Blockchain with Single-Valued Neutrosophic Hypersoft Sets Assisted Threat Detection for Secure IoT Assisted Consumer Electronics

Mesfer Al Duhayyim[*1]

[1] Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj 16273, Saudi Arabia
Emails: m.alduhayyim@psau.edu.sa

Abstract

The breakthrough technologies of the Internet of Things (IoT) have modernized classical Consumer Electronics (CE) into next-generation CE with high intelligence and connectivity. This connectivity amongst appliances, actuators, sensors, etc., offers automated control in CE and enables better data availability. However, the data traffic has been exponentially increased owing to its decentralization, diversity, and increasing number of CE devices. Furthermore, the static network-based approaches need exclusive management and manual configuration of CE devices. The generalization of a Neutrosophic Hypersoft Set (NHSS) is a concept of a soft set. This architecture is a mixture of neutrosophic sets with hypersoft sets. Therefore, the study introduce a Blockchain with Single-Valued Neutrosophic Hypersoft Sets Assisted Threat Detection (BCSVNHS-TD) technique for Secure IoT Assisted CE. The presented BCSVNHS-TD technique applies BC technology for secure communication among CEs. For threat detection, the BCSVNHS-TD method introduces the SVNHS model. Also, the parameter selection of the SVNHS method takes place using the chicken swarm optimization (CSO) technique. An extensive set of tests was involved for exhibiting the better effiency of the BCSVNHS-TD method. The experimental results emphasized that the BCSVNHS-TD method reaches optimal results over other techniques

Keywords: Internet of Things; Blockchain; Consumer Electronics; Neutrosophic Set; Chicken Swarm Optimization

1. Introduction

The Internet of Things (IoT) is a network, which is inserted with software program and sensor, which use Internet to convey data [1]. The combination of IoT with conventional Consumer electronics (CE) was modernized into next-generation CE with greater connectivity and intelligence. This developed data accessibility and automated device in the CE system are prepared probable by the connectivity of appliances, actuators, sensors, etc.,[2]. However, the connection of CE device are distantly retrieved at any time and anywhere in the global with the use of processing devices, such as smartphones, smartwatches, and laptops to which they are linked. These smart devices are utilized in numerous areas even in smart homes [3]. The IoT device's growth enlarged the data network bandwidth demand. However, many IoT devices contain resource restraints, making it more challenging to perform the conventional safety models for system protection besides cyber-attacks [4]. Significant concerns regarding IoT devices develop when there is a demand to procedure sensitive data. Hence, it is vital to present the MEC platform that allows addition to be executed at the end of network to find out the resource-constraint issues in IoT models. MEC permits IoT to unload higher computation-intensive tasks to the near-edge server [5].

As the IoT has become one of the powerful forces of the present manufacturing revolution and the method for gathering live-reliant data, it is important to take cybersecurity [6]. Therefore, a Network Intrusion Detection System (NIDS) is a must, which can able to identify present and future attacks for protecting the IoT network and the systems constructed on it. Cyber attackers start interior attacks over the compromised IoT devices related to

DOI: https://doi.org/10.54216/IJNS.250114
Received: April 27, 2024 Revised: June 02, 2024 Accepted: July 01, 2024

the system [7]. The 3rd parties outer the foremost network start exterior attacks. There are mainly 3 common elements of NIDS like Analysis, Observation, and Detection. The Observation unit observes the network traffic, patterns, and resources [8]. Detection and Analysis are the essential parts of NIDS, which can able to identify intrusions based on assumed instructions. If an intrusion is identified, then the alert component developed attack flags. Since the growth of NIDS for IoT methods signifies a major task for data security researchers, this study has enclosed the next topics like recognition model, safety threats, NIDS placement tactic, and validation tactic [9]. The theory that derived to the forefront with the research of fuzzy set (FS) to overwhelm uncertainty is the N-sets. Also, this theory is a simplification of intuitionistic FS. The theory is mainly employed to state uncertainty contains a logic set with 3 modules, which are independent of each other, containing indeterminacy, truth, and falsity memberships [10]. Hence, the most significant benefit of this numerical technique is its capability to procedure unknown data, which are not handled by FS and intuitionistic FS.

This study introduces a Blockchain with Single-Valued Neutrosophic Hypersoft Sets Assisted Threat Detection (BCSVNHS-TD) technique for Secure IoT Assisted CE. The presented BCSVNHS-TD technique applies BC technology for secure communication among CEs. For threat detection, the BCSVNHS-TD technique introduces the SVNHS model. Also, the parameter range of the SVNHS method takes place using the chicken swarm optimization (CSO) method. A wide set of experimentations was involved for exhibiting the superior results of the BCSVNHS-TD technique.

2. Literature Survey

Sasikumar et al. [11] presented a lightweight hierarchical attribute-based encryption (HABE) system incorporating BC and edge computing. This system provides an IoT data encryption system for processing the data. Furthermore, the study presents a BC-combined data-sharing system that allows users to share information through cloud storage and edge computing. Especially, IoT devices integrate an encryption-based authentication scheme for verifying the access rights of the users at the network's edge in a decentralized way. Javeed et al. [12] propose a new Software-Defined Networking (SDN)-orchestrated DL technique for designing a smart IDS for the smart CE system. In the proposed method, the SDN architecture is first considered to facilitate re-configuration over a static network system and deals with the decentralized structure of a smart CE system. Next, a DL-based IDS with Cuda-assisted BLSTM (Cu-BLSTM) is developed to recognize the attack type in the smart CE systems. In [13], proposed a permission-based BC network that makes use of the arbiter PUF technique for securing the encryption keys of IoT devices. Initially, a collaborative detection model is applied for DDoS detection on IoT devices with the ML-based ensemble algorithm, providing better detection and lower false-positive rates than the other classification algorithm. Then, the model integrated the BC network that steadily shares the alarm signal to the network nodes through secured authentication.

Kumar et al. [14] introduced a BC-enabled eXplainable AI (XAI) method. Particularly, BC is initially used for validating and storing information between cloud service providers by conducting a Clique Proof-of-Authority (C-PoA) consensus. Next, a new DL-based threat-hunting strategy is constructed by integrating Parallel Stacked LSTM (PSLSTM) models with an MHA module for more accurate detection of attack. Gupta et al. [15] introduce a novel concept for secured and privacy-preserving decentralized federated learning, to modified recommendation within the CE field. This technique leverages the power of homomorphic encryption. Furthermore, the BC is leveraged to create a decentralized, safe foundation for the management and interchange of data.

Khandekar and Ahmad [16] proposed a holistic solution with the combination of BC and DL models. In the proposed work, a federated BC incorporates distributed private clusters for storing secure information. Then, the study presents a decentralized hierarchical BC-based multi-chain code access control to protect the security of IoT. Moreover, consortium DL determines the relevant AC and best threshold parameters. In [17], developed a BC-Enabled Secure Smart Home Network with Gradient-Based Optimizer using Hybrid DL (BSSHN-GBOHDL) algorithm. The proposed method exploits the BC framework for improving data confidentiality in smart homes. Furthermore, this approach detects malicious activity in the smart homes through the three underlying processes including data pre-processing, HDL-based malicious activity identification, and BO-based parameter fine-tuning.

3. The Proposed Method

In this paper, we design a new BCSVNHS-TD model for secure IoT-assisted CE. To accomplish that, the BCSVNHS-TD technique comprises three distinct kinds of stages such as BC technology, SVNHS-based threat recognition, and CSO-based hyperparameter tuning are represented in Fig. 1.

DOI: https://doi.org/10.54216/IJNS.250114
Received: April 27, 2024 Revised: June 02, 2024 Accepted: July 01, 2024

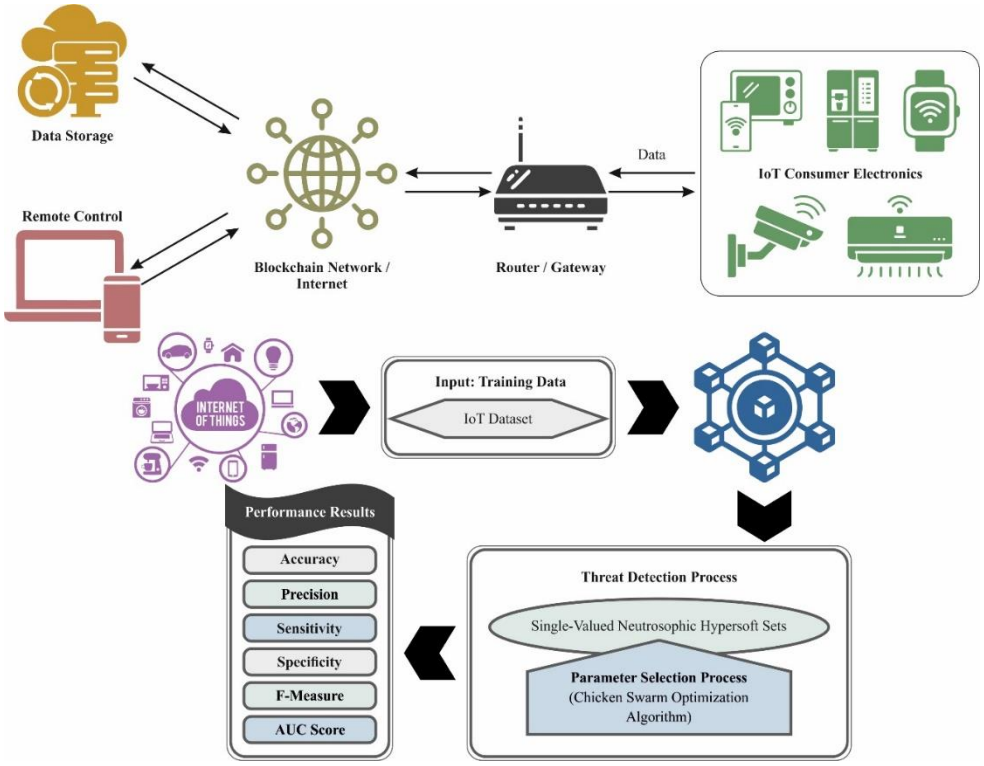

Figure 1: Overall process of BCSVNHS-TD technique

A. Stage I: BC Technology

At the primary stage, the presented BCSVNHS-TD technique applies BC technology for secure communication among CEs. BC is a method of recording data that becomes more challenging or difficult for the network to be manipulated, altered, or hacked [18]. As a decentralized technology, BC distributes and duplicates transactions through the computer network contributing to the BC. BC technology is a framework where the transactional information is stored, alternatively referred to as the block, of the public in numerous databases, called the "chain," in the connected network over a peer-to-peer node. Generally, this storage is represented as a 'digital ledger.' In this ledger, all the transactions are approved by the encrypted signature of the user that validates these transactions and protects them from tampering. Therefore, the digital ledger information comprises of higher level of security. The BC is a decentralized, distributed, and immutable ledger at its core that includes a chain of blocks and all the blocks have a set of data. The block is connected via a cryptographic technique and forms a chronological chain of information. The BC framework is intended for ensuring data security using its consensus model which has a distributed network that agrees on the transaction validity before adding them to the BC.

B. Stage II: SVNHS-based Threat Detection

For threat detection, the BCSVNHS-TD technique introduces the SVNHS model. This section analyses soft sets (SS), hypersoft sets (HS), and NHS [19].

The SS was proposed for handling random decision-making issues and vague states. Consider $\mathfrak{M} = \{\mathfrak{N}_1, \mathfrak{N}_2, \mathfrak{N}_3, \ldots \mathfrak{N}_s\}$ is a alternative set, and]) is a attribute set. Where $\mathcal{P}(\mathfrak{M})$ presents the power set of $\mathfrak{M}$ and $\mathcal{A} \subset \mathcal{P}$. A set $(\lambda, \mathcal{A})$ is named SS over $\mathfrak{M}$, whereas the set λ as assumed by

$$\lambda: \mathcal{A} \to \mathcal{P}(\mathfrak{M}) \tag{1}$$

Assume that parameter set as $\mathcal{P}$ and finite set as $y = \{y_1, y_2, y_3, \ldots y_s\}$. The power set of y was signified as (y). Assume $v^1, v^2, v^3 \ldots v^n$ for $n \geq 1$ as n definite feature, where equivalent feature set values are $\mathfrak{Z}^1, \mathfrak{Z}^2, \mathfrak{Z}^3, \ldots \mathfrak{Z}^n$ with $\mathfrak{Z}^l \cap \mathfrak{Z}^m = \emptyset$ for $l \neq m, l, m = 1,2 \ldots n$, correspondingly, and their sets as $\sigma = \mathfrak{Z}^1 \times \mathfrak{Z}^2 \times \mathfrak{Z}^3 \times \ldots \times \mathfrak{Z}^n$. Next, the set $(\mathfrak{P}, \mathcal{W})$ is named NHSS over y, whereas $\mathfrak{P}: \mathfrak{Z}^1 \times \mathfrak{Z}^2 \times \mathfrak{Z}^3 \times \ldots \times \mathfrak{Z}^n \to \mathcal{P}(\mathbb{Y})$ and $\mathfrak{P}(\mathfrak{Z}^1 \times \mathfrak{Z}^2 \times \mathfrak{Z}^3 \times \ldots \times \mathfrak{Z}^t) = \mathfrak{P}(\sigma)$, while $t \leq n$

$$= \left\{\left\{y, \mathbb{t}(\mathfrak{P}(\sigma)), \mathbb{i}(\mathfrak{P}(\sigma)), \mathbb{f}(\mathfrak{P}(\sigma)), y \in \mathcal{Y}\right\}\right\}$$

DOI: https://doi.org/10.54216/IJNS.250114
Received: April 27, 2024 Revised: June 02, 2024 Accepted: July 01, 2024

Here, $\mathbb{t}$, $\mathbb{i}$, and $\mathbb{f}$ denote the truth, indeterminacy, and false degrees correspondingly thus $\mathbb{t}$, $\mathbb{i}, \mathbb{f} : \mathbb{Y} \to [0,1]$ with

$$0 \leq \mathbb{t}(\mathfrak{P}(\sigma)) + \mathbb{i}(\mathfrak{P}(\sigma)) + \mathbb{f}(\mathfrak{P}(\sigma)) \leq 3. \quad (2)$$

Assume $\mathcal{P}$ and $\mathcal{Q}$ as dual NHSs then the Addition, Multiplication, Subtraction, and Division of $\mathcal{P}$ and $\mathcal{Q}$ were definite below

Addition:

$$\mathcal{P} \oplus \mathcal{Q} = \{\{\sigma, \mathbb{t}_{\mathcal{P}}(\mathfrak{P}(\sigma)) + \mathbb{t}_{\mathcal{Q}}(\mathfrak{P}(\sigma)) - \mathbb{t}_{\mathcal{P}}(\mathfrak{P}(\sigma))\mathbb{t}_{\mathcal{Q}}(\mathfrak{P}(\sigma)), \mathbb{i}_{\mathcal{P}}(\mathfrak{P}(\sigma))\mathbb{i}_{\mathcal{Q}}(\mathfrak{P}(\sigma)), \times \mathbb{f}_{\mathcal{P}}(\mathfrak{P}(\sigma))\mathbb{f}_{\mathcal{Q}}(\mathfrak{P}(\sigma)))\} \quad (3)$$

Multiplication:

$$\mathcal{P} \otimes \mathcal{Q} = \{\{\sigma, \mathbb{t}_{\mathcal{P}}(\mathfrak{P}(\sigma))\mathbb{t}_{\mathcal{Q}}(\mathfrak{P}(\sigma)), \times \mathbb{i}_{\mathcal{P}}(\mathfrak{P}(\sigma)) + \mathbb{i}_{\mathcal{Q}}(\mathfrak{P}(\sigma)) - \mathbb{i}_{\mathcal{P}}(\mathfrak{P}(\sigma))\mathbb{i}_{\mathcal{Q}}(\mathfrak{P}(\sigma)), \times \mathbb{f}_{\mathcal{P}}(\mathfrak{P}(\sigma)) + \mathbb{f}_{\mathcal{Q}}(\mathfrak{P}(\sigma)) - \mathbb{f}_{\mathcal{P}}(\mathfrak{P}(\sigma))\mathbb{f}_{\mathcal{Q}}(\mathfrak{P}(\sigma)))\} \quad (4)$$

Subtraction:

$$\mathcal{P} \ominus \mathcal{Q} = \left\{\left\{\sigma, \frac{\mathbb{t}_{\mathcal{P}}(\mathfrak{P}(\sigma)) - \mathbb{t}_{\mathcal{Q}}(\mathfrak{P}(\sigma))}{1 - \mathbb{t}_{\mathcal{Q}}(\mathfrak{P}(\sigma))} \times \frac{\mathbb{i}_{\mathcal{P}}(\mathfrak{P}(\sigma))}{\mathbb{i}_{\mathcal{Q}}(\mathfrak{P}(\sigma))}, \frac{\mathbb{f}_{\mathcal{P}}(\mathfrak{P}(\sigma))}{\mathbb{f}_{\mathcal{Q}}(\mathfrak{P}(\sigma))}\right\}\right\} \quad (5)$$

Which is valid beneath the condition $\mathcal{P} \geq \mathcal{Q}, \mathbb{t}_{\mathcal{Q}}(\mathfrak{P}(\sigma)) \neq 1, \mathbb{i}_{\mathcal{Q}}(\mathfrak{P}(\sigma)) \neq 0, \mathbb{f}_{\mathcal{Q}}(\mathfrak{P}(\sigma))0$

Division:

$$\mathcal{P} \oslash \mathcal{Q} = \left\{\left\{\sigma, \frac{\mathbb{t}_{\mathcal{P}}(\mathfrak{P}(\sigma))}{\mathbb{t}_{\mathcal{Q}}(\mathfrak{P}(\sigma))} \frac{\mathbb{i}_{\mathcal{P}}(\mathfrak{P}(\sigma)) - \mathbb{i}_{\mathcal{Q}}(\mathfrak{P}(\sigma))}{1 - \mathbb{i}_{\mathcal{Q}}(\mathfrak{P}(\sigma))}, \times \frac{\mathbb{f}_{\mathcal{P}}(\mathfrak{P}(\sigma)) - \mathbb{f}_{\mathcal{Q}}(\mathfrak{P}(\sigma))}{1 - \mathbb{f}_{\mathcal{Q}}(\mathfrak{P}(\sigma))}\right\}\right\} \quad (6)$$

Which is valid beneath the condition $\mathcal{P} \leq \mathcal{Q}, \mathbb{t}_{\mathcal{Q}}(\mathfrak{P}(\sigma)) \neq 0, \mathbb{i}_{\mathcal{Q}}(\mathfrak{P}(\sigma)) \neq 1, \mathbb{f}_{\mathcal{Q}}(\mathfrak{P}(\sigma)) \neq 1$

Assume $\mathcal{P}$ and $\mathcal{Q}$ as dual NHSs then Inclusion, Compliment, Union, Intersection, and Equality of $\mathcal{P}$ and $\mathcal{Q}$ were expressed below

Complement:

$$\mathcal{P}^c = \left\{\left\{\sigma, \mathbb{f}_{\mathcal{P}}(\mathfrak{P}(\sigma)), 1 - \mathbb{i}_{\mathcal{P}}(\mathfrak{P}(\sigma)), \mathbb{t}_{\mathcal{P}}(\mathfrak{P}(\sigma))\right\}\right\} \quad (7)$$

In this, the instance is dependent upon the pendency neutrosophic model, all truth, indeterminacy, and false degrees are reliant.

$$And\ \mathcal{P}^c = \left\{\left\{1 - \mathbb{t}_{\mathcal{P}}(\mathfrak{P}(\sigma)), 1 - \mathbb{i}_{\mathcal{P}}(\mathfrak{P}(\sigma)), 1 - \mathbb{f}_{\mathcal{P}}(\mathfrak{P}(\sigma))\right\}\right\} \quad (8)$$

In this, the instance is dependent upon the independency neutrosophic model, all truth, indeterminacy, and false are self-determining.

Inclusion:

$\mathcal{P} \subseteq \mathcal{Q}$ if and only if $\mathbb{t}_{\mathcal{P}}(\mathfrak{P}(\sigma)) \leq \mathbb{t}_{\mathcal{P}}(\mathfrak{P}(\sigma))$,

$$\mathbb{i}_{\mathcal{P}}(\mathfrak{P}(\sigma)) \leq \mathbb{i}_{\mathcal{Q}}(\mathfrak{P}(\sigma))\mathbb{f}_{\mathcal{P}}(\mathfrak{P}(\sigma)) \geq \mathbb{f}_{\mathcal{Q}}(\mathfrak{P}(\sigma))$$

$$for\ any\ \mathfrak{P}(\sigma) \quad (9)$$

Equality:

$$\mathcal{P} = \mathcal{Q}\ if\ and\ only\ if\ \mathcal{P}subseteq\mathcal{Q}\ and\ \mathcal{Q}subseteq\mathcal{P} \quad (10)$$

Union:

DOI: https://doi.org/10.54216/IJNS.250114
Received: April 27, 2024 Revised: June 02, 2024 Accepted: July 01, 2024

$$\mathcal{P} \cup \mathcal{Q} = \{\{\sigma, \mathbb{t}_{\mathcal{P}}(\wp(\sigma)) v \mathbb{t}_{\mathcal{Q}}(\mathfrak{P}(\sigma)), \mathbb{i}_{\mathcal{P}}(\mathfrak{P}(\sigma)) \times\wedge \mathbb{i}_{\mathcal{Q}}(\mathfrak{P}(\sigma)),$$
$$\mathbb{f}_{\mathcal{P}}(\mathfrak{P}(\sigma)) \wedge \mathbb{f}_{\mathcal{Q}}(\mathfrak{P}(\sigma))\} \quad (11)$$

Intersection:

$$\mathcal{P} \cap \mathbb{Q} = \{\{\sigma, \mathbb{t}_{\mathcal{P}}(\mathfrak{P}(\sigma)) \wedge \mathbb{t}_{\mathcal{Q}}(\mathfrak{P}(\sigma)), \mathbb{i}_{\mathcal{P}}(\mathfrak{P}(\sigma)) \times\vee \mathbb{i}_{\mathcal{Q}}(\mathfrak{P}(\sigma)),$$
$$\mathbb{f}_{\mathcal{P}}(\mathfrak{P}(\sigma)) \vee \mathbb{f}_{\mathcal{Q}}(\mathfrak{P}(\sigma))\} \quad (12)$$

Assume $\mathcal{P}$ as an SVNHS over the general universe y. Where $\mathcal{P}$ refers to an Absolute SVNHS if

$$\mathbb{t}_{\mathcal{P}}(\mathfrak{P}(\sigma)) = 1, \mathbb{i}_{\mathcal{P}}(\mathfrak{P}(\sigma)) = 0 \; and \; \mathbb{f}_{\mathcal{P}}(\mathfrak{P}(\sigma)) = 0 \quad (13)$$

Assume $\mathcal{P}$ as an SVNHSS over the general universe y. While $\mathcal{P}$ is assumed to be Empty SVNHS if

$$\mathbb{t}_{\mathcal{P}}(\mathfrak{P}(\sigma)) = 0, \mathbb{i}_{\mathcal{P}}(\mathfrak{P}(\sigma)) = 0 \; and \; \mathbb{f}_{\mathcal{P}}(\mathfrak{P}(\sigma)) = 1 \quad (14)$$

C. Stage III: Hyperparameter Tuning

Eventually, the parameter selection of the SVNHS technique takes place utilizing the CSO technique. CSO is bio-inspired optimization approach stimulated by the behaviors of CS [20]. The chicken with least strength is known as a chick and with maximum strength is known as a rooster. The biological behavior of chickens follows the mother to find food. The two stages in the CS technique are initialization and updating. The number of roosters and population size, hens, and chicks are defined at the initialization stage, and later the fitness values are assessed. Based on the food-searching ability, the member of the group varies, and the food-searching capability of the rooster differs based on the fitness value. The location updating equation for the rooster is represented as follows:

$$x_{i,j}^{t+1} = x_{i,j}^{t} \times \left(1 + randn(0, \sigma^2)\right) \quad (15)$$

$$\text{If} f_i \leq f_k, then \; \sigma^2 = 1, or \; else \sigma^2 = \exp\left(\frac{(f_k - f_i)}{|f_i| + \varepsilon}\right) \quad (16)$$

Where $randn(0, \sigma^2)$ is the Gaussian distribution function, f is the value of fitness equivalent to x, k indicates the index of the rooster, and division by 0 is prevented by presenting the constant σ.

The rooster follows hens to find food and the location upgrading formulation for hen is shown below

$$x_{i,j}^{t+1} = x_{i,j}^{t} + S_1 \times rand \times \left(x_{r1,j}^{t} - x_{i,j}^{t}\right) + S_2 \times rand\left(x_{r2,j}^{t} - x_{i,j}^{t}\right) \quad (17)$$

$$S_1 = \exp\left(\frac{f_i - f_{r1}}{abs(f_i) + \varepsilon}\right) \; and \; S_2 = \exp(f_{r2} - f_i) \quad (18)$$

Where $r_1, r_2 \varepsilon [1, N]$ are not equal, $rand$ is selected between 0 and 1.

Generally, the chick follows the mother, and the mathematical formula for position updating of the chick is shown as follows:

$$x_{i,j}^{t+1} = x_{i,j}^{t} + FL \times \left(x_{m,j}^{t} - x_{i,j}^{t}\right) \quad (19)$$

In Eq. (19), $x_{i,j}^{t}$ refers to the location of the i^{th} mother, FL is chosen between 0 and 1.

A new hybrid mechanism, the GBCS model contains the benefits of both genetic algorithm (GA) and CS algorithms, like robustness, simplicity, the ability to resolve complicated problems, and convergence. In the beginning, the population is generated randomly, and the fitness values are assessed for all the solutions. After, the populace is classified into two sub-gourps, where one group is upgraded as per the GA and the other is upgraded as per the CS model. The novel solution produced by all the operations is integrated with the next generation where the fittest values for K_p and K_j are obtained. Fig. 2 signifies the flowchart of CSO.

DOI: https://doi.org/10.54216/IJNS.250114
Received: April 27, 2024 Revised: June 02, 2024 Accepted: July 01, 2024

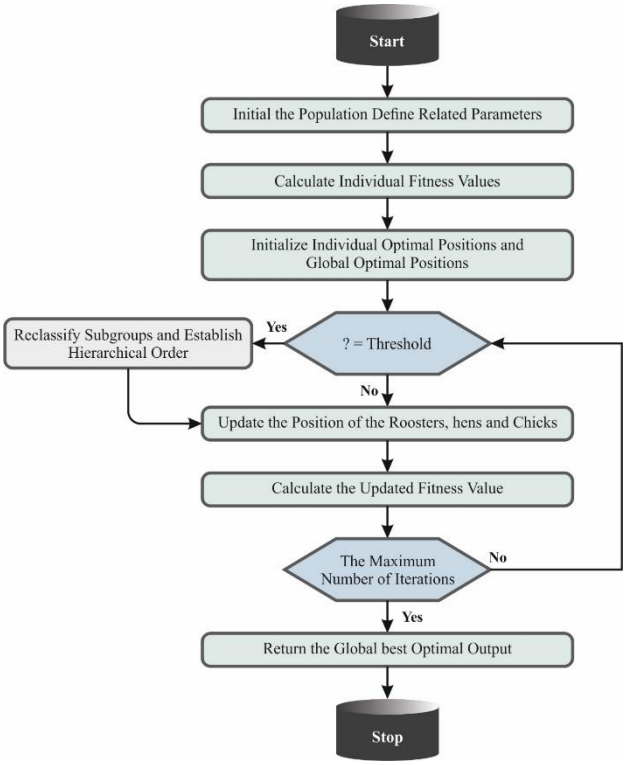

Figure 2: Flowchart of CSO

The fitness range is the major influence manipulating the efficiency of CSO model. The hyperparameter collection method covers the solution encode technique to measure the solution of the candidate. The CSO method take accuracy as the foremost criterion in this paper to project FF and formulated below.

$$Fitness = \max(P) \tag{20}$$

$$P = \frac{TP}{TP + FP} \tag{21}$$

Here, TP and FP signify the value of true and false positives, correspondingly.

4. Result Analysis and Discussion

The simulation analysis of the BCSVNHS-TD technique is examined using the BoT-IoT dataset, encompassing 23500 samples with 10 class labels are represented in Table 1.

Table 1: Details on dataset

Type of Event	No. of Data Record
Backdoor	2500
DoS	2500
DDoS	2500
Injection	2500
MITM	1000
Scanning	2500
Ransomware	2500
Password	2500
XSS	2500
Normal	2500

DOI: https://doi.org/10.54216/IJNS.250114
Received: April 27, 2024 Revised: June 02, 2024 Accepted: July 01, 2024

Total Data Record	23500

Fig. 3 forms the classifier results of the BCSVNHS-TD system on the test database. Figs. 3a-3b signifies the confusion matrices presented by the BCSVNHS-TD method on 70:30 of TRP/TSP. The outcome represented that the BCSVNHS-TD method has known and categorized different classes exactly. Equally, Fig. 3c establishes the PR analysis of the BCSVNHS-TD method. The outcome described that the BCSVNHS-TD method has increased the greatest performance of PR on every classes. Finally, Fig. 3d determines the ROC investigation of the BCSVNHS-TD method. The results represented that the BCSVNHS-TD approach has caused in promising solution with the greatest ROC value below dissimilar class labels.

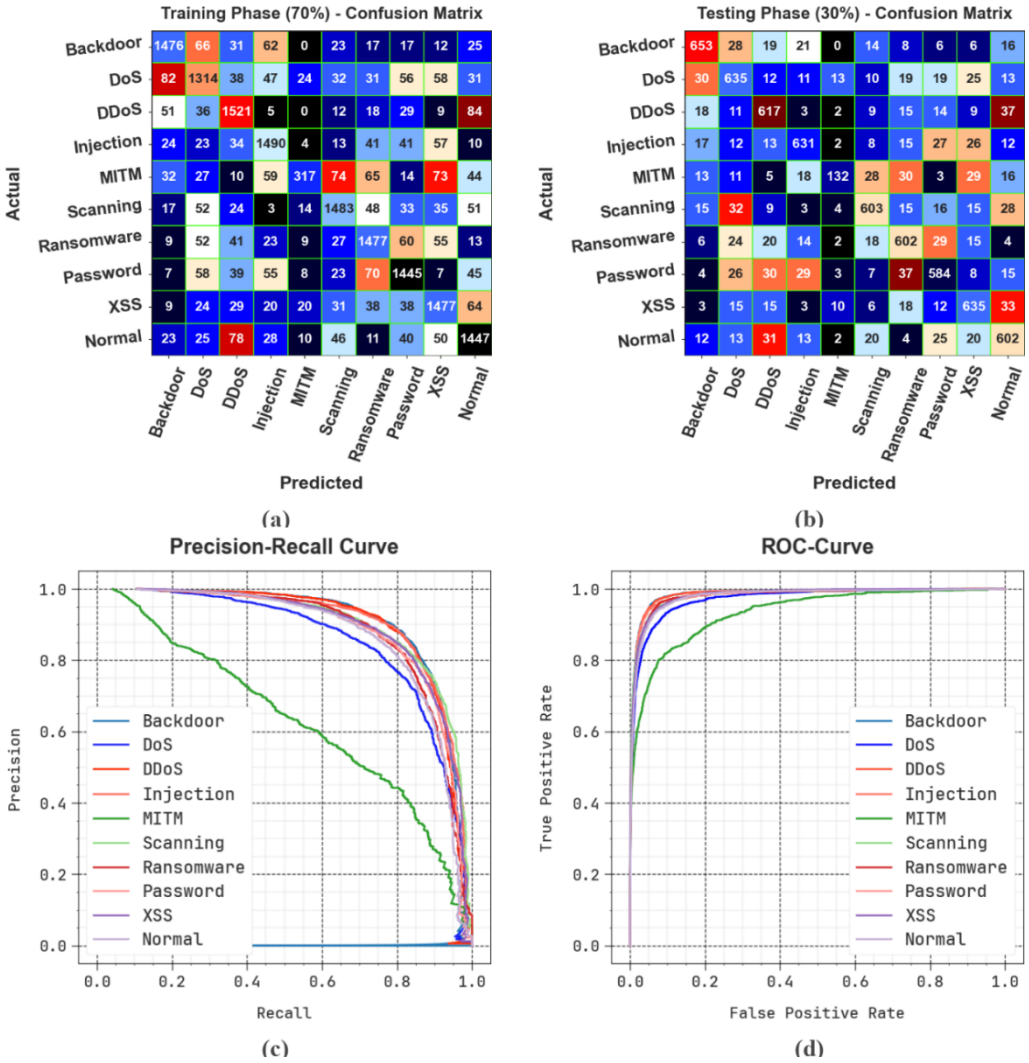

Figure 3: Classifier outcome of (a-b) Confusion matrices and (c-d) PR and ROC

In Table 2 and Fig. 4, a brief threat detection analysis of the BCSVNHS-TD system on 70%TRP and 30%TSP is defined. The experimentation values stated that the BCSVNHS-TD method correctly recognized 10 classes. With 70%TRAS, the BCSVNHS-TD model presented an average $accu_y$, $prec_n$, $sens_y$, $spec_y$, $F_{measure}$, and AUC_{score} of 96.35%, 81.46%, 79.52%, 97.96%, 80.01%, and 88.74%, respectively. In addition, with 30%TESS, the BCSVNHS-TD system offered average $accu_y$, $prec_n$, $sens_y$, $spec_y$, $F_{measure}$, and AUC_{score} of 96.15%, 80.56%, 78.62%, 97.85%, 79.17%, and 88.24%, respectively.

Table 2: Threat detection outcome of BCSVNHS-TD technique on 70%TRAS and 30%TESS

Classes	$Accu_y$	$Prec_n$	$Sens_y$	$Spec_y$	$F_{Measure}$	AUC_{Score}
TRAS (70%)						
Backdoor	96.92	85.32	85.37	98.27	85.34	91.82
DoS	95.37	78.35	76.71	97.54	77.52	87.12

DOI: https://doi.org/10.54216/IJNS.250114
Received: April 27, 2024 Revised: June 02, 2024 Accepted: July 01, 2024

DDoS	96.55	82.44	86.18	97.79	84.27	91.98
Injection	96.66	83.15	85.78	97.95	84.44	91.86
MITM	97.04	78.08	44.34	99.43	56.56	71.89
Scanning	96.61	84.07	84.26	98.09	84.17	91.17
Ransomware	96.18	81.33	83.64	97.69	82.47	90.66
Password	96.11	81.50	82.24	97.77	81.87	90.01
XSS	96.18	80.58	84.40	97.58	82.44	90.99
Normal	95.88	79.77	82.31	97.50	81.02	89.91
Average	96.35	81.46	79.52	97.96	80.01	88.74
TESS (30%)						
Backdoor	96.65	84.70	84.70	98.12	84.70	91.41
DoS	95.40	78.69	80.69	97.25	79.67	88.97
DDoS	96.14	80.03	83.95	97.56	81.94	90.75
Injection	96.50	84.58	82.70	98.17	83.63	90.44
MITM	97.29	77.65	46.32	99.44	58.02	72.88
Scanning	96.35	83.40	81.49	98.10	82.43	89.79
Ransomware	95.84	78.90	82.02	97.45	80.43	89.73
Password	95.60	79.46	78.60	97.61	79.03	88.10
XSS	96.20	80.58	84.67	97.57	82.57	91.12
Normal	95.55	77.58	81.13	97.24	79.31	89.19
Average	96.15	80.56	78.62	97.85	79.17	88.24

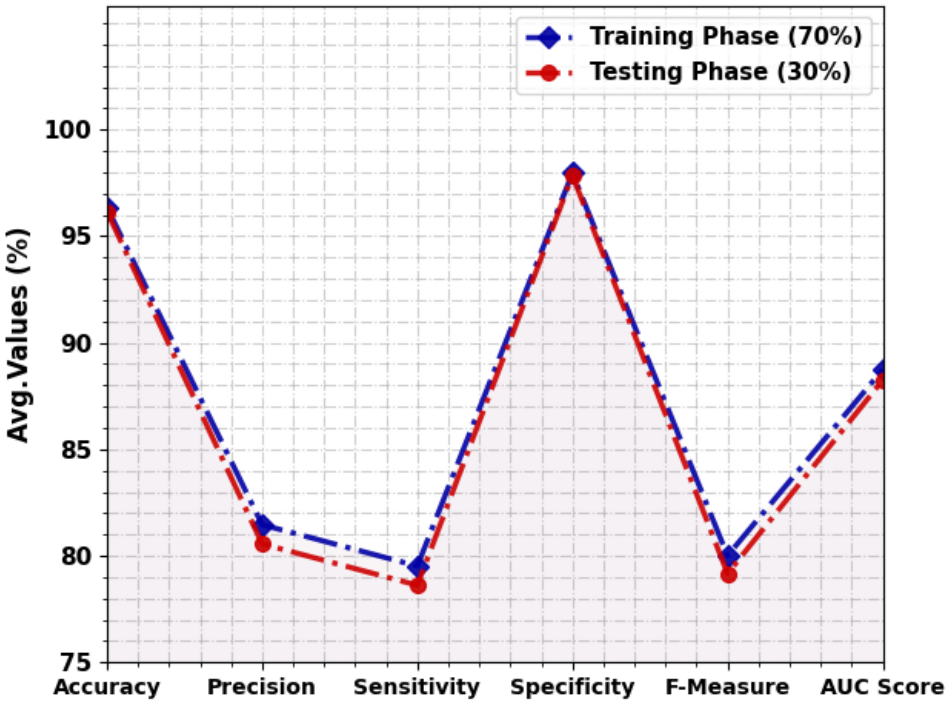

Figure 4: Average outcome of BCSVNHS-TD technique on 70%TRAS and 30%TESS

In Fig. 5, the training and validation accuracy outcomes of the BCSVNHS-TD system are established. The outcome emphasized that the training and validation accuracy values show a rising tendency which notified the capability of the BCSVNHS-TD technique with amended performance over numerous iterations.

In Fig. 6, the training and validation loss graph of the BCSVNHS-TD system is shown. It is denoted that the training and validation accuracy values exemplify a declining tendency, which notified the skill of the BCSVNHS-TD approach in balancing a trade-off between data fitting and generalization.

DOI: https://doi.org/10.54216/IJNS.250114
Received: April 27, 2024 Revised: June 02, 2024 Accepted: July 01, 2024

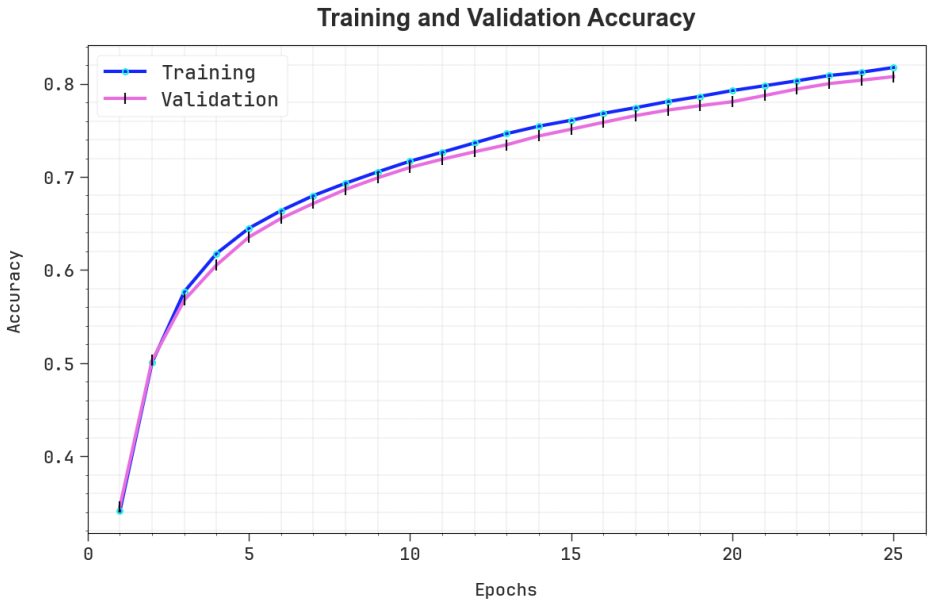

Figure 5: $Accu_y$ curve of the BCSVNHS-TD technique

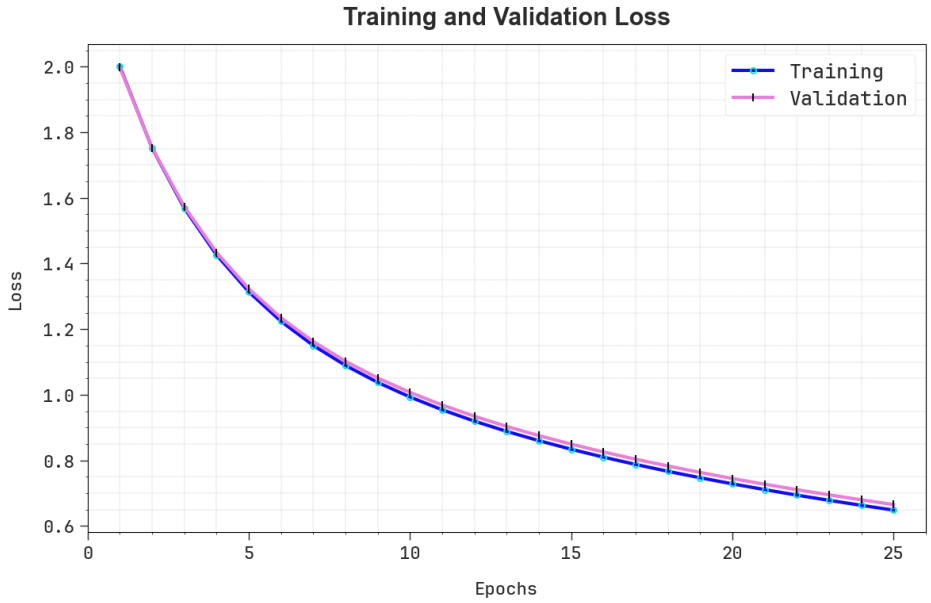

Figure 6: Loss curve of the BCSVNHS-TD technique

In Table 3 and Fig. 7, an extensive comparison study is prepared the improved performance of the BCSVNHS-TD system [21]. The experimental values specified that the DBN, LD, and ensemble bag approaches have increased worse performance over other techniques. Likewise, the LSTM, KNN, SVM, and DT methodologies have gotten closer to performance equated to current approaches. Nevertheless, the BCSVNHS-TD system determines better performance with maximum $accu_y$, $prec_n$, $reca_l$, and $F_{measure}$ of 96.35%, 81.46%, 79.52%, and 80.01%, correspondingly.

Table 3: Comparative analysis of BCSVNHS-TD model with existing approaches

Classifiers	$\boldsymbol{Accu_y}$	$\boldsymbol{Prec_n}$	$\boldsymbol{Reca_l}$	$\boldsymbol{F_{Measure}}$
BCSVNHS-TD	96.35	81.46	79.52	80.01
DT	95.31	78.23	73.09	79.78
Ensemble Bag	92.11	80.64	77.30	76.18

DOI: https://doi.org/10.54216/IJNS.250114
Received: April 27, 2024 Revised: June 02, 2024 Accepted: July 01, 2024

KNN	94.53	77.22	69.97	76.07
DBN	90.70	80.15	65.87	70.52
LD Classifier	92.12	77.91	78.45	79.52
SVM	95.81	76.51	68.80	71.92
LSTM	92.20	75.99	66.26	67.05

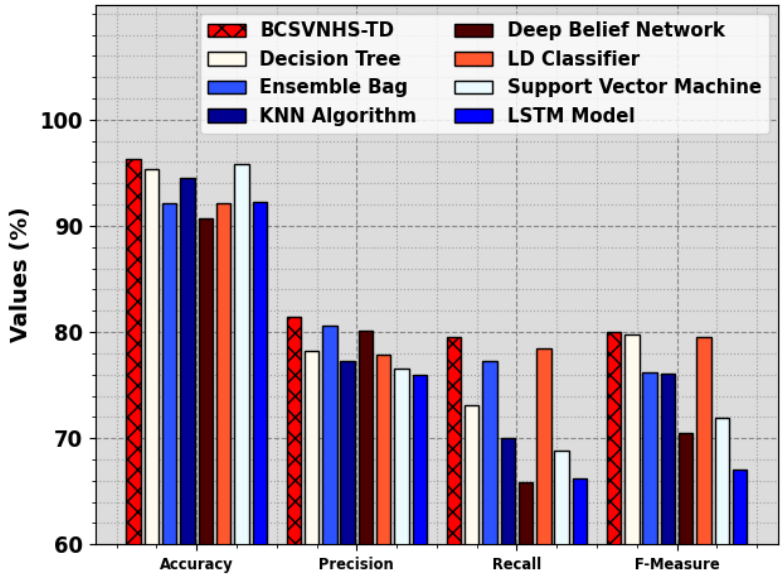

Figure 7: Comparative analysis of BCSVNHS-TD method with existing models

In Table 4 and Fig. 8, the comparative training time (TRT) and testing time (TST) analysis of the BCSVNHS-TD system with present techniques are made. The results specified that the DBN, LD, and ensemble bag methods have gained worse performance over other approaches. Besides, the LSTM, KNN, SVM, and DT models have attained closer performance equated to recent approaches. Nevertheless, the BCSVNHS-TD technique determines better performance with a smaller TRT of 1.85s and TST of 4.46s, respectively.

Table 4: Time analysis of BCSVNHS-TD method with present approaches

Time (sec)		
Classifiers	Training	Testing
BCSVNHS-TD	1.85	4.46
Decision Tree	4.86	6.92
Ensemble Bag	3.73	7.89
KNN Algorithm	5.71	7.89
Deep Belief Network	4.57	8.02
LD Classifier	3.69	8.10
SVM Model	3.75	7.01
LSTM Model	2.59	7.37

DOI: https://doi.org/10.54216/IJNS.250114
Received: April 27, 2024 Revised: June 02, 2024 Accepted: July 01, 2024

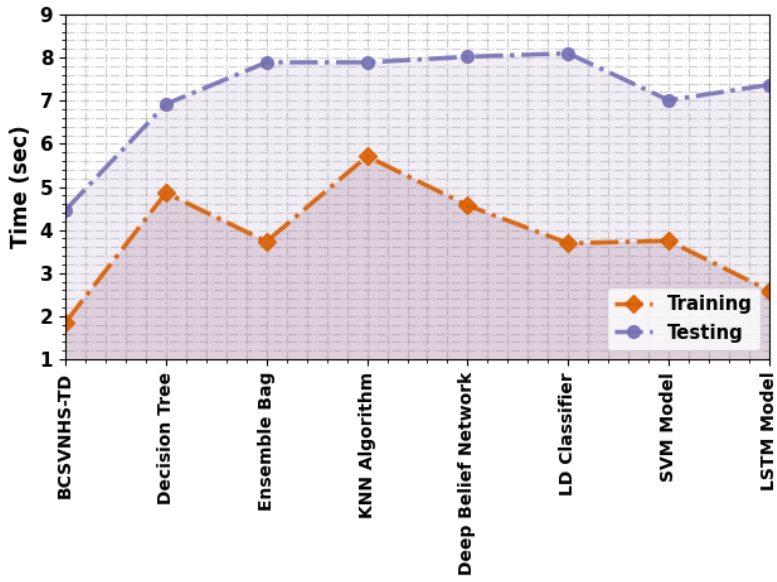

Figure 8: Time analysis of BCSVNHS-TD method with existing approaches

5. Conclusion

In this paper, we design a new BCSVNHS-TD method for secure IoT-assisted CE. To accomplish that, the BCSVNHS-TD technique comprises three distinct kinds of stages such as BC technology, SVNHS-based threat detection, and CSO-based hyperparameter tuning. At the primary stage, the presented BCSVNHS-TD technique applies BC technology for secure communication among CEs. For threat detection, the BCSVNHS-TD technique introduces the SVNHS model. Also, the parameter selection of the SVNHS approach takes place using the CSO technique. A wide set of experimentations was involved for exhibiting the superior results of the BCSVNHS-TD method. The experimental results emphasized that the BCSVNHS-TD method reaches optimal results over other approaches.

Funding: "The authors extend their appreciation to Prince Sattam bin Abdulaziz University for funding this research work through the project number (PSAU/2024/01/29442)"

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

References

[1] Smarandache F., and Abobala, M., " n-Refined Neutrosophic Vector Spaces", International Journal of Neutrosophic Science, Vol. 7, pp. 47-54, 2020.

[2] Tuqa A. H. Al-Tamimi, Luay A. A. Al-Swidi , Ali H. M. Al-Obaidi. "Partner Sets for Generalizations of MultiNeutrosophic Sets." International Journal of Neutrosophic Science, Vol. 24, No. 1, 2024 ,PP. 08-13

[3] Parimala, M., Karthika, M. and Smarandache, F., 2020. A review of fuzzy soft topological spaces, intuitionistic fuzzy soft topological spaces and neutrosophic soft topological spaces. International Journal of Neutrosophic Science, Vol. 10, No. 2, 2020 ,PP. 96-104.

[4] Ashraf, S. and Abdullah, S., 2020. Decision support modeling for agriculture land selection based on sine trigonometric single valued neutrosophic information. International Journal of Neutrosophic Science (IJNS), 9(2), pp.60-73..

[5] Hazra, A., Alkhayyat, A. and Adhikari, M., 2022. Blockchain-aided integrated edge framework of cybersecurity for Internet of Things. IEEE Consumer Electronics Magazine.

[6] Saad, M., Bhutta, M.R., Kim, J. and Chung, T.S., 2024. A Framework for Enhancing Privacy and Anonymity in Blockchain-Enabled IoT Devices. Computers, Materials & Continua, 78(3).

[7] Bagchi, P., Bera, B., Das, A.K., Shetty, S., Vijayakumar, P. and Karuppiah, M., 2023. Post quantum lattice-based secure framework using aggregate signature for ambient intelligence assisted blockchain-based IoT applications. IEEE Internet of Things Magazine, 6(1), pp.52-58.

DOI: https://doi.org/10.54216/IJNS.250114
Received: April 27, 2024 Revised: June 02, 2024 Accepted: July 01, 2024

[8] Mishra, K.N., Bhattacharjee, V., Saket, S. and Mishra, S.P., 2024. Security provisions in smart edge computing devices using blockchain and machine learning algorithms: a novel approach. Cluster Computing, 27(1), pp.27-52.
[9] Chandrakar, P., Bagga, R., Kumar, Y., Dwivedi, S.K. and Amin, R., 2023. Blockchain based security protocol for device to device secure communication in internet of things networks. Security and Privacy, 6(1), p.e267.
[10] Patel, P., Bhatt, R., Joshi, M., Patil, G., Pal, H. and Qureshi, A.R.K., 2024. Blockchain-Enabled Decentralized Edge Computing in Cyber Security for Intrusion Detection. International Journal of Intelligent Systems and Applications in Engineering, 12(13s), pp.28-40.
[11] Sasikumar, A., Ravi, L., Devarajan, M., Selvalakshmi, A., Almaktoom, A.T., Almazyad, A.S., Xiong, G. and Mohamed, A.W., 2024. Blockchain-Assisted Hierarchical Attribute-Based Encryption Scheme for Secure Information Sharing in Industrial Internet of Things. IEEE Access.
[12] Javeed, D., Saeed, M.S., Ahmad, I., Kumar, P., Jolfaei, A. and Tahir, M., 2023. An intelligent intrusion detection system for smart consumer electronics network. IEEE Transactions on Consumer Electronics.
[13] Babu, E.S., SrinivasaRao, B.K.N., Nayak, S.R., Verma, A., Alqahtani, F., Tolba, A. and Mukherjee, A., 2022. Blockchain-based Intrusion Detection System of IoT urban data with device authentication against DDoS attacks. Computers and Electrical Engineering, 103, p.108287.
[14] Kumar, P., Javeed, D., Kumar, R. and Islam, A.N., 2024. Blockchain and explainable AI for enhanced decision making in cyber threat detection. Software: Practice and Experience.
[15] Gupta, B.B., Gaurav, A. and Arya, V., 2023. Secure and Privacy-Preserving Decentralized Federated Learning for Personalized Recommendations in Consumer Electronics using Blockchain and Homomorphic Encryption. IEEE Transactions on Consumer Electronics.
[16] Khandekar, A. and Ahmad, S.F., 2024. Secured IoT architecture for personalized marketing using blockchain framework with deep learning technology. Cluster Computing, pp.1-16.
[17] Almuqren, L., Mahmood, K., Aljameel, S.S., Salama, A.S., Mohammed, G.P. and Alneil, A.A., 2023. Blockchain Assisted Secure Smart Home Network using Gradient Based Optimizer with Hybrid Deep Learning Model. IEEE Access.
[18] Singh, P., Kumar, A. and Chopra, M., 2023. Real-World Applications of BC Technology in Internet of Things. Machine Learning Applications: From Computer Vision to Robotics, pp.97-122.
[19] Jafar, M.N., Saeed, M., Khan, K.M., Alamri, F.S. and Khalifa, H.A.E.W., 2022. Distance and similarity measures using max-min operators of neutrosophic hypersoft sets with application in site selection for solid waste management systems. Ieee Access, 10, pp.11220-11235.
[20] Aandal, R. and Ravi, A., 2024. Design of Z source converter with the genetic-based chicken swarm algorithm for closed loop control of PV integrated grid. Automatika, 65(3), pp.675-690.
[21] Alosaimi, S. and Almutairi, S.M., 2023. An intrusion detection system using BoT-IoT. Applied Sciences, 13(9), p.5427.

DOI: https://doi.org/10.54216/IJNS.250114
Received: April 27, 2024 Revised: June 02, 2024 Accepted: July 01, 2024