEE Transactions on Consumer Electronics*, 2024.

[15] A. Kumar et al., “A secure architectural model using blockchain and estimated trust mechanism in electronic consumers,” *IEEE Transactions on Consumer Electronics*, 2023.

[16] A. Sheeba et al., “Secure smart city application using webservice model and Mayfly optimization-based lightweight CNN,” *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 1, p. e4869, 2024.

[17] S. Singh et al., “A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology,” *Future Generation Computer Systems*, vol. 129, pp. 380–388, 2022.

[18] H. Xie et al., “Verifiable federated learning with privacy-preserving data aggregation for consumer electronics,” *IEEE Transactions on Consumer Electronics*, 2023.

[19] S. Menon et al., “Blockchain and machine learning-inspired secure smart home communication network,” *Sensors*, vol. 23, no. 13, p. 6132, 2023.

[20] J. Zhang et al., “Feature fusion text classification model combining CNN and BiGRU with the multi-attention mechanism,” *Future Internet*, vol. 11, no. 11, p. 237, 2019.

[21] Y. Liu et al., “Chinese event subject extraction in the financial field integrated with BiGRU and multi-head attention,” in *Journal of Physics: Conference Series*, vol. 1828, no. 1, p. 012032, Feb. 2021.

[22] M. Liu et al., “Fault recovery of distribution network with distributed generation based on pigeon-inspired optimization algorithm,” *Electronics*, vol. 13, no. 5, p. 886, 2024.

[23] Kaggle Dataset, “NSL-KDD dataset,” available at: https://www.kaggle.com/datasets/hassan06/nslkdd.

[24] F. F. Alruwaili et al., “A decentralized approach to smart home security: Blockchain with red-tailed hawk-enabled deep learning,” *IEEE Access*, 2024.