IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 21 June 2023, accepted 3 August 2023, date of publication 7 August 2023, date of current version 18 August 2023.

*Digital Object Identifier 10.1109/ACCESS.2023.3303087*

RESEARCH ARTICLE

# Blockchain-Assisted Secure Smart Home Network Using Gradient-Based Optimizer With Hybrid Deep Learning Model

**LATIFAH ALMUQREN[1], KHALID MAHMOOD[2], SUMAYH S. ALJAMEEL[3], AHMED S. SALAMA[4], GOUSE PASHA MOHAMMED[5], AND AMANI A. ALNEIL[5]**

[1]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia
[2]Department of Information Systems, College of Science and Art at Mohayil, King Khalid University, Abha 61421, Saudi Arabia
[3]SAUDI ARAMCO Cybersecurity Chair, Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia
[4]Department of Electrical Engineering, Faculty of Engineering and Technology, Future University in Egypt, New Cairo 11845, Egypt
[5]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia

Corresponding author: Khalid Mahmood (kasgr@kku.edu.sa)

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number (RGP2/112/44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R349), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. We Would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project. This study is partially funded by the Future University in Egypt (FUE). This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444).

**ABSTRACT** The Internet of Things (IoT) refers to a technology enabler to enhance the urban physical architecture and render public services. But, public access to accumulated heterogeneous IoT urban information is prone to hackers attacking connected devices to the internet intellectual property as well. IoT security serves a dynamic part in the smart city. Some IoT devices are connected in smart homes, and these connections were centred on gateways. In smart homes, the gateways gain a lot of significance; but their centralized structure causes many security vulnerabilities like availability, integrity, and certification. Unified ''cloud-like'' computing networks and Blockchain (BC) type systems should be used to sort out these problems. Therefore, this article develops a Blockchain-Assisted Secure Smart Home Network using Gradient Based Optimizer with Hybrid Deep Learning (BSSHN-GBOHDL) model. The presented BSSHN-GBOHDL technique employs BC technology to improve the confidentiality of the data in the smart home environment. In addition, the BSSHN-GBOHDL technique identifies malicious activities in the smart home environment via three sub-processes namely data preprocessing, hybrid deep learning (HDL)-based malicious activity classification, and GBO-based hyperparameter tuning. The GBO algorithm assists in the proficient hyperparameter selection of the HDL model, which aids in accomplishing increased detection efficiency. The experimental validation of the BSSHN-GBOHDL approach is tested on a benchmark NSL-KDD dataset with 65495 normal and 60743 attack samples. The results highlight the betterment of the BSSHN-GBOHDL approach over other recent methods with maximum accuracy of 98.29%.

**INDEX TERMS** Smart homes, Internet of Things, blockchain, network security, deep learning, gradient-based optimizer.

## I. INTRODUCTION

The Internet of Things (IoT) is a blooming phenomenon with the progression of technological abilities that brings low-powered devices and ubiquitous connectivity [1]. In simple words, IoT is millions of devices linked to the internet. Such IoT gadgets were memory-limited gadgets that could transmit and collect data over the network without the support of humans [2]. It presents digital intelligence that converts urban services and infrastructures. Smart Home can

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

be referred to as a private home that receives and sends data in real-time. It affords intelligent and automatic services by different home devices namely refrigerators, TVs, and lights [3]. The above-mentioned machines are several home-based communication systems between other environments and devices without the interference of humans. Users handle the usage of many home products to control and monitor themselves as per user settings related to the network configuration of the home [4]. The most significant factor is the IoT and network setting of these smart homes. Above all, the network architecture of the smart home containing embedded computers is linked to numerous IoT gadgets based on the Internet, and the communication shifts to wireless [5]. Unlike how users manipulated all devices, it could be probably able to handle other devices over gateways, both outside and inside the smart home. With the convergence of several industries, hardware advances, and the commercialization of 5G, a more systematic and potential smart home network configuration can be expected [6].

Integrity and confidentiality of data need to be guaranteed, and in smart home networks, the latency and availability of the services rendered to users should be mainly considered while meeting other security concerns [7]. To accommodate the complexities of smart home networks, the manageability and scalability of systems have to be considered. In recent times, Blockchain (BC) has become a desirable one and was used in most of the next-generation applications to deliver security on a large number of platforms, namely smart city, IoT, etc. The reason behind this is the BC, which presents trust-free and decentralized solutions [8], where online-distributed ledgers were utilized to save data over the network in a decentralized manner. Existing techniques make use of a signature-based technique to detect exceptional arrangements and for this underlying problem [9]; a comprehensive Intrusion Detection System (IDS) emerges as a potential solution. Managing smart BC-based applications becomes significant by developing versatile and powerful methods for processing this vast volume of data. Machine learning (ML) includes machines for reasoning, training, and performing without interference from humans [10]. The core objective of ML is to build a productive algorithm to extract data from input, make predictions, and change outputs over statistical analysis. ML can process a large amount of data and take decisions guided by evidence.

This article develops a Blockchain Assisted Secure Smart Home Network using Gradient Based Optimizer with Hybrid Deep Learning (BSSHN-GBOHDL) model. The presented BSSHN-GBOHDL technique employs BC technology to improve the confidentiality of the data in the smart home environment. In addition, the BSSHN-GBOHDL technique identifies malicious activities in the smart home environment via three sub-processes namely data preprocessing, HDL-based malicious activity classification, and GBO-based hyperparameter tuning. The performance validation of the BSSHN-GBOHDL approach was tested on a benchmark dataset.

## II. RELATED WORKS

In [11], a private BC-based smart home network structure to estimate IDS enabled with the Fused Real-Time Sequential Deep ELM (RTS-DELM) method was presented. This paper establishes the presented technique in BC-based smart homes for detecting some malicious actions. Yakub et al. [12] present a lightweight authentication process which allows safe D2D interfaces in smart homes. The Ethereum BC allows the execution of decentralized prototypes and P2P distributed ledger scheme. Al-Qarafi et al. [13] establish an OMLIDS-PBIoT approach abbreviated as Optimal ML-based IDS for Privacy-Preserving BIoT with Smart City Environment. In achieving that, the projected OMLIDS-PBIoT system utilizes data pre-processed in a primary step for converting data into compatible design. Besides, a golden eagle optimizer (GEO)-oriented FS technique was planned for deriving suitable feature subsets.

Sohail et al. [14] present a method which assumes either the problems of explainability of the ANN approach and hyperparameter selective for this method that is simply trusted and modified by consumers of smart home applications. Besides, this method assumes a subset of the database to better hyperparameter selection to decrease the overhead of the procedure of ANN structure. Azumah et al. [15] introduces a new DL-based AD technique for predicting cyber-security on smart home IoT network device and learn novel outliers as it appears over time utilizing IoT network intrusion databases. The presented method was dependent upon a long-term memory structure that attains an important accuracy enhancement related to the recent AD methods for IoT networks from smart homes. Babu et al. [16] examined a permission-based BC scheme which utilizes the arbiter PUF method for securing the important pairs of IoT gadgets utilizing lightweight machinery. A collaborative detection method was primarily utilized for detecting DDoS on IoT gadgets utilizing the ML-based ensemble approach that offers a minimum FPR and optimum detection rate than the other classifier method. Cheema et al. [17] introduce distributed ML-oriented IDS in IoT exploiting BC technology. Specifically, spectral partitioning has been projected for separating the IoT network as autonomous systems (AS) permitting traffic monitoring for IDS that is applied by the selective AS border region nodes from distributed systems. The IDS depends on ML, but the SVM system has been trained to exploit well-known IoT databases and the detection of attackers is presented.

In [18], the BC-enabled IDS was established in this work dependent upon the Battle Royale Dingo optimizer (BRDO) focused on the deep stacked network method. At present, a deep stacked network was executed to detect the intrusion, and it can be trained depending on the optimizer system to improve detection efficiency. Yang and Wang [19] progress a privacy-preserving distributed method which allows users to optimally control their energy usage in parallel using the smart contract on BC. In [20], an effectual BC-Assisted Cluster-based IDS for IIoT, named as BAC-IDS system was developed. The presented BAC-IDS approach

purposes to cluster IIoT devices to detect intrusions and enable BC-based secure data broadcast. Abdel-Basset et al. [21] present a federated DL-based IDS (FED-IDS) to effectively identify attacks by offloading the learning method in the server to distributed vehicular edge nodes. FED-IDS establishes a context-aware transformer network for learning spatial-temporal representations of vehicular traffic flows needed to classify distinct types of attacks. Katib and Ragab [22] propose a hybrid Harris Hawks with sine cosine and DL-based IDS (H3SC-DLIDS) for the BC-enabled IoT platform. The purpose of the projected H3SC-DLIDS system is to identify the occurrence of DDoS attacks from the BC-assisted IoT platform.

## III. THE PROPOSED MODEL

In this article, we have introduced a new BSSHN-GBODHL approach for optimal identification of malicious activities in the smart home environment. Besides, the presented BSSHN-GBOHDL technique exploited the BC technology for enhancing the confidentiality of the data in the smart home environment. Moreover, the BSSHN-GBOHDL technique identifies malicious activities in the smart home environment via three sub-processes namely data preprocessing, HDL-based malicious activity classification, and GBO-based hyperparameter tuning. Fig. 1 represents the overall flow of the BSSHN-GBODHL method.

### A. BC TECHNOLOGY

The utility of a BC-based system can be smoother by using the computational technology of BSSHN-GBOHDL [23]. The data confidentiality is improvised while applying the BSSHN-GBOHDL distributed BC technology. Also, the BSSHN-GBOHDL model is used for increasing the pace at which comprehension can be accomplished by further interchanging knowledge, thus enhancing understanding. It provides the network structure and framework to design a decentralized BC application. The study analyzes the deployment of the BSSHN-GBOHDL structure, which was an advanced mechanism. The appropriate usage of this technology is to gather experience from various sources of data like mobile devices, IoT systems, and sensors. Knowledge is derived by using this technique for smart applications. The BC was the basic feature of smart applications. Nevertheless, for inspection, the BSSHN-GBOHDL technique is utilized for evaluating and forecasting real-time information. Also, the BC process every piece of information from the BSSHN-GBOHDL architecture. The BC technology focuses on the edge of IoT and includes 3 key components: knowledge architecture, the BC layer, the BSSHN-GBOHDL infrastructure, and smart contracts. In this work, several activating mechanisms, large numbers of hidden layers, and hidden neurons were used for optimizing the security and privacy of smart homes. In the proposed method, there are three different stages in analyzing the information: the data preprocessing, assessment, and acquisition phases. The evaluation layer was composed of two sublayers: the performance and prediction layers. Accurate information is attained from actuators and sensors for the analysis. Next, the information is provided as raw data and utilized by the collection layer. In the preprocessing layer, a wide-ranging method for data cleaning and preparing were used for removing discrepancy. The BSSHN-GBOHDL model is implemented to increase home network protection by avoiding invasive or disruptive applications. We present the following explanation to illuminate how BCs contribute to secured access.

- First, the user has to determine the access level and added it to the home service computer. For instance, at the maximum level, the Admin (owner) was permissible, whereas youths, teenagers, adolescents, and visiting relatives require mid-level permission.
- For a consumer who is authorized to access smart homes and was utilizing applications inside.
- Visitors and relatives have comparatively poor access permits. While processing a request from a user, the home server checks the security access to the repository. By getting an order from the client, the home server transfers the encoded password and username to the BC layer.
- For user and implementation, a BC regulation header has a collection of authorization rules.

### B. DATA PREPROCESSING

Standardization is the transforming process that converts variables applied in this study to one with a standard deviation of 1 and a mean of 0. The equation is as follows:

$$x_{standardization} = \frac{x - mean(\ )}{standard\ \ deviation} \tag{1}$$

X is the value that should be normalized. Mean indicates the arithmetic means of the distribution. Standard deviation denotes the standard deviation of the distribution.

### C. HDL-BASED CLASSIFICATION

For the identification of malicious activities in the smart home environment, the HDL model is used. LSTM is a kind of RNN which has the potential to learn long-term dependency and is built to resolve the issue of long-term dependency using short-term memory tools [24]. LSTM can progress data up to the long sequence without vanishing gradient; presently, LSTM is widely applied for encountering the case of data sequences such as recognition of speech, images' automatic annotation, and processing of natural language. LSTM possess dual property value, the former is the state of hidden $H(t)$ which is cell value modified according to the consumed time and the latter is the cell state $C(t)$ that provides long-term memory, the cell state changes in horizon form with LSTM cell top line in the brown rectangular box. LSTM is capable of erasing or adding data in the state of the cell. The forget gate $F(t)$ preserves the input connection $X(t)$ and the previous hidden state $H(t-1)$ to the cell state $C(t)$; this enables the cell to memorize or forget X(t) and H(t-l) at the required time. Moreover, the input gate $I(t)$ and $\hat{I}(t)$ selects either to pass

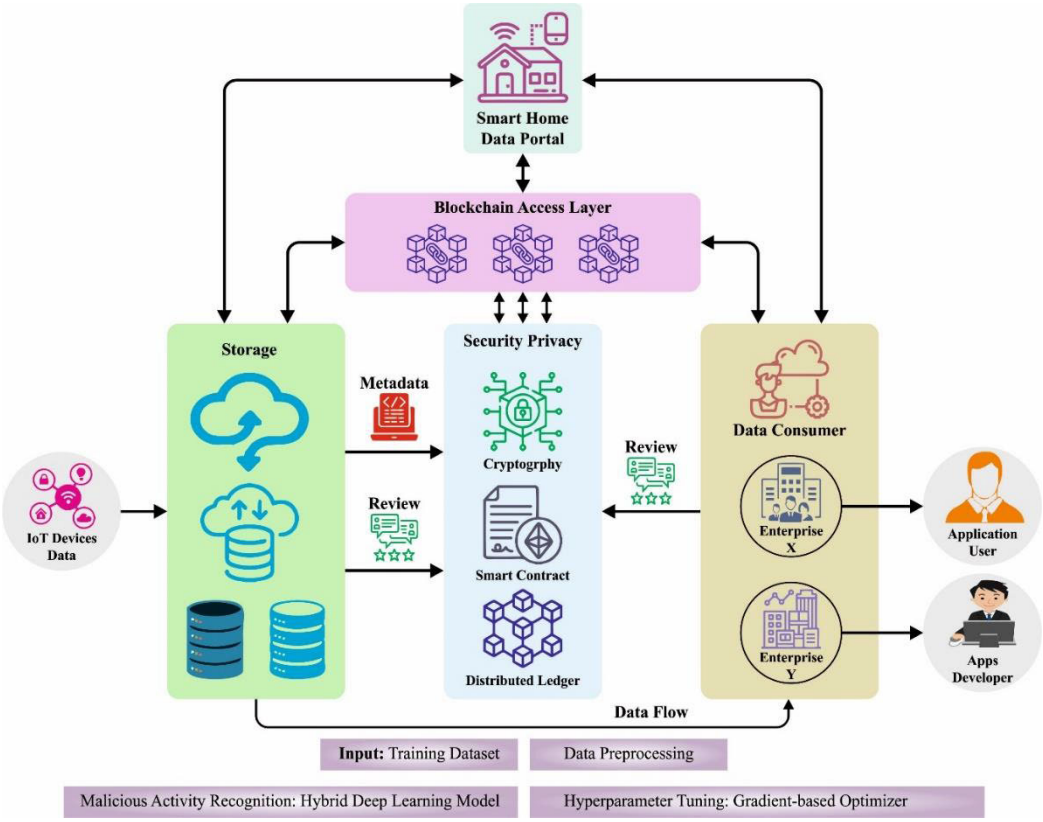


**FIGURE 1.** Overall flow of the BSSHN-GBODHL approach.

or not the input values towards the cell state $C(t)$. The output gate $O(t)$ selects the exit relies on the cell state $C(t)$

$$F(t) = \sigma\left(W_f\left[H(t-1), X(t)\right] + B_f\right), \quad (2)$$

$$I(t) = \sigma\left(W_i\left[H(t-1), X(t)\right] + B_i\right), \quad (3)$$

$$O(t) = \sigma\left(W_O\left[H(t-1), X(t)\right] + B_O\right), \quad (4)$$

$$I(t) = tanh\left(W_i\left[H(t-1), X(t)\right] + B_i\right), \quad (5)$$

$$C(t) = F(t).C(t-1) + I(t).I(t), \quad (6)$$

$$H(t) = WO(i).\tanh\left(C(t)\right), \quad (7)$$

From the expression, *tanh* shows the hyperbolic tangent function, $\sigma$ denotes the sigmoid function $B$ and $W$ represents the weight matrix, correspondingly. It may be considered that the accurate input dataset and internal state control, which reflect in the cell state from LSTM's features, can able to progress according to the fixed- and variable-length dataset at the entrance and exit. This benefit is more significant if LSTM was applied together with other types of DNN than standalone LSTM.

A hybrid method was a combination of many techniques to proficiently solve an issue. This method was built for offering better accuracy compared to the investigated DL and ML prediction methods. This method was devised for classification. This technique has numerous layers of LSTM and CNN. CNN can cause several helpful features for ensuring potential prediction related to the kernel size that chooses from the input data. Moreover, conversely, LSTM can potentially denote long-term data progress in the input dataset; yet, it was not capable of removing the input's dynamic features, which is required in predicting as potentially as CNN. In the HDL method, the CNN technique captured the feature vectors, and outcomes were used as input datasets for the LSTM layer to learn and augment prediction methods related to the historical time series input dataset.

### D. GBO-BASED HYPERPARAMETER TUNING

In this work, the GBO model is used for the optimal hyperparameter tuning of the HDL method. GBO is a metaheuristic algorithm that depends on gradient information and population [25]. Despite new members of MAs, GBO was employed to various problems since its introduction.

GBO begins parameter initialization with the majority of *MAs*. Thus, GBO involves the $nP$ amount of vector agents in an $nV$-dimension space that is initialized by the following expression:

$$X_{n,d} = [X_{n,1}, X_{n,2}, \ldots, X_{n,d}], \quad n = 1, 2, \ldots, nPd = 1, 2, \ldots, nV. \quad (8)$$

The initialization in every population is expressed by.

$$X_n = X_{\min} + rand\,(0, 1) \times (X_{\max} - X_{\min}), \quad (9)$$

where $X_{\max}$ represent the maximum population, $X_{\min}$ denotes the minimal of decision parameters $X$, and rand (0, 1) indicates the random integer within [0, 1].

As abovementioned, the GBO begins with a random initial population and later upgrades every solution based on gradient specified direction. During the exploration stage, a random variable $\rho_1$ is applied:

$$\rho_1 = 2 \times rand \times \alpha - \alpha, \tag{10}$$

$$\alpha = \left|\beta \times \sin\left(\frac{3\pi}{2} + \sin\left(\beta \times \frac{3\pi}{2}\right)\right)\right|, \tag{11}$$

$$\beta = \beta_{\min} + (\beta_{\max} - \beta_{\min}) \times \left(1 - \left(\frac{m}{M}\right)\right), \tag{12}$$

where $M$ represents the overall iterations,s $\rho_1$ denotes a function decided by $\alpha, \alpha$ changes based on $\beta$, *rand* indicates an arbitrarily selected number from zero to one, $\beta_{\min}$ is equivalent to 0.2 and $\beta_{\max}$ is equivalent to 1.2, and $m$ means the present calculation numbers.

The gradient search rule (GSR) is outlined by the Newton's gradient. It makes the GBO technique random through iteration and it can be expressed as follows

$$GSR = randn \times \frac{2\Delta x \times x_n}{(x_{worst} - x_{best} + \varepsilon)}, \tag{13}$$

In Eq. (13) $\varepsilon$ represents a random value from zero to one, $\Delta x$ is the difference between the optimum solution $(x_{best})$ and a present solution $(x_{r1}^m)$, $x_{best}$ denotes the better solution, *randn* shows the random integer, and $x_{worJt}$ shows the worst solution. The computation of GSR is exploited by Eq. (14).

$$GSR = randn \times \rho_1 \times \frac{2\Delta x \times x_n}{(x_{worst} - x_{best} + \varepsilon)}. \tag{14}$$

To change $\Delta x$ via iteration, $\delta$ is determined in the following. The computation of $\Delta x$ is formulated as.

$$\Delta x = rand\,(1:N) \times |step|, \tag{15}$$

$$step = \frac{(x_{best} - x_{r1}^m) + \delta}{2}, \tag{16}$$

$$\delta = 2 \times rand \times \left(\left|\frac{x_{r1}^m + x_{r2}^m + x_{r3}^m + x_{r4}^m}{4} - x_n^m\right|\right) \tag{17}$$

where $r1$, $r2$, $r3$ and $r4$ indicate randomly selected from [1, $N\rfloor$, $rand(1{:}N\forall)$ signifies a vector with $N\forall$ dimensions, and *step* can be evaluated as Eq. (16).

The GBO exploits directed movement (DM), which converges the local search of $x_n$. The computation can be given as follows.

$$DM = rand \times \rho_2 \times (x_{best} - x_n), \tag{18}$$

In Eq. (18), *rand* indicates a uniformly distributed value from zero to one, $\rho_2$ denotes a random variable, and the formula of $\rho_2$ can be given as follows.

$$\rho_2 = 2 \times rand \times \alpha - \alpha. \tag{19}$$

Eventually, based on the term, the formula of GSR is calculated as.

$$x1_n^m = x_n^m - GJR + DM, \tag{20}$$

$$x1_n^m = x_n^m - randn \times \rho_1 \times \frac{2\Delta x \times x_n^m}{(x_{worst} - x_{best} + \varepsilon)} + rand \times \rho_2 \times \left(x_{b_{\theta JI}} - x_n^m\right), \tag{21}$$

where $x1_n^m$ denotes the new vector acquired by $x_n^m$. Integrating with GSR and $DM$, the new solution is computed in the iteration randomly.

Additionally, the vector $x_n^m$ takes the place of optimum solution $x_{best}$, and a novel vector $x2_n^m$ is computed as follows.

$$x2_n^m = x_{best} - randn \times \rho_1 \frac{2\Delta x \times x_n^m}{(x_{worst} - x_{best} + \varepsilon)} + rand \times \rho_2 \times \left(x_{r1}^m - x_{r2}^m\right). \tag{22}$$

The GBO method improves global search in the exploration level depending on Eq. (21) and improves the local search in the exploitation level depending on Eq. (22). As per the preceding vector $x1_n^m$ and $x2_n^m$, the novel solution to $x_n^{m+1}$ is generated in the following.

$$x3_n^m = x_n^m - \rho_1 \times \left(x2_n^m - x1_n^m\right), \tag{23}$$

$$x_n^{m+1} = r_a \times \left(r_b \times x1_n^m + (1 - r_b) \times x2_n^m\right) + (1 - r_a) \times x3_n^m, \tag{24}$$

where $r_a$ and $r_b$ denote uniform numbers within [0, 1].

The local escaping operator (LEO) was proposed in the original GBO to accelerate the convergence rate and prevent getting trapped in local optima. The newest solution to $X_n^{m+1}$ is produced by the LEO operator, with different solutions (two solutions $x_{r1}^m$ and $x_{r2}^m$, the optimum solution $x_{b_{\theta JI}}$, a randomly obtained solution $x_k^m$, and the random solution $X1_n^m$ and $X2_n^m$). The formula of GSR meets the specific condition and updates the effective existing solution. The description of $pr$ is a probability value, which decides the probability of GSR. The LEO can be executed by the subsequent equation.

$$X_n^{m+1} = X_n^{m+1} + f_1 \times (u_1 \times x_{best} - u_2 \times x_k^m) + f_2 \times \rho_1 \times \frac{u_3 \times \left(X2_n^m - X1_n^m\right) + u_2 \times \left(x_{r1}^m - x_{r2}^m\right)}{2} rand < 0.5, \tag{25}$$

$$X_n^{m+1} = x_{best} + f_1 \times \left(u_1 \times x_{best} - u_2 \times x_k^m\right) + f_2 \times \rho_1 \times \frac{u_3 \times \left(X2_n^m - X1_n^m\right) + u_2 \times \left(x_{r1}^m - x_{r2}^m\right)}{2} rand\ 0.5, \tag{26}$$

where $u_1, u_2,$ *and* $u_3$ denote three random values, which can be defined in the following, $f_1$ denotes a uniformly distributed number from $-1$ to 1, $f_2$ is similar to $f_1$, and.

$$u_1 = L_1 \times 2 \times rand + (1 - L_1), \tag{27}$$

$$u_2 = L_1 \times rand + (1 - L_1), \tag{28}$$

$$u_3 = L_1 \times rand + (1 - L_1), \tag{29}$$

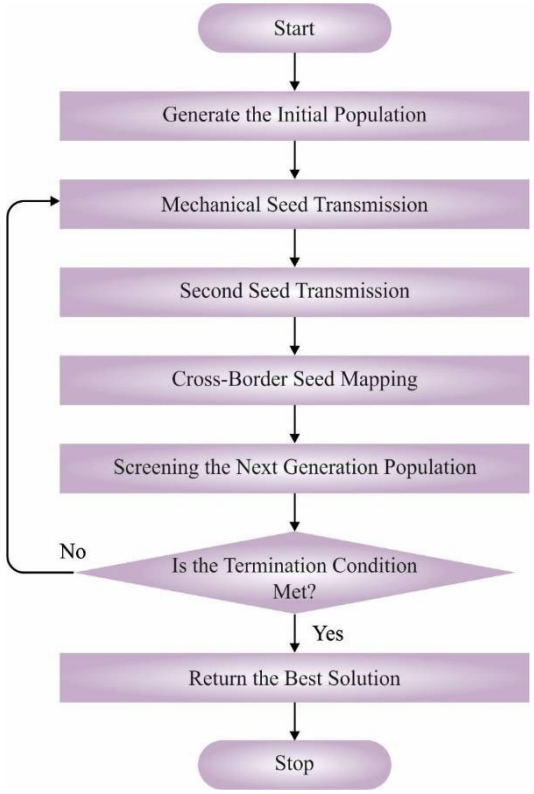


**FIGURE 2.** Flowchart of GBO.

where *rand* denotes a parameter ranging from zero to one, and $L_1$ denotes the binary number, either 0 or 1. Fig. 2 illustrates the flowchart of GBO.

The preceding solution $x_k^m$ can be described using Eq. (30), $x_{p^m}$ shows a randomly selected solution and $x_{rand}$ represent the uniform value between 0 and 1.

$$x_k^m = \begin{cases} x_{rand} & u_2 < 0.5 \\ x_p^m & otherwise, \end{cases} \tag{30}$$

$$x_{rand} = X_{min} + rand \times (X_{max} - X_{min}). \tag{31}$$

The fitness selection serves as a significant component in the GBO technique. Solution encoding is used to assess the candidate solution's goodness. Herein, the accuracy value was the main condition applied to develop a fitness function.

$$Fitness = \max(P) \tag{32}$$

$$P = \frac{TP}{TP + FP} \tag{33}$$

Here, FP signifies the false positive value and TP denotes the true positive.

## IV. RESULTS AND DISCUSSION

In this section, the experimental results are investigated on the NSL-KDD dataset [26], comprising 126238 samples and two class labels as represented in Table 1.

The confusion matrices of the BSSHN-GBOHDL technique on malicious attack recognition are shown in Fig. 3.

**TABLE 1.** Details of dataset.

| Class | No. of Samples |
|---|---|
| Normal | 65495 |
| Attack | 60743 |
| Total No. of Samples | 126238 |

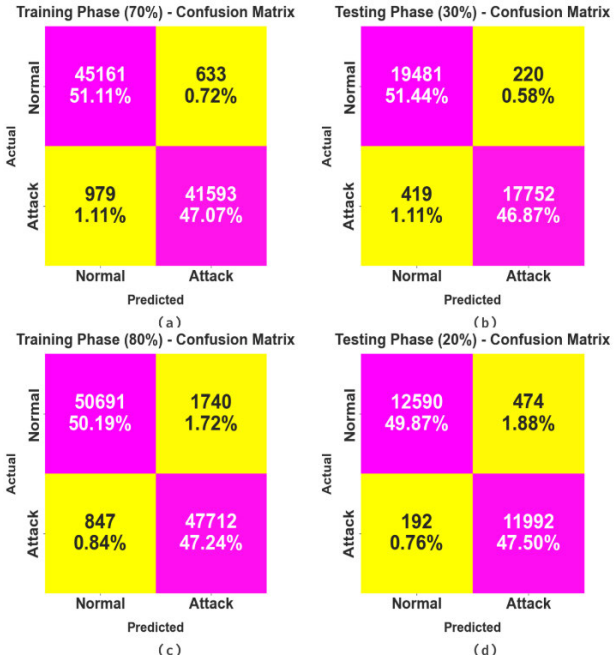


**FIGURE 3.** Confusion matrices of BSSHN-GBOHDL approach (a-b) 70:30 of TRP/TSP and (c-d) 80:20 of TRP/TSP.

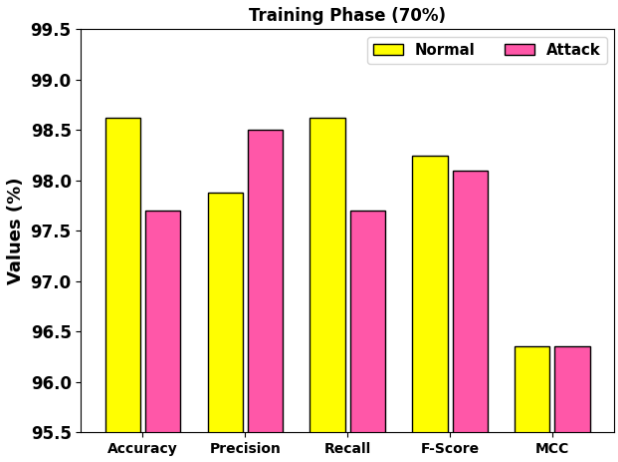


**FIGURE 4.** Classifier outcome of BSSHN-GBOHDL approach on 70% of TRP.

The figure indicates the accuracy of the BSSHN-GBOHDL technique on the identification of normal and attack samples.

In Table 2, the overall results of the BSSHN-GBOHDL technique under 70:30 of TRP/TSP are reported. Fig. 4

**TABLE 2.** Classifier outcome of BSSHN-GBOHDL approach on 70:30 of TRP/TSP.

| Class | $Accu_y$ | $Prec_n$ | $Reca_l$ | $F_{score}$ | MCC |
|---|---|---|---|---|---|
| Training Phase (70%) | | | | | |
| Normal | 98.62 | 97.88 | 98.62 | 98.25 | 96.35 |
| Attack | 97.70 | 98.50 | 97.70 | 98.10 | 96.35 |
| Average | 98.16 | 98.19 | 98.16 | 98.17 | 96.35 |
| Testing Phase (30%) | | | | | |
| Normal | 98.88 | 97.89 | 98.88 | 98.39 | 96.62 |
| Attack | 97.69 | 98.78 | 97.69 | 98.23 | 96.62 |
| Average | 98.29 | 98.34 | 98.29 | 98.31 | 96.62 |

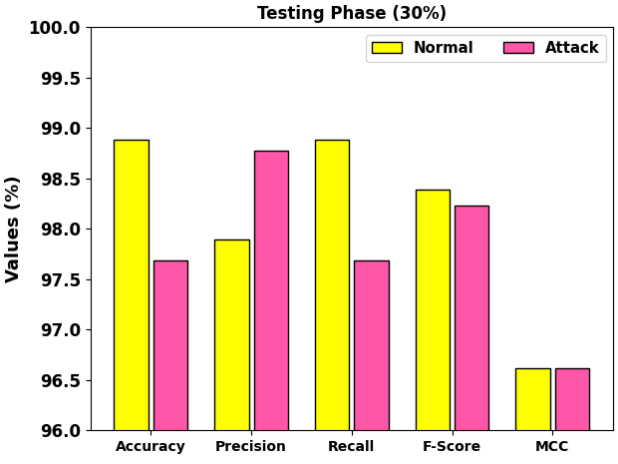


**FIGURE 5.** Classifier outcome of BSSHN-GBOHDL approach on 30% of TSP.

represents the classifier outcome of the BSSHN-GBOHDL approach under 70% of TRP. The results identify that the BSSHN-GBOHDL technique recognizes normal and attack samples proficiently. In addition, it is noticed that the BSSHN-GBOHDL technique attains an average $accu_y$ of 98.16%, $prec_n$ of 98.19%, $reca_l$ of 98.16%, $F_{score}$ of 98.17%, and MCC of 96.35%.

Fig. 5 signifies the classifier outcome of the BSSHN-GBOHDL technique under 30% of TSP. The results identify that the BSSHN-GBOHDL system recognizes normal and attack samples proficiently. As well, it is noted that the BSSHN-GBOHDL method attains an average $accu_y$ of 98.29%, $prec_n$ of 98.34%, $reca_l$ of 98.29%, $F_{score}$ of 98.31%, and MCC of 96.62%.

In Table 3, the overall results of the BSSHN-GBOHDL method under 80:20 of TRP/TSP are reported. Fig. 6 denotes the classifier outcome of the BSSHN-GBOHDL algorithm under 80% of TRP. The results show that the BSSHN-GBOHDL method recognizes normal and attack samples proficiently. Moreover, the BSSHN-GBOHDL approach attains an average $accu_y$ of 97.47%, $prec_n$ of 97.42%, $reca_l$ of 97.47%, $F_{score}$ of 97.44%, and MCC of 94.89%.

Fig. 7 represents the classifier outcome of the BSSHN-GBOHDL approach under 20% of TSP. The figure exhibits

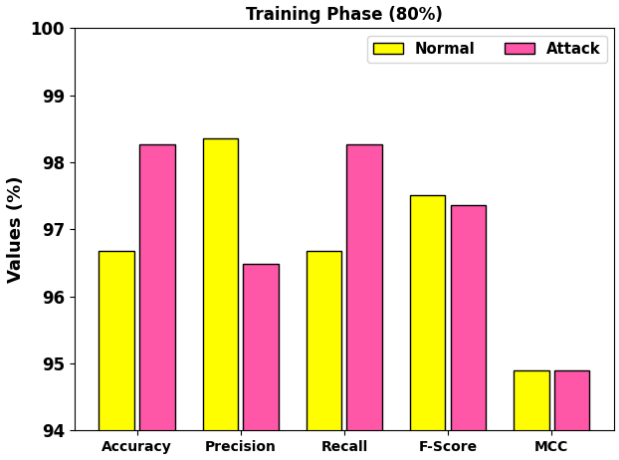


**FIGURE 6.** Classifier outcome of BSSHN-GBOHDL approach on 80% of TRP.

**TABLE 3.** Classifier outcome of BSSHN-GBOHDL approach on 80:20 of TRP/TSP.

| Class | $Accu_y$ | $Prec_n$ | $Reca_l$ | $F_{score}$ | MCC |
|---|---|---|---|---|---|
| Training Phase (80%) | | | | | |
| Normal | 96.68 | 98.36 | 96.68 | 97.51 | 94.89 |
| Attack | 98.26 | 96.48 | 98.26 | 97.36 | 94.89 |
| Average | 97.47 | 97.42 | 97.47 | 97.44 | 94.89 |
| Testing Phase (20%) | | | | | |
| Normal | 96.37 | 98.50 | 96.37 | 97.42 | 94.75 |
| Attack | 98.42 | 96.20 | 98.42 | 97.30 | 94.75 |
| Average | 97.40 | 97.35 | 97.40 | 97.36 | 94.75 |

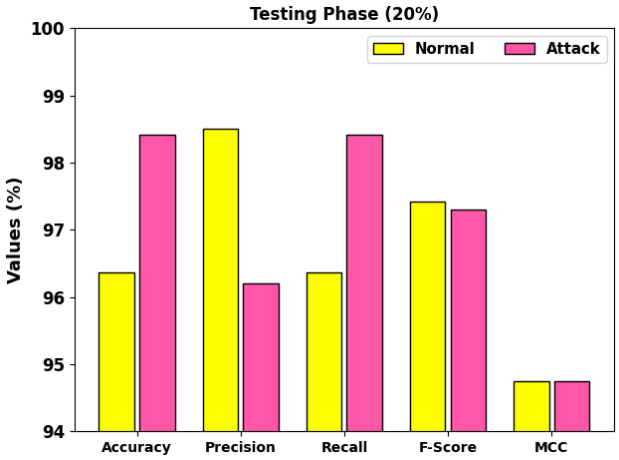


**FIGURE 7.** Classifier outcome of BSSHN-GBOHDL approach on 20% of TSP.

that the BSSHN-GBOHDL technique recognizes normal and attack samples proficiently. In addition, the BSSHN-GBOHDL method gains an average $accu_y$ of 97.40%, $prec_n$ of 97.35%, $reca_l$ of 97.40%, $F_{score}$ of 97.36%, and MCC of 94.75%.

Fig. 8 demonstrates the classifier results of the BSSHN-GBOHDL technique under 70:30 and 80:20 of

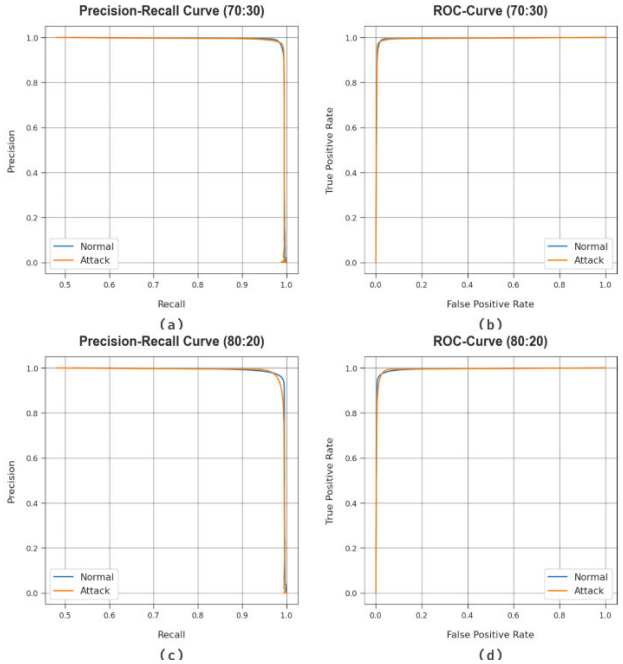


**FIGURE 8.** (a-c) PR curve of 70:30 and 80:20; (b-d) ROC curve of 70:30 and 80:20.

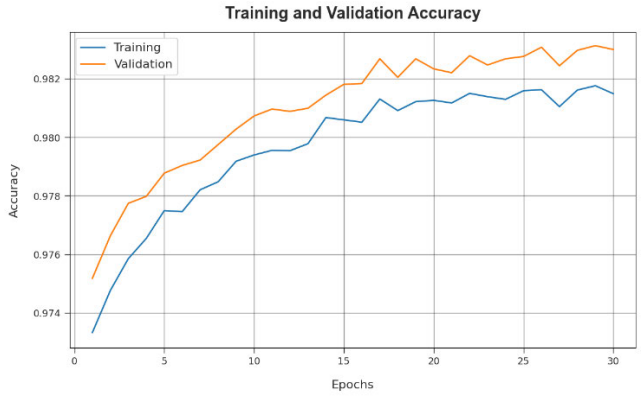


**FIGURE 9.** Accuracy curve of the BSSHN-GBOHDL approach.

TRP/TSP. Figs. 8a-8c demonstrates the PR analysis of the BSSHN-GBOHDL model under 70:30 and 80:20 of TRP/TSP. The figures reported that the BSSHN-GBOHDL model has obtained maximum PR performance under all classes. Finally, Figs. 8b-8d illustrates the ROC investigation of the BSSHN-GBOHDL model under 70:30 and 80:20 of TRP/TSP. The figure depicted that the BSSHN-GBOHDL method has proficient results with higher ROC values under distinct class labels.

Fig. 9 scrutinizes the accuracy of the BSSHN-GBOHDL technique during the training and validation process on the test dataset. The figure notifies that the BSSHN-GBOHDL technique reaches increasing accuracy values over increasing epochs. Moreover, the increasing validation accuracy over training accuracy exhibits that the BSSHN-GBOHDL approach learns efficiently on the test dataset.


**FIGURE 10.** Loss curve of the BSSHN-GBOHDL approach.

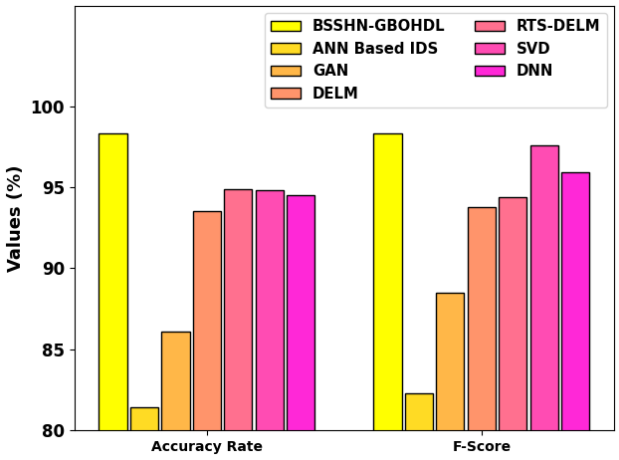


**FIGURE 11.** AR and $F_{score}$ outcome of BSSHN-GBOHDL approach with recent algorithms.

The loss analysis of the BSSHN-GBOHDL technique at the time of training and validation is demonstrated on the test dataset in Fig. 10. The results indicate that the BSSHN-GBOHDL technique reaches closer values of training and validation loss. The BSSHN-GBOHDL technique learns efficiently on the test dataset.

In Table 4, a brief comparison result analysis of the BSSHN-GBOHDL technique with recent models is provided [11]. In Fig. 11, a detailed AR and $F_{score}$ assessment of the BSSHN-GBOHDL method with existing methods is given. The results indicate that the BSSHN-GBOHDL technique reaches improved values of AR and $F_{score}$. Based on AR, the BSSHN-GBOHDL technique offers enhancing AR of 98.29% while the ANN-based IDS, GAN, DELM, RTS-DELM, SVD, and DNN models obtain decreasing AR of 81.43%, 86.09%, 93.52%, 94.85%, 94.83%, and 94.51% respectively.

Besides, based on $F_{score}$, the BSSHN-GBOHDL technique offers enhancing $F_{score}$ of 98.31% while the ANN-based IDS, GAN, DELM, RTS-DELM, SVD, and DNN

**TABLE 4.** Comparative outcome of BSSHN-GBOHDL technique with recent algorithms.

| Methods | Accuracy Rate | Precision | Recall | F-Score |
|---|---|---|---|---|
| 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 |
| SVD | 94.83 | 96.11 | 96.41 | 97.55 |
| DNN | 94.51 | 94.16 | 95.21 | 95.94 |

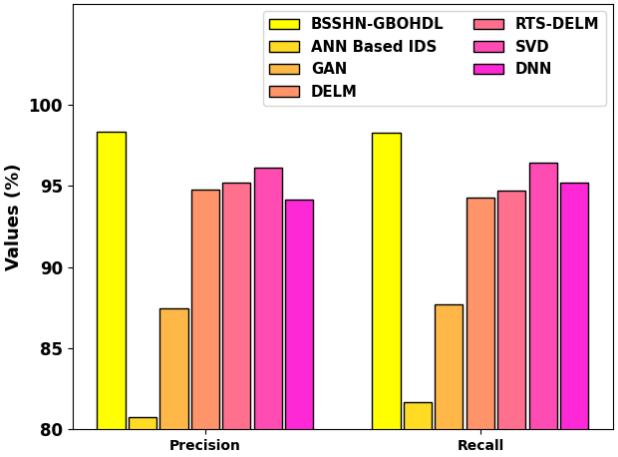


**FIGURE 12.** $Prec_n$ and $Reca_l$ outcome of BSSHN-GBOHDL approach with recent algorithms.

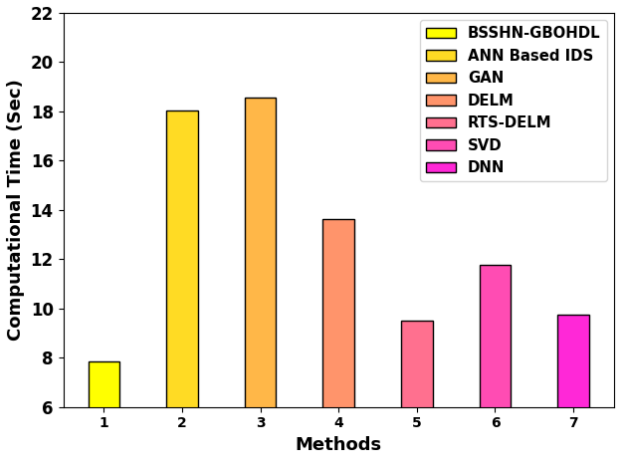


**FIGURE 13.** CT outcome of BSSHN-GBOHDL approach with recent algorithms.

**TABLE 5.** CT outcome of BSSHN-GBOHDL approach with recent algorithms.

| Methods | Computational Time (Sec) |
|---|---|
| BSSHN-GBOHDL | 07.85 |
| ANN Based IDS | 18.05 |
| GAN | 18.58 |
| DELM | 13.63 |
| RTS-DELM | 09.51 |
| SVD | 11.78 |
| DNN | 09.74 |

models obtain decreasing $F_{score}$ of 82.26%, 88.46%, 93.80%, 94.36%, 97.55%, and 95.94% respectively.

In Fig. 12, a detailed $prec_n$ and $reca_l$ assessment of the BSSHN-GBOHDL method with prevailing approaches is given. The outcomes indicate that the BSSHN-GBOHDL technique reaches improved values of $prec_n$ and $reca_l$. Based on $prec_n$, the BSSHN-GBOHDL technique offers to enhance $prec_n$ of 98.34% while the ANN-based IDS, GAN, DELM, RTS-DELM, SVD, and DNN models obtain decreasing $prec_n$ of 80.74%, 87.48%, 94.75%, 95.20%, 96.11%, and 94.16% respectively. Besides, based on $reca_l$, the BSSHN-GBOHDL technique offers enhancing $reca_l$ of 98.29% while the ANN-based IDS, GAN, DELM, RTS-DELM, SVD, and DNN models obtain decreasing $reca_l$ of 81.67%, 87.68%, 94.28%, 94.73%, 96.41%, and 95.21% respectively.

In Table 5 and Fig. 13, the computation time (CT) examination of the BSSHN-GBOHDL method with existing approaches is made. The outcomes highlight the improvements of the BSSHN-GBOHDL technique with a minimal CT of 7.85s. Contrastingly, the ANN-based IDS, GAN, DELM, RTS-DELM, SVM, and DNN models offer increasing CT values.

These results reassured that the BSSHN-GBOHDL technique accomplishes maximum performance over other existing models. These results showcased the better performance of the BSSHN-GBOHDL technique over other existing techniques. The enhanced performance of the BSSHN-GBOHDL technique is due to the inclusion of the HDL model and hyperparameter tuning approach. The design of the GBO algorithm has a significant impact on the performance of the model, and selecting the optimal values can lead to better accuracy.

## V. CONCLUSION

In this article, we have introduced a novel BSSHN-GBODHL approach for optimal identification of malicious activities in the smart home environment. Besides, the presented BSSHN-GBOHDL technique exploited the BC technology for enhancing the confidentiality of the data in the smart home environment. Moreover, the BSSHN-GBOHDL technique identifies malicious activities in the smart home environment via three sub-processes namely data preprocessing, HDL-based malicious activity classification, and GBO-based hyperparameter tuning. The experimental result analysis of the BSSHN-GBOHDL approach is tested on a benchmark

dataset and the results highlight the betterment of the BSSHN-GBOHDL technique over other recent approaches with maximum accuracy of 98.29%. Therefore, the key contribution of combining BC with DL-based malicious activity detection in a smart home network is the creation of a secure, decentralized, and privacy-preserving system that leverages the collective intelligence of devices to detect and mitigate threats effectively. It enhances the security posture of smart home networks, safeguards user privacy, and promotes a collaborative approach to defending against emerging security threats. In future, the performance of the BSSHN-GBOHDL technique can be tested in the smart healthcare environment.

## ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number (RGP2/112/44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R349), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. We Would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444).

## REFERENCES

[1] W. Meng, W. Li, S. Tug, and J. Tan, "Towards blockchain-enabled single character frequency-based exclusive signature matching in IoT-assisted smart cities," *J. Parallel Distrib. Comput.*, vol. 144, pp. 268–277, Oct. 2020.

[2] I. 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 Gener. Comput. Syst.*, 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 Informat. J.*, vol. 23, no. 4, pp. 69–75, Dec. 2022.

[4] S. Cao, S. Dang, Y. Zhang, W. Wang, and N. Cheng, "A blockchain-based access control and intrusion detection framework for satellite communication systems," *Comput. Commun.*, vol. 172, pp. 216–225, Apr. 2021.

[5] A. Rehman, S. Abbas, M. A. Khan, T. M. Ghazal, K. M. Adnan, and A. Mosavi, "A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique," *Comput. Biol. Med.*, vol. 150, Nov. 2022, Art. no. 106019.

[6] Y. Ren, Y. Leng, J. Qi, P. K. Sharma, J. Wang, Z. Almakhadmeh, and A. Tolba, "Multiple cloud storage mechanism based on blockchain in smart homes," *Future Gener. Comput. Syst.*, vol. 115, pp. 304–313, Feb. 2021.

[7] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, "A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network," *J. Parallel Distrib. Comput.*, vol. 164, pp. 55–68, Jun. 2022.

[8] 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.

[9] A. 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 Commun. Mobile Comput.*, vol. 2021, pp. 1–23, Nov. 2021.

[10] M. Baza, A. Rasheed, A. Alourani, G. Srivastava, H. Alshahrani, and A. Alshehri, "Privacy-preserving blockchain-assisted private-parking scheme with efficient matching," *Comput. Electr. Eng.*, vol. 103, Oct. 2022, Art. no. 108340.

[11] M. S. Farooq, S. Khan, A. Rehman, S. Abbas, M. A. Khan, and S. O. Hwang, "Blockchain-based smart home networks security empowered with fused machine learning," *Sensors*, vol. 22, no. 12, p. 4522, Jun. 2022.

[12] 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.

[13] A. Al-Qarafi, F. Alrowais, S. S. Alotaibi, N. Nemri, F. N. Al-Wesabi, M. Al Duhayyim, R. Marzouk, M. Othman, and M. Al-Shabi, "Optimal machine learning based privacy preserving blockchain assisted Internet of Things with smart cities environment," *Appl. Sci.*, vol. 12, no. 12, p. 5893, Jun. 2022.

[14] S. Sohail, Z. Fan, X. Gu, and F. Sabrina, "Explainable and optimally configured artificial neural networks for attack detection in smart homes," 2022, *arXiv:2205.08043*.

[15] S. W. Azumah, N. Elsayed, V. Adewopo, Z. S. Zaghloul, and C. Li, "A deep LSTM based approach for intrusion detection IoT devices network in smart home," in *Proc. IEEE 7th World Forum Internet Things (WF-IoT)*, Jun. 2021, pp. 836–841.

[16] E. S. Babu, S. Bkn, S. R. Nayak, A. Verma, F. Alqahtani, A. Tolba, and A. Mukherjee, "Blockchain-based intrusion detection system of IoT urban data with device authentication against DDoS attacks," *Comput. Electr. Eng.*, vol. 103, Oct. 2022, Art. no. 108287.

[17] M. A. Cheema, H. K. Qureshi, C. Chrysostomou, and M. Lestas, "Utilizing blockchain for distributed machine learning based intrusion detection in Internet of Things," in *Proc. 16th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2020, pp. 429–435.

[18] N. Kumaran and J. S. S. Mohan, "BRDO: Blockchain assisted intrusion detection using optimized deep stacked network," *Cybern. Syst.*, pp. 1–22, Feb. 2023.

[19] Q. Yang and H. Wang, "Privacy-preserving transactive energy management for IoT-aided smart homes via blockchain," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11463–11475, Jul. 2021.

[20] R. F. Mansour, "Blockchain assisted clustering with intrusion detection system for industrial Internet of Things environment," *Expert Syst. Appl.*, vol. 207, Nov. 2022, Art. no. 117995.

[21] M. Abdel-Basset, N. Moustafa, H. Hawash, I. Razzak, K. M. Sallam, and O. M. Elkomy, "Federated intrusion detection in blockchain-based smart transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2523–2537, Mar. 2022.

[22] I. Katib and M. Ragab, "Blockchain-assisted hybrid Harris hawks optimization based deep DDoS attack detection in the IoT environment," *Mathematics*, vol. 11, no. 8, p. 1887, Apr. 2023.

[23] M. A. Khan, S. Abbas, A. Rehman, Y. Saeed, A. Zeb, M. I. Uddin, N. Nasser, and A. Ali, "A machine learning approach for blockchain-based smart home networks security," *IEEE Netw.*, vol. 35, no. 3, pp. 223–229, May 2021.

[24] A. Yafouz, A. N. Ahmed, N. Zaini, M. Sherif, A. Sefelnasr, and A. El-Shafie, "Hybrid deep learning model for ozone concentration prediction: Comprehensive evaluation and comparison with various machine and deep learning algorithms," *Eng. Appl. Comput. Fluid Mech.*, vol. 15, no. 1, pp. 902–933, Jan. 2021.

[25] S. Yu, Z. Chen, A. A. Heidari, W. Zhou, H. Chen, and L. Xiao, "Parameter identification of photovoltaic models using a sine cosine differential gradient based optimizer," *IET Renew. Power Gener.*, vol. 16, no. 8, pp. 1535–1561, Jun. 2022.

[26] [Online]. Available: https://www.unb.ca/cic/datasets/nsl.html