IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 4 January 2024, accepted 7 January 2024, date of publication 10 January 2024, date of current version 30 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3352502

RESEARCH ARTICLE

A Decentralized Approach to Smart Home Security: Blockchain With Red-Tailed Hawk-Enabled Deep Learning

FAHAD F. ALRUWAILI[1], MANAL ABDULLAH ALOHALI[2], NOUF ALJAFFAN[3], ASMA A. ALHASHMI[4], AHMED MAHMUD[5], AND MOHAMMED ASSIRI[6]

[1]Department of Computer & Network Engineering, College of Computing and Information Technology, Shaqra University, Sharqa, Saudi Arabia
[2]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[3]Department of Computer Science and Engineering, College of Applied Science and Community Services, King Saud University, P.O. Box 103786, Riyadh 11543, Saudi Arabia
[4]Department of Computer Science at College of Science, Northern Border University, Arar, Saudi Arabia
[5]Research Center, Future University in Egypt, New Cairo 11835, Egypt
[6]Department of Computer Science, College of Sciences and Humanities-Aflaj, Prince Sattam bin Abdulaziz University, Al Aflaj 16273, Saudi Arabia

Corresponding author: Mohammed Assiri (m.assiri@psau.edu.sa)

Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R330), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Research Supporting Project number (RSPD2024R922), King Saud University, Riyadh, Saudi Arabia. The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number "NBU-FFR-2024- 2913-01". The author, Fahad F. Alruwaili, would like to thank the Deanship of Scientific Research at Shaqra University for supporting this research. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444). This study is partially funded by the Future University in Egypt (FUE).

ABSTRACT The fast development of smart home devices and the Internet of Things (IoTs) presents unprecedented accessibility into our day-to-day lives; however, it has also increased major problems regarding security and privacy. A smart home network is a vital element of modern home automation systems, enabling the interconnectivity and control of different smart devices. These networks allow homeowners to remotely control lighting, security, temperature, and entertainment systems via voice commands or smartphones. These offer energy efficiency, convenience, and improved security by permitting residents to monitor and modify their living surroundings. Safeguarding the flexibility of smart home networks against cyberattacks and unauthorized access is important to comprehending the maximum ability of smart living while retaining data integrity and privacy of connected devices. This research develops the Blockchain with Red-Tailed Hawk Algorithm-Enabled Deep Learning (BC-RTHADL) model, aimed to strengthen the safety of smart home systems. BC-RTHADL integrates the safety features of blockchain with a strong malicious action recognition procedure. The blockchain module certifies immutability, transparency, and decentralization, donating to a safe smart home atmosphere. The malicious action detection influences the Red-Tailed Hawk Algorithm for feature selection and an ensemble of Extreme Learning Machine (ELM), Gated Recurrent Unit (GRU), and Long Short-Term Memory (LSTM) techniques for precise recognition. The Equilibrium Optimizer algorithm enhances parameters for improved effectiveness. Complete tests show the greater performance of BC-RTHADL across numerous metrics, reaffirming its promising potential in safeguarding smart home networks.

INDEX TERMS Blockchain, deep learning, ensemble learning, red-tailed hawk algorithm, feature selection.

I. INTRODUCTION

A smart home is nothing but an Internet of Things (IoT) combined residence that provides users security, comfort, healthiness, enhanced regular living, etc [1]. Smart home techniques have been mainly proficient in creating people's lives more easily and improved. It offers beneficial tools such as tracking behaviors and then safety assessments, which involve consumers' and device designers', care [2]. While intelligent homes deliver many profits to landholders and

The associate editor coordinating the review of this manuscript and approving it for publication was Byung-Seo Kim.

concerned individuals these can theoretically be in malicious danger of cyberattacks to risk consumers' security as well as confidentiality. Such dangers have predictable solutions, which are federal and helpless to fierce occurrences [3]. Therefore, scalability and flexibility are needed for the right use in innovative regions of independent smart home uses and facilities. Numerous intelligent techniques make people's lives easier. This kind of program offers a massive quantity of data [4]. The storage of such regularly developing data into sources forms security worries.

Blockchain (BC) provides promising performance as a keystone of cybersecurity organizations in a diversity of smart home models such as data transmission and remote connectivity. BC models and centralized storage systems are mainly employed to find out these problems [5]. BC technique was invented by Satoshi Nakamoto in 2008 and contained within a timestamped assortment of malice-proof documents that measured by a community of decentralized methods. Decentralization, inflexibleness, and honesty are the bases of the BC method. The 3 functions protracted their doors to a huge extent of uses such as the nature of digital money and probability analysis of intelligent uses, while the BC model assurances safety [6]. For example, types of attacks currently grow highly difficult such as the majority of attacks directed choose, Sybil attacks for false identity formation in observing accord.

BC technique is a decentralized database. The dealings being achieved by the chain are support of technology. The blocks of data spread are protected by employing cryptographical models. After a novel block is combined into the chain, it is highly thought that the novel block can able to cooperate with all other blocks in the chain [7]. Proof of Work (PoW) is an effective method that is mainly employed for merging blocks by adding a hash function in the present block and then piting it. PoW offers a very simple technique with broad control and acquires node-free access. However, with the benefits, it is likely to be a waste of energy [8]. For managing the continuously developing smart BC-based applications [9], it is important to make a versatile and robust system. Machine learning (ML) is a technique that comprises computers, which clarifies itself by employing an intelligent approach [10]. Based on one argument, ML is the foremost usage case of Artificial Intelligence (AI). The system of ML supports machines for solving activities without being programmed [11]. The main aim of this category of analysis is to design a realistic technique, which can be obtained data from the input and predict it. Also modifying the outputs employing statistical analysis [12]. By implementing ML, one could process a large data quantity and attain a decision that depends on facts.

This study presents a blockchain with a red-tailed hawk algorithm-enabled deep learning (BC-RTHADL) technique for securing smart home networks. The purpose of the BC-RTHADL technique is to accomplish security via BC and malicious activity detection. Besides, the BC-RTHADL technique, the malicious activity recognition process takes place using the based feature selection (FS) approach. The extreme learning machine (ELM), gated recurrent unit (GRU), and long short-term memory (LSTM) models are the ensemble of three models of the BC-RTHADL technique for the recognition process. At last, the equilibrium optimizer (EO) algorithm is applied for the optimal parameter tuning process. A wide range of experiments were implemented to illustrate the higher efficiency of the BC-RTHADL method.

II. LITERATURE REVIEW

Almuqren et al. [13] propose a BC-aided secured Smart Home Network employing a Gradient Optimizer with a Hybrid DL (BSSHN-GBOHDL) approach. The proposed method uses BC methodology to enhance data privacy in the smart home atmosphere. GBO technique helps in expert hyperparameter selection of HDL as well as to achieve enlarged recognition efficiency. Shah et al. [14] presented an AI- and BC-assisted safe structure to challenge network-related occurrences on smart home methods. Meanwhile, IoT devices in smart home methods utilize weaker network edges and rules, attackers influence this state and exploit sensor data exchange. Therefore, the vulnerability of these methods to cyber threats as well as unapproved access is considerably delicate, posing dangerous safety hazards and underlining essential for strong defensive events and innovative safety answers.

The authors in [15] present an Optimal ML-based IDS for Privacy-Preserving BIoT in (OMLIDS-PBIoT) Smart city environments. The developed method feats BC and ML models to achieve safety in the smart city atmosphere. To achieve this, the developed technology uses data pre-processing in an early phase to convert information into a well-matched setup. Furthermore, the study presents a golden eagle optimization (GEO)-based feature selection (FS) technique to originate suitable feature subsets. Apat et al. [16] developed a Block-CFS architecture which is an advanced BC-aided fog computing structure as a secure data-tranmiss system for smart homes. As well as it demonstrates a systematic sequence diagram for BlockCFS to register and transmit information from a wide range of smart devices that are related.

Li et al. [17] present a novel ITS structure by employing the BC technique that solves confidentiality shield and safety issues as well as helping consumers and vehicles to offer data to ITSs. The offered design employs BC as a trust structure to guard consumers' confidentiality and deliver reliable services. It is also well-matched with legacy ITS structure and services. In [18], recommended a BC-aided secured data management framework (BSDMF) for information on health depending on IoMT to firmly alter patient information and improve scalability as well as data availability healthcare atmosphere. A developed BSDMF delivers secured data management among individual servers and implantable medical strategies amongst personal and cloud servers.

Alqaralleh et al. [19] project DL with BSDMF and analysis technique for IoMT atmosphere. At first, elliptic curve cryptography (ECC) is used, and the main group of ECC takes place by employing the grasshopper with fruit fly optimization (GO-FFO) method. Next, the neighborhood indexing sequence with burrow wheeler transform (NIS-BWT) is mainly utilized to translate hash values. Lastly, a DBN model is applied for detection techniques to identify the occurrence of disease. Bargayary et al. [20], authors greatly use features of BC to authorize consumers in Software-Defined Network IoT (SDN-IoT) systems. It offers central organization of rising IoT devices. BC is nothing but the tamper-proof and decentralized technique for sharing and storing authentication data that makes it appropriate for the system.

Khan et al. [21] present a resource-efficient, BC-based solution for safe and private IoT. The effective solution is made likely over new exploitation of computational resources in a usual IoT atmosphere (e.g., smart homes), besides the usage of an example of Deep Extreme Learning Machine (DELM). Lee et al. [22] developed a BC-based smart home gateway network that stands probable attacks on the gateway of smart homes. The BC technology is used at the gateway layer where data is kept and replaced in the method blocks of BC to support decentralization and overcome the issue from traditional centralized architecture. In [23], private BC execution employing Ethereum smart contract is proposed for the smart home to ensure only the homeowner can access and observe home uses. Simple smart contracts are intended to permit devices to interconnect without the necessity for a reliable third party. In [24], a private BC-based smart home network architecture for assessing intrusion detection empowered with a Fused Real-Time Sequential DELM (RTS-DELM) model is presented. This research examines the approach of RTS-DELM employed in BC-based smart homes to detect any malicious action.

III. THE PROPOSED MODEL

In this study, we have presented a new BC-RTHADL technique for securing smart home networks. The purpose of the BC-RTHADL technique is to accomplish security via BC and malicious activity detection. Fig. 1 demonstrates the entire process of the BC-RTHADL technique.

A. BC TECHNOLOGY

The BC-RTHADL method exploits BC technology to increase data confidentiality in the smart home environment. In the CPS environment, the BC technique was mainly developed to reinforce security [25]. A BC is an absolute distributed dataset where time-marked transactions are gathered as well as attached to a hash chain of blocks.

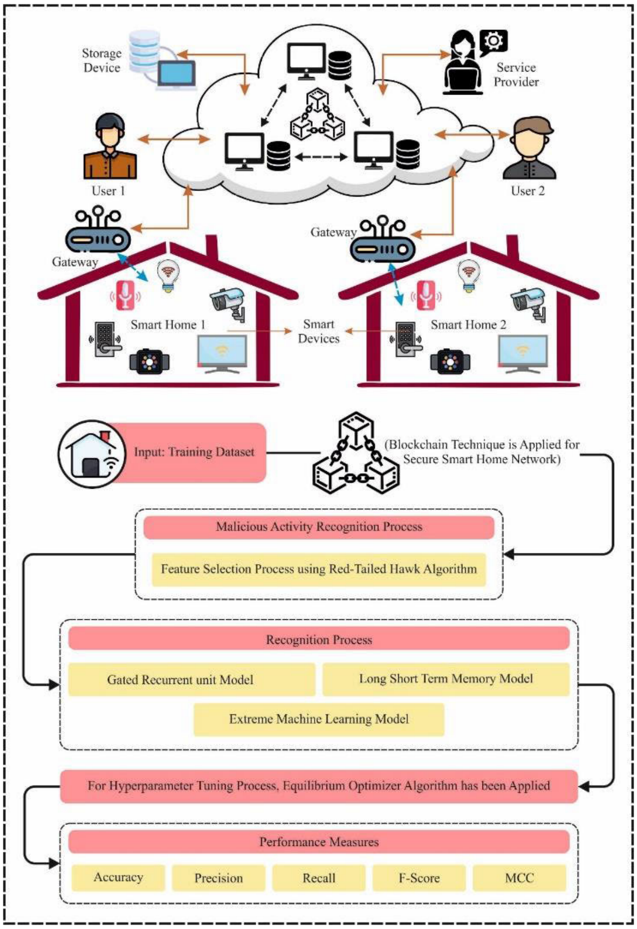
Storage Device
Service Provider
User 1
User 2
Gateway
Gateway
Smart Home 1
Smart Devices
Smart Home 2
Input: Training Dataset
(Blockchain Technique is Applied for Secure Smart Home Network)
Malicious Activity Recognition Process
Feature Selection Process using Red-Tailed Hawk Algorithm
Recognition Process
Gated Recurrent unit Model
Long Short Term Memory Model
Extreme Machine Learning Model
For Hyperparameter Tuning Process, Equilibrium Optimizer Algorithm has been Applied
Performance Measures
Accuracy
Precision
Recall
F-Score
MCC

FIGURE 1. Overall process of the BC-RTHADL technique.

A fundamental protocol of BC defines how many copies of the block could be kept and built in a spread method. One of the critical factors of this procedure is to determine how a network of contestants termed miners can able to define agreement on the current state of BC. Public, private, permissioned, and permission-less are the different types of BC architecture. Also, PoW and Proof of Stake (PoS) are the dual dominant methods. When this task finished, a novel transaction was added to BC. Entire blocks hold an exclusive code termed hash that contains previous blocks in the chain and is used for linking blocks collected in a certain order. Few miners must execute a set of computations to create reliability. This calculation solves a puzzle for charting arbitrary-sized data into stable size. Whereas in other methods, a leader must be preferred over one among the dual models. In PoW, numerous miners attempt to solve the puzzle, and one who finishes at an initial stage will be broadcasted to group proof. Then, the other miner authorizes whether the work finished is precise or not. When the confirmation is over, they select a definite miner as leader. The foremost aim of the block is to keep a list of established transactions by cryptographic hash function. This function is useful due to the following properties:

- Delivers an output of fixed size irrespective of input size.
- Determined that make related output for a delivered input.
- It is unchangeable that receiving related input from output is difficult.
- An original input creates a novel output.
- Hash computation quicker with minimum overhead.

The block in BC is associated with early genes of block and established by hash. Every block is related through the link of each hash that suggests all blocks contain the previous hash and acquire hash in the next block. Such alteration to hash prompts the chain to be destroyed then a unique hash is attached to the subsequent block. Recount the original hash for rejuvenating and then the chain needs a huge amount of computation power. In addition, we add nonce so the miner plays with data to create a hash that output has 3 zeroes. Once the miner originates a nonce, then it chiefs to block hash below the challenging threshold. At last, it is considered that the block is effective and spread to the network. BC can able to shield the honesty of data storage and safeguard procedure transparency as well as can be used in an intrusion detection area. The deficiency of universal trust suggests an essential for the distributed consensus tool for block validation in BC technology. BC-based anomaly classification techniques are mainly employed to improve security.

B. FEATURE SELECTION USING RTHA

The malicious activity recognition process takes place using RTHA for the feature selection process. The RTHA technique stimulates the hunting behaviour of red-tailed hawks [26]. The actions taken during the hunting process are modelled and presented. Low soaring, high soaring, and stooping and swooping are three different phases of RTHA.

High soaring: the individuals soar far into the sky, searching for a better place relating to food availability, and the mathematical modelling is shown in Eq. (1):

$$X\ (t) = X_{best} + (X_{mean} - X\ (t-1)) \cdot Levy\,(\mathrm{dim}) \cdot TF\ (t) \tag{1}$$

In Eq. (1), the red-tailed hawk location at the t^{th} iteration is $X\ (t)$, the optimal location attained so far is X_{best}, X_{mean} denotes the locations' mean, *Levy* denotes the levy fight distribution function and the transition factor function is denoted as $TF(t)$.

$$\begin{aligned} Levy(\mathrm{dim}) &= s\frac{\mu \cdot \sigma}{|v|^{\beta-1}} \\ \sigma &= \left(\frac{\Gamma\ (1+\beta) \cdot \sin\left(\frac{\pi\beta}{2}\right)}{\Gamma\left(\frac{1+\beta}{2}\right) \cdot \beta \cdot 2^{\left(1-\frac{\beta}{2}\right)}}\right) \end{aligned} \tag{2}$$

where the problem dimension is *dim*, β is a constant (1.5), s is a constant (0.01), and u and v are random integers [0,1].

$$TF\ (t) = 1 + \sin\left(2.5 + \left(\frac{\mathrm{t}}{T_{\max}}\right)\right) \tag{3}$$

where $T_{\max}$ indicates the maximum iteration counter.

Low soaring: the individuals encircle the target by flying lower toward the ground in a spiral line and the mathematical modelling is shown in Eq. (4):

$$\begin{aligned} X\ (t) &= X_{best} + (x\ (t) + y\ (t))\ .StepSize\ (t) \\ StepSize(t) &= X\ (t) - X_{mean} \end{aligned} \tag{4}$$

where x and y are coordinate directions

$$\begin{cases} x(t) = R(t) \cdot \sin(\theta(t)) \\ y(t) = R(t) \cdot \cos(\theta(t)) \end{cases} \quad \begin{cases} R\ (t) = R_0 \cdot (r - t/T_{\max}) \cdot rand \\ \theta\ (t) = A \cdot (1 - t/T_{\max}) \cdot rand \end{cases}$$

$$\begin{cases} x(t) = x(t)/\max|x(t)| \\ y(t) = y(t)/\max|y\ (t)\ | \end{cases} \tag{5}$$

where r denotes a control gain [1], [2], the initial value ranges within [0.5−3] is R_0, A indicates the angel gain [515], and *rand* shows the random integer [0,1]. This parameter helps the hawk fly around the target with spiral movement.

Stooping and Swooping: The hawk rapidly stoops and attacks the target from the optimum location during low soaring and the mathematical modelling is shown in Eq. (6):

$$\begin{aligned} X\ (t) = \alpha\ (t) \cdot X_{best} &+ x\ (t)\ .\mathrm{StepSize1}\ (t) \\ &+ y\ (t)\ .\mathrm{StepSize2}\ (t) \end{aligned} \tag{6}$$

$$\begin{aligned} \mathrm{StepSize1}\ (t) &= X\ (t) - TF\ (t) \cdot X_{mean} \\ \mathrm{StepSize2}(t) &= G(t) \cdot X(t) - TF(t) \cdot X_{best} \end{aligned} \tag{7}$$

where the acceleration and the gravity factors are α and G respectively:

$$\begin{aligned} \alpha\ (t) &= \sin^2(2.5 - t/T_{\max}) \\ G\ (t) &= 2 \cdot \left(1 - \frac{t}{T_{\max}}\right) \end{aligned} \tag{8}$$

In Eq. (8), the acceleration α of hawk rises with increasing t to improve the convergence rate and the gravity effect G that reduces the exploitation diversity once they get nearer to the target.

Choosing a relevant feature that aids the classifier in identifying a sample class in data is challenging [27]. In the selection process, it is necessary to improve the performance of classification problems and automatically eliminate the unnecessary ones for the classification once the selected feature. The RTHA is used to find the optimum feature subset and exploits the classifier for calculating the classification performance. Where A_c denotes classification accuracy b_s represents the feature subset dimension, and D_t is the overall amount of features in the dataset. Thus, the classifier error is $1 - A_c$ and the subset of features selected from the data is represented as $\frac{d_s}{D_t}$. Therefore, the fitness function can be described as follows:

$$\downarrow Fitness = \mu \cdot (1 - A_c) + (1 - \mu) \cdot \frac{d_s}{D_t} \tag{9}$$

In Eq. (9), the weight allocated to the error classification is $\mu \in [0, 1]$.

C. ENSEMBLE LEARNING-BASED CLASSIFICATION

In this work, GRU, LSTM, and ELM models are used in the ensemble of three models in the BC-RTHADL technique for the recognition process.

1) LSTM

LSTM is a kind of RNN that is proficient in forecasting long as well as short-term needs in time sequence information [28]. When compared to a simple RNN, the use of LSTM is capable of solving the vanishing gradient problems, where the training behavior of the system overloads after a definite amount of training iteration. Additionally, time-delayed

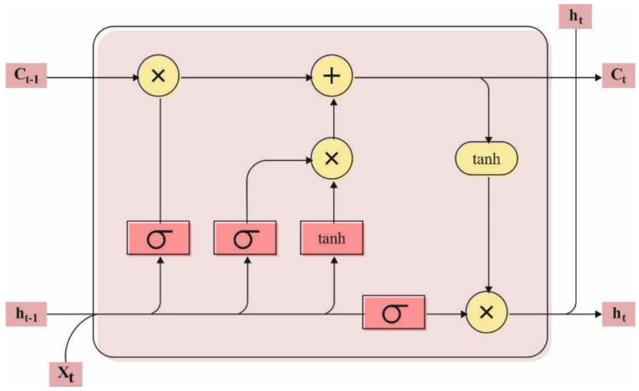

FIGURE 2. LSTM architecture.

effects representation is significant for unstable aerodynamic modelling and combined in the LSTM model. The LSTM cell procedures external data via forget, input, and output gates. Fig. 2 represents the structural design of LSTM.

The forget gate f procedures input of present time stage x_t and vector signifies output from preceding time phase h_{t-1}, which is mentioned as a hidden layer (HL) of LSTM cell:

$$f_t = \sigma\left(W_f x_t + W_f h_{t-1} + b_f\right). \tag{10}$$

Both inputs of the forget gate increased with weights W_f and bias b_f added. By using sigmoid (σ) activation, portions of data received are rejected from the cell.

Equivalent to the forget gate, the input gate also procedures existing time phase x_t and HL from the previous time step h_{t-1} by sigmoid activation function:

$$i_t = \sigma\left(W_i x_t + W_i h_{t-1} + b_i\right) \tag{11}$$

W_i defines weigh and b_i defines the bias of the input gate. In 2nd stage, both inputs are managed by the tanh activation that forms novel cell state vector $\tilde{c}_t$:

$$\tilde{c}_t = \tanh\left(W_h x_t + W_h h_{t-1} + b_h\right). \tag{12}$$

Depending on the new cell state $\tilde{c}_t$, old data in the cell is upgraded. So, the cell state from the prior time stage c_{t-1} increased with forgetting gate vector f_t and the current cell state upgraded by input gate vector i_t:

$$c_t = f_t c_{t-1} + i_t \tilde{c}_t. \tag{13}$$

After passing the input gate, the current input data is x_t, the previous HL is h_{t-1} and the current cell state is c_t managed by a sigmoid and tanh activation:

$$\begin{aligned} o_t &= \sigma\left(W_o x_t + W_o h_{t-1} + b_o\right) \\ h_t &= o_t \cdot tanh\left(c_t\right). \end{aligned} \tag{14}$$

A forecast labeled by upgraded HL h_t that are conveyed to the next HL or output layer.

2) GRU

GRU and LSTM belong to RNN [29]. The main dissimilarity of GRU is that it integrates input and forget gate into the update gate, hence GRU has less trainable parameters, simple converges, and quicker trainable rapidity. Similarly, GRU is a modified LSTM that deals with the extended distance necessity issue of RNN, precisely forecasts via engaged memory data, and trains semantic data that follows to number of exact areas. GRU training text comes with robust suitability as well as the significance of non-continuous related data. So, we can employ GRU for feature learning as well as memory.

Due to the special gate structure, GRU selects information to transfer to control data. The expressions are described below:

$$z_t = \sigma\left(W_z x_t + U_Z h_{t-1}\right) \tag{15}$$

$$r_t = \sigma\left(W_r x_t + U_r h_{t-1}\right) \tag{16}$$

$$\tilde{h}_t = \tanh\left(W_h x_t + U_h\left(r_t \odot h_{t-1}\right)\right) \tag{17}$$

$$h_t = \left(1 - z_t\right) \odot h_{t-1} + z_t \odot \hat{h}_t \tag{18}$$

whereas $W_z, U_r, W_r,$ *and* U_z signify the weight matrix of update and reset gates. W_h and U_h denote candidate HL. $\sigma(\cdot)$ represents the sigmoid function, r_t, and z_t symbolize the status of reset and update gates, tanh$(\cdot)$ signifies the hyperbolic tangent function, *and* $\odot$ represents the Hadamard product operator. h_t signifies hidden state at time $t.t$ refers to candidate HL.x_t characterizes model input.

GRU defines its output over dual instants beforehand as well as afterwards so that it learns semantic features of context when handling consecutive text. However, it does not have special attention, therefore we include a word-level attention device on the GRU base for improving the symbol of references compared to other words.

3) ELM MODEL

The ELM model allows a unified pattern with a broad range of feature communications used in the HL that are directly exploited in multi-class classification and regression [30]. ELM is a learning algorithm for Single Hidden Neural Network (SHNN) that offers random initialization for input weights and biases together with the evaluation of analytic output weights. D-dimension classification with N number of training instances can be given as follows:

$$\left(x^{(n)}, t^{(n)}\right), \quad n = 1 : N \tag{19}$$

For $n = 1 : N, t^{(n)} \in \mathbb{R}^K$, and $x^{(n)} \in \mathbb{R}^D$.

A feedforward ELM model can be expressed as follows:

$$t^{(n)} = \sum_{\mathrm{m}=1}^{M} \beta_{\mathrm{m}} g\left(w_m^T x^{(n)} + b_{\mathrm{m}}\right) \tag{20}$$

In Eq. (20), b_m denotes the bias of m^{th} neurons of the HL, $g(\cdot)$ describes the activation function, M defines the neurons of HL, $w_m = [w_{m1}, w_{m2}, \ldots, w_{mD}]$ indicates the weight input vector that links the input neuron to the m^{th} neurons of the HL,

$\beta_m = [\beta_{m1}, \beta_{m2}, \ldots, \beta_{mK}]$ defines the weight vector which links the output layer to m^{th} neurons of HL. This concept can be obtained by the following expression:

$$H \times \beta = T \tag{21}$$

where

$$H = \begin{bmatrix} g\left(w_m^T x^{(1)} + b_1\right) & \ldots & g\left(w_M^T x^{(1)} + b_1\right) \\ \vdots & \ddots & \vdots \\ g\left(w_1^T x^{(N)} + b_1\right) & \ldots & g\left(w_M^T x^{(N)} + b_M\right) \end{bmatrix} \tag{22}$$

$$H = [\beta_1^T,\ \beta_2^T,\ \ldots,\ \beta_M^T]_{M\times N}^T \tag{23}$$

$$T = [t_1^T,\ t_2^T,\ \ldots,\ t_M^T]_{N\times K}^T \tag{24}$$

Meanwhile, if the number of training instances is more than HL neurons, then H will be a non-square matrix. Hence, the Moore-Penrose matrix inverse ($H\dagger$) is used. To overcome these problems:

$$\hat{\beta} = H^{\dagger} \times T \tag{25}$$

D. EO-BASED PARAMETER TUNING

At last, the EO algorithm is exploited for the optimal parameter tuning process. EO is the new optimization algorithm inspired by the physical behavior and the balance of control volume mass with equilibrium and dynamic states [31]. Every searching agent randomizes its concentration in line with the better solution attained so far to obtain the optimum solution (viz., equilibrium state). To prevent from getting into local minima and improve its search abilities, the EO applied "generation rate". The EO optimization strategy can be discussed in the following

Step1: Randomly generate the initial population of concentration.

$$Q_{ij}^{initial} = lb_j + rand_j.(ub_j - lb_j), \quad i = 1, 2, \ldots, N, j = 1, 2, \ldots, n \tag{26}$$

In Eq. (26), the size of the population is N, the i^{th} initial vector of particles of the j^{th} concentration is $Q_{ij}^{initial}$. *rand* denotes the random integer ranges within [0,1].

Step2. In the optimization-seeking technique, generate the equilibrium pooling ($\overline{Q}_{eq.pool}$) with the four different particles as follows:

$$Q_{eq,pool} = \left\{Q_{eq(1)}, Q_{eq(2)}, Q_{eq(3)}, Q_{eq(4)}, Q_{eq(ave)}\right\} \tag{27}$$

Step3. Update the particle concentration after randomly choosing candidate $\overline{Q}$ to guide the search.

$$\bar{Q} = \bar{Q}_{eq} + \left(\bar{Q} - \bar{Q}_{eq}\right).\bar{F} + \frac{\overline{G}}{\bar{\lambda}V}\left(1 - \bar{F}\right) \tag{28}$$

In Eq. (28), V represents a unit, and $\overline{F}$ denotes the vector of the exponential term

$$\bar{F} = b_1.sign\left(\bar{r}{-}0.5\right)\left[1 - e^{-\overline{\gamma}t}\right] \tag{29}$$

In Eq. (29), $\bar{\gamma}$ is a turnover rate that falls within [0,1], and t represents the time that relies on iteration (It) that gets smaller once the iteration count increases and is formulated below.

TABLE 1. Details on database.

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

$$t = \left(1 - \frac{lt}{lt_{\max}}^{\left(b_2 \frac{It}{It_{max}}\right)}\right) \tag{30}$$

The following description applies to the starting point at time (t_0).

$$\bar{t}_0 = \frac{1}{\bar{\gamma}}\ln\left(-b_1.sign\left(\bar{r}{-}0.5\right)\left[1 - e^{-\overline{\gamma}t}\right]\right) + t \tag{31}$$

where $It_{\max}$ defines the maximal iteration size, the constant parameters b_1, *and* b_2 manage the exploration and the exploitation abilities set to 2, and 1 correspondingly, $\overline{r}$ represents a uniform distribution random vector within [0-1]. Furthermore, $\overline{G}$ denotes the generation rate to enhance the exploitation stage:

$$G = e^{-\gamma(;-;_0)}.\overline{G} = \overline{FG} \tag{32}$$

$$\overline{G}_0 = \overline{GCP}(\overline{Q}_{eq} - \overline{\lambda Q})_)\overline{GCP} = \begin{cases} 0.5a_1 & a_2 \geq SP \\ 0 & a_2 < SP \end{cases} \tag{33}$$

Now, a_1 and a_2 are randomly generated integers within [0,1]; the parameter $\overline{GCP}$ controls the generation rate. The switching probability SP is fixed as 0.5 to accomplish a good balance between the exploitation and exploration features.

The EO system develops an FF to accomplish greater classification solution. It expresses a positive integer to imply the optimal result of candidate performance. At this point, the reduction of the classifier errors is supposed that FF, as defined in Eq. (34).

$$\begin{aligned} fitness\left(x_i\right) &= ClassifierErrorRate\left(x_i\right) \\ &= \frac{No.of\ misclassified\ instances}{Total\ no.of\ instances} {*}100 \end{aligned} \tag{34}$$

IV. EXPERIMENTAL VALIDATION

In this section, the stimulation outcomes are examined on the NSL-KDD dataset [32], including 2 class labels and 126238 samples as shown in Table 1.

Fig. 3 illustrates the confusion matrices attained by the BC-RTHADL algorithm at 70:30 and 80:20 of TRPH/TSPH. The simulation value referred to the efficient detection of the normal and attack samples under all classes.

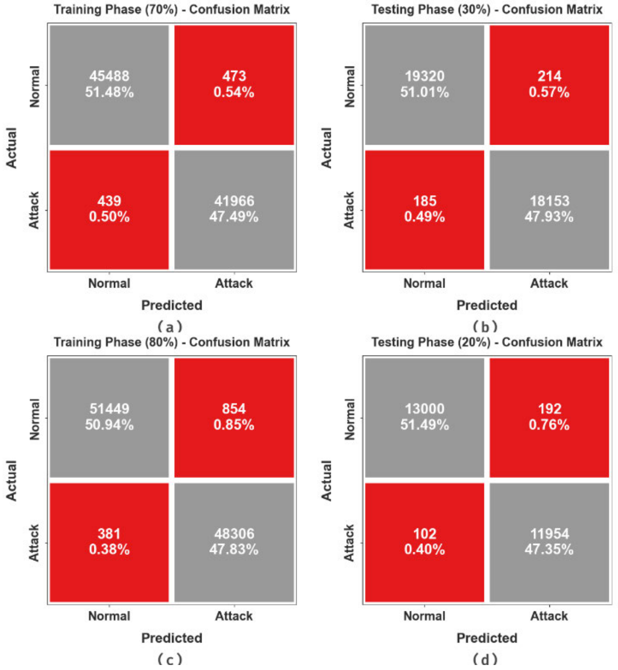

FIGURE 3. Confusion matrices of (a-b) 70:30 of TRPH/TSPH and (c-d) 80:20 of TRPH/TSPH.

TABLE 2. Classification outcome of BC-RTHADL method under 70:30 of TRPH/TSPH.

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	MCC
TRPH (70%)					
Normal	98.97	99.04	98.97	99.01	97.93
Attack	98.96	98.89	98.96	98.93	97.93
Average	98.97	98.96	98.97	98.97	97.93
TSPH (30%)					
Normal	98.90	99.05	98.90	98.98	97.89
Attack	98.99	98.83	98.99	98.91	97.89
Average	98.95	98.94	98.95	98.95	97.89

In Table 2 and Fig. 4, the detection result of the BC-RTHADL method under 70:30 of TRPH/TSPH is portrayed. The results pointed out that the BC-RTHADL technique achieves enhanced recognition results. On 70% of TRPH, the BC-RTHADL method gains an average $accu_y$ of 98.97%, $prec_n$ of 98.96%, $reca_l$ of 98.97%, F_{score} of 98.97%, and MCC of 97.93%. Additionally, on 30% of TSPH, the BC-RTHADL method achieves an average $accu_y$ of 98.95%, $prec_n$ of 98.94%, $reca_l$ of 98.95%, F_{score} of 98.95%, and MCC of 97.89%.

Fig. 3 illustrates the confusion matrices attained by the BC-RTHADL algorithm at 70:30 and 80:20 of TRPH/TSPH. The simulation value referred to the efficient detection of the normal and attack samples under all classes.

In Table 2 and Fig. 4, the detection result of the BC-RTHADL method under 70:30 of TRPH/TSPH is portrayed. The results pointed out that the BC-RTHADL technique achieves enhanced recognition results. On 70% of TRPH, the BC-RTHADL method gains an average $accu_y$ of 98.97%, $prec_n$ of 98.96%, $reca_l$ of 98.97%, F_{score} of 98.97%, and MCC of 97.93%. Additionally, on 30% of TSPH, the BC-RTHADL method achieves an average $accu_y$ of 98.95%, $prec_n$ of 98.94%, $reca_l$ of 98.95%, F_{score} of 98.95%, and MCC of 97.89%.

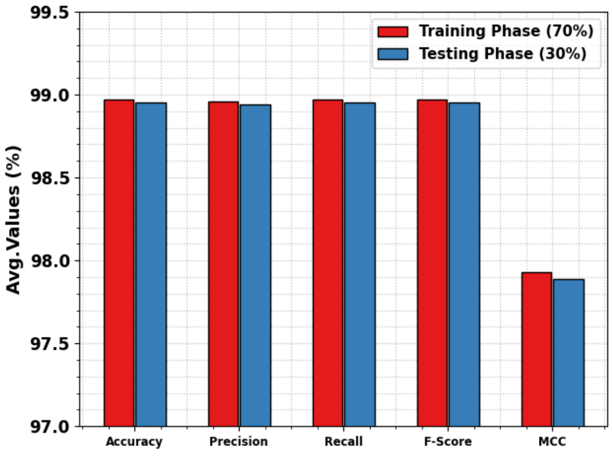

FIGURE 4. Average of BC-RTHADL technique under 70:30 of TRPH/TSPH.

TABLE 3. Classification outcome of BC-RTHADL method under 80:20 of TRPH/TSPH.

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	MCC
80% of TRPH					
Normal	98.37	99.26	98.37	98.81	97.56
Attack	99.22	98.26	99.22	98.74	97.56
Average	98.79	98.76	98.79	98.78	97.56
20% of TSPH					
Normal	98.54	99.22	98.54	98.88	97.67
Attack	99.15	98.42	99.15	98.79	97.67
Average	98.85	98.82	98.85	98.83	97.67

In Table 3 and Fig. 5, the detection outcome of the BC-RTHADL method at 80:20 of TRPH/TSPH is depicted. The outcome indicated that the BC-RTHADL system gains improved recognition outcomes. On 80% of TRPH, the BC-RTHADL algorithm achieves an average $accu_y$ of 98.79%, $prec_n$ of 98.76%, $reca_l$ of 98.79%, F_{score} of 98.78%, and MCC of 97.56%. Furthermore, on 20% of TSPH, the BC-RTHADL method reaches an average $accu_y$ of 98.85%, $prec_n$ of 98.82%, $reca_l$ of 98.85%, F_{score} of 98.83%, and MCC of 97.67%.

The training and validation $accu_y$ curves of the BC-RTHADL technique under 70:30 of TRPH/TSPH displayed in Fig. 6, provide valuable insights into the outcome of the BC-RTHADL technique over multiple epochs. These

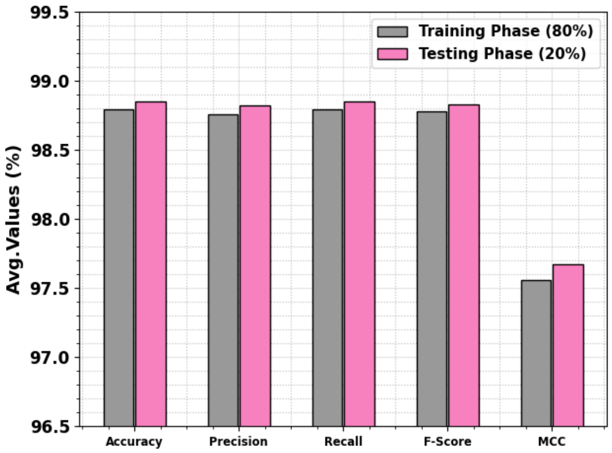

FIGURE 5. Average of BC-RTHADL method under 80:20 of TRPH/TSPH.

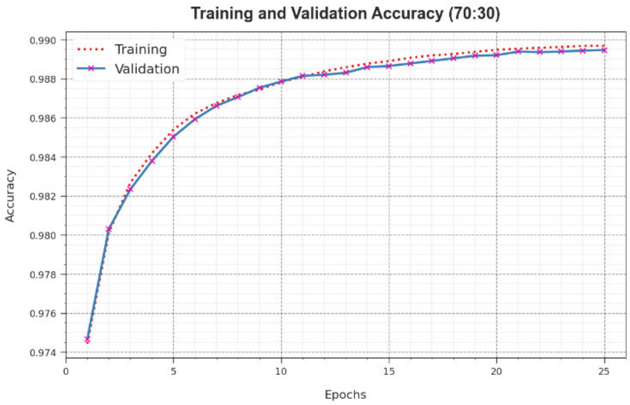

FIGURE 6. ***Accu$_y$*** **curve of BC-RTHADL technique under 70:30 of TRPH/TSPH.**

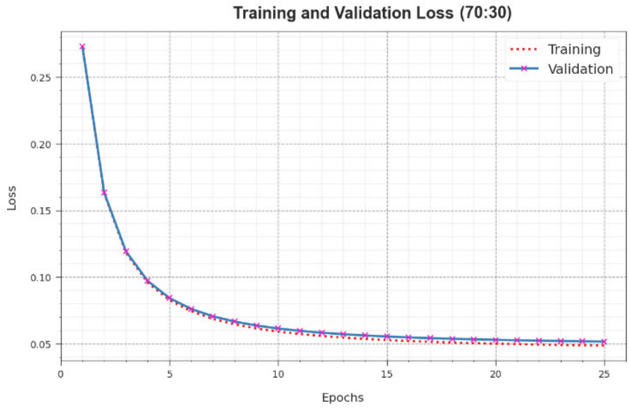

FIGURE 7. Loss curve of BC-RTHADL technique under 70:30 of TRPH/TSPH.

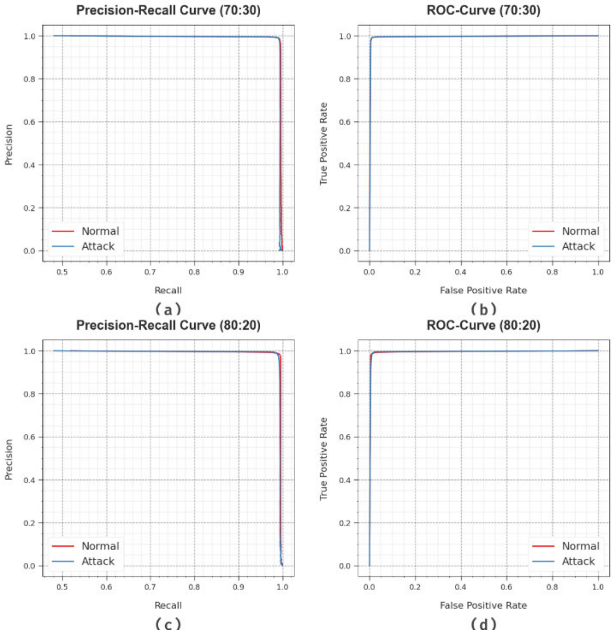

FIGURE 8. (a-c) PR curve on 70:30 and 80:20 and (b-d) ROC curve on 70:30 and 80:20.

curves demonstrate the essential insights into the learning process and the model's generalization capability. Besides, it can be noticeable that there is a consistent improvement in the TR and TS $accu_y$ over maximum epochs. It notes that the model's capacity to learn and recognize patterns within both the training and testing datasets. The increasing testing accuracy recommends that the model not only adapts to the training data but also excels in making correct predictions on previously unseen data, highlighting its robust generalization abilities.

In Fig. 7, we signify a comprehensive view of the TR and TS loss values for the BC-RTHADL technique under 70:30 of TRPH/TSPH across various epochs. The TR loss progressively decreases as the model optimizes its weights to reduce classification errors on both TR and TS databases. These loss curves provide a clear picture of how well the model aligns with the training data, underlining its capability to effectively hold patterns in both datasets. It is worth noting that the BC-RTHADL technique incessantly refines its parameters to minimize the discrepancies between the predictive and actual TR labels.

Fig. 8 signifies the classifier performances of BC-RTHADL algorithm at 70:30 and 80:20. The PR curve of the BC-RTHADL algorithm is shown in Figs. 8a-8c. The outcomes inferred that the BC-RTHADL system outcomes in higher PR values. Moreover, it can be obvious that the BC-RTHADL algorithm obtains greater PR values on all classes. Finally, the ROC outcome of the BC-RTHADL algorithm is demonstrated in Figs. 8b-8d. The outcome defined that the BC-RTHADL methodology resulted in higher values of ROC. In addition, the BC-RTHADL algorithm extends higher values of ROC on all classes.

Table 4 offers a comprehensive comparison analysis of the BC-RTHADL method [13]. In Fig. 9, a comparative $accu_y$ and F_{score} analysis of the BC-RTHADL technique. The results highlighted that the BC-RTHADL technique reaches

TABLE 4. Comparative outcome of BC-RTHADL technique with existing models.

Methods	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
BC-RTHADL	98.97	98.96	98.97	98.97
BSSHN- GBOHDL	98.29	98.34	98.29	98.31
ANN Based IDS	81.43	80.74	81.67	82.26
GAN Algorithm	86.09	87.48	87.68	88.46
DELM Model	93.52	94.75	94.28	93.8
RTS-DELM	94.85	95.2	94.73	94.36
SYD Model	94.83	96.11	96.41	97.55
DNN Algorithm	94.51	94.16	95.21	95.94

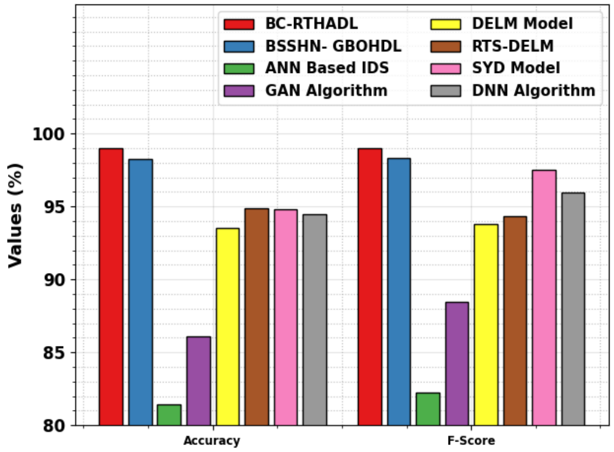

FIGURE 9. $Accu_y$ and F_{score} outcome of BC-RTHADL technique with other methods.

enhanced performance. Based on $accu_y$, the BC-RTHADL technique provides increased $accu_y$ of 98.97% whereas the BSSHN-GBODL, ANN-based IDS, GAN, GELM, RTS-DELM, SYD, and DNN techniques accomplish decreased $accu_y$ values of 98.29%, 81.43%, 86.09%, 93.52%, 94.85%, 94.83%, and 94.51%, correspondingly. Additionally, based on F_{score}, the BC-RTHADL approach offers a superior F_{score} of 98.97% whereas the BSSHN-GBODL, ANN-based IDS, GAN, GELM, RTS-DELM, SYD, and DNN methods gain reduced F_{score} values of 98.31%, 82.26%, 88.46%, 93.8%, 94.36%, 97.55%, and 95.94%, correspondingly.

In Fig. 10, a comparative $prec_n$ and $reca_l$ outcomes of the BC-RTHADL algorithm. The simulation value defined that the BC-RTHADL method attains improved outcomes. Based on $prec_n$, the BC-RTHADL method achieves a maximal $prec_n$ of 98.96% whereas the BSSHN-GBODL, ANN-based IDS, GAN, GELM, RTS-DELM, SYD, and DNN approaches realize minimal $prec_n$ values of 98.34%, 80.74%, 87.48%, 94.75%, 95.2%, 96.11%, and 94.16%, correspondingly. Furthermore, based on $reca_l$, the BC-RTHADL technique provides increased $reca_l$ of 98.97% whereas the BSSHN-GBODL, ANN-based IDS, GAN, GELM, RTS-DELM, SYD, and DNN approaches achieve reduced $reca_l$ values of 98.29%, 81.67%, 87.68%, 94.28%, 94.73%, 96.41%, and 95.21%, correspondingly.

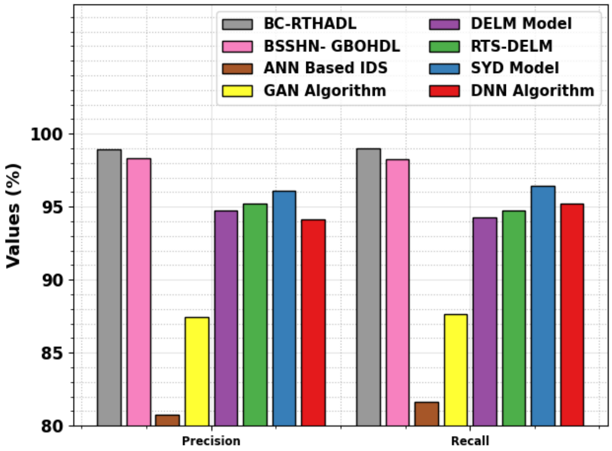

FIGURE 10. $Prec_n$ and $reca_l$ outcome of BC-RTHADL technique with other methods.

TABLE 5. CT outcome of BC-RTHADL technique with existing approaches.

Methods	Computational Time (Sec)
BC-RTHADL	03.59
BSSHN- GBOHDL	07.85
ANN Based IDS	18.05
GAN Algorithm	18.58
DELM Model	13.63
RTS-DELM	09.51
SYD Model	11.78
DNN Algorithm	09.74

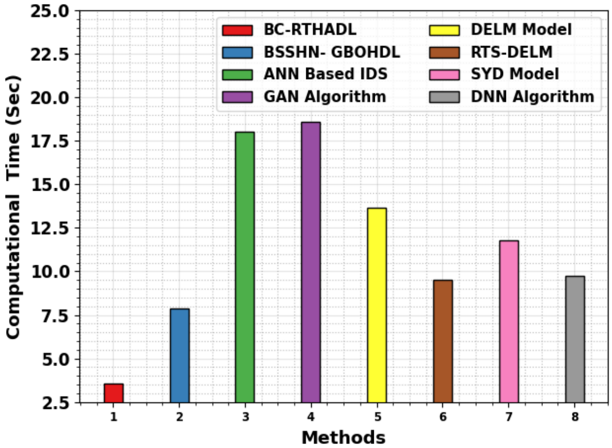

FIGURE 11. CT outcome of BC-RTHADL technique with recent approaches.

Finally, a comprehensive computation time (CT) result of the BC-RTHADL approach with other techniques is given in Table 5 and Fig. 11. The outcome indicated that the BC-RTHADL method reaches better performance with a minimal CT value of 3.59s. On the other hand, the existing BSSHN-GBODL, ANN-based IDS, GAN, GELM, RTS-DELM, SYD, and DNN models obtain increased CT outcomes. Thus, the BC-RTHADL technique is found to be superior to other models.

The BC-RTHADL model determines greater performance owing to its new mixture of BC and the RTHA-Enabled DL techniques. The integration of BC improves the safety of smart home systems by delivering immutability, transparency, and decentralization which is vital for protecting sensitive data in linked devices. This safeguards a tamper-resistant and trustworthy situation. Furthermore, the combination of the RTHA-enabled DL technique, including ensemble learning with ELM, GRU, and LSTM approaches, donates to strong malicious action recognition. The RTHA-based FS mechanism improves the model's capacity to recognize and diminish safety dangers effectually. Moreover, the application of the EO system for optimum parameter tuning perfects the models for the finest performance. The BC-RTHADL model comprehensive model, uniting the powers of BC and innovative DL systems, outcomes in a more robust, safe, and effectual result for certifying the reliability and confidentiality of smart home systems.

V. CONCLUSION

In this study, we have presented a new BC-RTHADL method for securing smart home networks. The purpose of the BC-RTHADL technique is to accomplish security via BC and malicious activity detection. In the presented BC-RTHADL technique, BC technique is applied which integrates the transparency, immutability, and decentralized nature of BC for a secure smart home network. Besides, the BC-RTHADL technique, the malicious activity recognition process takes place using RTHA based FS approach. The ELM, GRU, and LSTM models are the ensemble of three models of the BC-RTHADL technique for the recognition process. A wide range of experiments were implemented to illustrate the higher efficiency of the BC-RTHADL method. The comprehensive study analysis reported the promising performance of the BC-RTHADL technique under various measures.

The decentralized technique of BC-RTHADL can be almost executed in smart home safety to find numerous real-world states. For example, in a smart home atmosphere where manifold IoT devices communicate, the decentralized blockchain safeguards protected and obvious communication. Homeowners can observe and control entree to smart locks, surveillance cameras, and devices with augmented confidence, significant that the organism is resilient to tampering or illegal alterations. Moreover, in scenarios connecting common or borrowed smart homes, the decentralized nature of BC-RTHADL offers an immutable record of device actions, promising all stakeholders of the honesty of the logged data.

Network scalability may be a problem as the number of related devices rises, possibly foremost due to performance bottlenecks. Also, decentralized systems frequently include greater upfront prices and energy utilization, particularly in BC executions. Future work can discover more effectual consensus systems and scalable BC architectures to further boost the performance and scalability of decentralized methods in the framework of growing smart home systems. In addition, privacy-preserving technologies can be proposed that authorize users with rough control over their data, promising transparency and user-centric algorithms for data confidentiality.

ACKNOWLEDGMENT

Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R330), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Research Supporting Project number(RSPD2024R922), King Saud University, Riyadh, Saudi Arabia. The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number ''NBU-FFR-2024- 2913-01''. The author, Fahad F. Alruwaili, would like to thank the Deanship of Scientific Research at Shaqra University for supporting this research. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444). This study is partially funded by the Future University in Egypt (FUE).

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] S. F. Khan, S. S. Priya, M. Soni, I. Keshta, and I. R. Khan, "A blockchain-based AI approach towards smart home organization security," *Artificial Intelligence, Blockchain, Computing and Security* vol. 1. Boca Raton, FL, USA: CRC Press, 2024, pp. 589–596.

[13] 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*, 2023.

[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, Aug. 2023.

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

[16] H. K. Apat, B. Sahoo, S. Mohanty, M. Mukul, and R. K. Barik, "A Blockchain-assisted fog computing framework for secure data sharing mechanism in smart home," in *Proc. IEEE Int. Conf. Contemp. Comput. Commun. (InC4)*, vol. 1, Apr. 2023, pp. 1–6.

[17] Y. Li, K. Ouyang, N. Li, R. Rahmani, H. Yang, and Y. Pei, "A blockchain-assisted intelligent transportation system promoting data services with privacy protection," *Sensors*, vol. 20, no. 9, p. 2483, Apr. 2020.

[18] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, "Blockchain-assisted secured data management framework for health information analysis based on the Internet of Medical Things," *Pers. Ubiquitous Comput.*, pp. 1–14, Jun. 2021.

[19] B. A. Alqaralleh, T. Vaiyapuri, V. S. Parvathy, D. Gupta, A. Khanna, and K. Shankar, "Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment," *Pers. Ubiquitous Comput.*, pp. 1–11, Feb. 2021.

[20] B. Bargayary and N. Medhi, "A blockchain-assisted authentication for SDN-IoT network using smart contract," in *Proc. 4th Int. Conf. Comput. Commun. Syst. (I3CS)*, Mar. 2023, pp. 1–6.

[21] 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 network security," *IEEE Netw.*, vol. 35, no. 3, pp. 223–229, Nov. 2020.

[22] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, pp. 1–14, Dec. 2020.

[23] A. Qashlan, P. Nanda, and X. He, "Automated Ethereum smart contract for block chain based smart home security," in *Proc. Smart Syst. IoT, Innov. Comput. (SSIC)*. Singapore: Springer, Oct. 2020, pp. 313–326.

[24] 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.

[25] R. F. Mansour, "Artificial intelligence-based optimization with deep learning model for blockchain-enabled intrusion detection in CPS environment," *Sci. Rep.*, vol. 12, no. 1, p. 12937, Jul. 2022.

[26] S. Ferahtia, A. Houari, H. Rezk, A. Djerioui, M. Machmoum, S. Motahhir, and M. Ait-Ahmed, "Red-tailed hawk algorithm for numerical optimization and real-world problems," *Sci. Rep.*, vol. 13, no. 1, p. 12950, Aug. 2023.

[27] O. A. Akinola, A. E. Ezugwu, O. N. Oyelade, and J. O. Agushaka, "A hybrid binary dwarf mongoose optimization algorithm with simulated annealing for feature selection on high dimensional multi-class datasets," *Sci. Rep.*, vol. 12, no. 1, p. 14945, Sep. 2022.

[28] R. Zahn, A. Weiner, and C. Breitsamter, "Prediction of wing buffet pressure loads using a convolutional and recurrent neural network framework," *CEAS Aeronaut. J.*, pp. 1–17, Mar. 2023.

[29] E. Zhao, Y. Wang, and Y. Zhang, "Multi-level attention based coreference resolution with gated recurrent unit and convolutional neural networks," *IEEE Access*, vol. 5, pp. 4895–4904, 2023.

[30] Y. P. Xu, J. W. Tan, D. J. Zhu, P. Ouyang, and B. Taheri, "Model identification of the proton exchange membrane fuel cells by extreme learning machine and a developed version of arithmetic optimization algorithm," *Energy Rep.*, vol. 7, pp. 2332–2342, Nov. 2021.

[31] R. M. Rizk-Allah, A. E. Hassanien, and A. Marafie, "An improved equilibrium optimizer for numerical optimization: A case study on engineering design of the shell and tube heat exchanger," *J. Eng. Res.*, Aug. 2023.

[32] Accessed: Jul. 14, 2023. [Online]. Available: https://www.unb.ca/cic/datasets/nsl.html