Computers, Materials & Continua
DOI: 10.32604/cmc.2022.025828
Article

Tech Science Press

A Blockchain-Based Architecture for Enabling Cybersecurity in the Internet-of-Critical Infrastructures

Mahmoud Ragab[1,2,3,*] and Ali Altalbe[1]

[1]Information Technology Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[2]Center of Artificial Intelligence for Precision Medicines, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[3]Mathematics Department, Faculty of Science, Al-Azhar University, Naser City, 11884, Cairo, Egypt
*Corresponding Author: Mahmoud Ragab. Email: mragab@kau.edu.sa
Received: 06 December 2021; Accepted: 12 January 2022

Abstract: Due to the drastic increase in the number of critical infrastructures like nuclear plants, industrial control systems (ICS), transportation, it becomes highly vulnerable to several attacks. They become the major targets of cyberattacks due to the increase in number of interconnections with other networks. Several research works have focused on the design of intrusion detection systems (IDS) using machine learning (ML) and deep learning (DL) models. At the same time, Blockchain (BC) technology can be applied to improve the security level. In order to resolve the security issues that exist in the critical infrastructures and ICS, this study designs a novel BC with deep learning empowered cyber-attack detection (BDLE-CAD) in critical infrastructures and ICS. The proposed BDLE-CAD technique aims to identify the existence of intrusions in the network. In addition, the presented enhanced chimp optimization based feature selection (ECOA-FS) technique is applied for the selection of optimal subset of features. Moreover, the optimal deep neural network (DNN) with search and rescue (SAR) optimizer is applied for the detection and classification of intrusions. Furthermore, a BC enabled integrity checking scheme (BEICS) has been presented to defend against the misrouting attacks. The experimental result analysis of the BDLE-CAD technique takes place and the results are inspected under varying aspects. The simulation analysis pointed out the supremacy of the BDLE-CAD technique over the recent state of art techniques with the $accu_y$ of 92.63%.

Keywords: BC; internet of critical infrastructure; ids; deep learning; security; deep neural network; machine learning

1 Introduction

Critical infrastructure system has been utilized for underpinning the functions of an economy and society. Also, it ranges from conventionally-defined physical assets to a broader description of current assets in the fields of agriculture, gas, transportation, water supply, electricity, telecommunication,

public health, security services, and so on [1]. Such transformation is mainly because of the extensive utilization of Internet of Things (IoT) and their considerable aid for critical infrastructure systems in industry 4.0 [2]. The IoT system has become essential part of critical infrastructure in industry 4.0, which creates smart services like smart grids and offers numerous benefits for efficiencies and cost savings. The international data corporation (IDC) have predicted that there would be an estimation of 41.6 billion interconnected IoT device, which generate 79.4 zettabytes (ZB) by 2025 [3].

The industrial control system (ICS) is the core of critical infrastructure system [4]. It is largely accountable for supervisory control and data collection (SCADA), which monitors the control flows and processes of data in industry. The possible application areas of critical infrastructure with IoT are shown in Fig. 1 [5]. The wider adaption of Internet connected IoT devices have offered different challenges to critical infrastructure. Initially, ICS was mainly developed for a closed infrastructure and proprietary without taking care of security problems into account, since conventional critical infrastructure is kind of isolated and is invulnerable to cyber-attacks. With this infrastructure being interconnected to the Internet via IoT system, a wide-ranging of cyberattacks, including malware, Man-in-the-middle attack, distributed denial-of service (DDoS), Brute force, breach, and phishing attacks are threatening the process of ICS [6,7]. The compromised ICS by cyber attackers might generate possible risk for the loss of information [8]. Next, scalability is another challenge where ICS wasn't initially developed to resolve. Assuming the dramatic growth in the volume of data and the number of IoT devices they are analyzing and collecting, the centralized method for data analysis and collection has become a bottleneck of ICS. A decentralized method is crucially needed to satisfy the evolving needs of ICS.

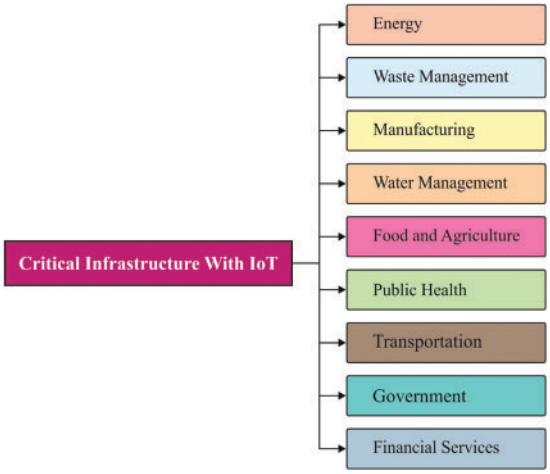

Figure 1: Application areas of critical infrastructures with IoT

Blockchain (BC) and Artificial intelligence (AI) have their own benefits, but, all of them have relative drawbacks. BC has problems relating to scalability, security, energy consumption, efficiency, and privacy, whereas AI systems face problems like effectiveness and interpretability. As two distinct directions of research, they could be associated with one another and have the benefits of natural integration. Both techniques have shared requirements for data trust, analysis, and security, and they could empower one another [9]. For example, AI technique based on three most important components: computing power, data, and algorithms, and the BC could break the island of data and realize the flow of data resources, algorithms, and computing power, according to its specific features, involving immutability, anonymization, and decentralization. Additionally, BC could ensure

the audit traceability and credibility of AI and the credibility of the original data. Furthermore, BC could record the decision-making of AI that assists in analyzing and understanding the behaviour of AI and eventually promote the decision-making of AI, which makes it more explainable, trustworthy, and transparent. The AI technique could improve the BC construction for making it more efficient, secure, and energy-saving [10].

Gumaei et al. [11] presented an architecture which integrates a BC with a deep recurrent neural network (DRNN) and edge computing for 5G-enabled assisted mode detection and drone identification. In the presented approach, raw RF signals of dissimilar drones under various flight modes are collected and sensed remotely on a cloud framework for training a DRNN method and allocate the training models on edge devices to detect their flight modes and drones. BC is utilized in this architecture for securing data transmission and integrity. Alkadi et al. [12] presented a DBF to provide security-based privacy-based BC and distributed IDS with smart contracts in IoT networks. The IDS is applied by a BiLSTM-DL method for handling sequential network data and is measured by the data sets. The smart contract and privacy-based BC methodologies are designed by utilizing the Ethereum library to offer security to the distributed IDS engine.

Singh et al. [13] introduced a DL-based IoT-based framework for a secured smart city in which BC provides a distributed platform at the transmission stage of software defined networks (SDN) and cyber-physical systems (CPS) established the protocol for forwarding information. A DL based cloud is employed at the application layer for resolving transmission scalability, centralization, and latency. Zhang et al. [14] presented an edge intelligence and BC enabled industrial IoT architecture that attains secure and flexible edge service management. Next, developed a credit-differentiated edge transaction approval method and present a cross-domain sharing inspired edge resource scheduling system.

This study designs a novel BC with deep learning empowered cyber-attack detection (BDLE-CAD) in critical infrastructures and ICS. The proposed BDLE-CAD technique aims to identify the existence of intrusions in the network. In addition, the presented enhanced chimp optimization based feature selection (ECOA-FS) technique is applied for the selection of optimal subset of features. Moreover, the optimal deep neural network (DNN) with search and rescue (SAR) optimizer is applied for the detection and classification of intrusions. Furthermore, a BC enabled integrity checking scheme (BEICS) has been presented to defend the misrouting attacks. The experimental result analysis of the BDLE-CAD technique takes place and the results are inspected under varying aspects.

2 The Proposed Model

In this study, a new BDLE-CAD technique has been developed to identify the existence of intrusions in critical infrastructures. The proposed BDLE-CAD technique encompasses ECOA-FS technique for the selection of optimal subset of features. Moreover, the DNN with SAR optimizer is can be used as a classifier and the BEICS has been presented to defend over the misrouting attacks. The experimental result analysis of the BDLE-CAD technique takes place and the results are inspected under varying aspects.

2.1 ECOA Based Feature Selection

Primarily, the ECOA-FS technique is executed to choose the optimal subset of features. The chimp optimization algorithm (COA) is a mathematical method that is dependent upon intelligent diversity [15]. Drive, chase, block, and attack are capable of 4 distinct kinds of chimps that are realized by attacker, obstacle, chaser, and driver. The 4 hunting stages are finalized in 2 phases. In primary stage is the exploration step, and the second step is the exploitation phase. The exploration phase contains

driving, blocking, and chasing the prey. Since the exploitation step, it has attacked the prey. Where the drive and chase are demonstrated as in Eqs. (1) and (2).

$$d = |c \cdot x_{prey}(t) - m \cdot x_{chimp}(t)| \tag{1}$$

$$x_{chimp}(t+1) = x_{prey}(t) - a \cdot d \tag{2}$$

where X_{prey} implies the vector of prey place, x_{chimp} refers the vector of chimp place, t stands for the amount of present iterations, a, c, m represents the coefficient vector and it is attained with Eqs. (3)–(5).

$$a = 2 \cdot f \cdot r_1 - f \tag{3}$$

$$c = 2 \cdot r_2 \tag{4}$$

$$m = chaotic\_value \tag{5}$$

where f implies the non-linearly declined in 2.5 to 0, r_1 and r_2 refers the arbitrary number amongst *zero* and one, and m refers the chaotic vector. The dynamic coefficient f has chosen to distinct curve as well as slope, so the chimps are utilizing distinct capabilities for searching the prey. The chimps are upgrading their places dependent upon another chimp, and this mathematical method is signified by Eqs. (6) and (8).

$$\begin{aligned} d_{Attacker} &= |c_2 x_{Attacker} - m_1 x| \\ d_{Barrier} &= |c_2 x_{Barrier} - m_{2\chi}| \\ d_{Chaser} &= |c_3 x_{Chaser} - m_3 x| \\ d_{Driver} &= |c_4 x_{Driver} - m_4 x| \end{aligned} \tag{6}$$

$$\begin{aligned} &\chi_2 = x_{Barrier} - a_2(d_{Barrier}) \;\; \chi_1 = x_{Aiiacker} - a_1(d_{Aiiacker}) \\ &x_4 = x_{Driver} - a_4(d_{Driver}) \; x_3 = x_{Chaser} - a_3(d_{Chaser}) \end{aligned} \tag{7}$$

$$\begin{aligned} x(t+1) &= \frac{x_1 + x_2 + x_3 + x_4}{4} \\ x_1 &= x_{Attacker} - a_1(d_{Attacker}) \\ x_2 &= x_{Barrier} - a_2(d_{Barrier}) \\ x_3 &= x_{Chaser} - a_3(d_{Chaser}) \\ x_4 &= x_{Driver} - a_4(d_{Driver}) \end{aligned} \tag{8}$$

In ECOA, the extremely disruptive polynomial mutation is increased version of polynomial mutation technique [16]. It could resolve the limitation that polynomial mutation technique is fall as to local optimal once the variable is nearby boundary. In Eqs. (9)–(12) illustrate the procedure of HDPM modifies the x_i

$$\delta_1 = \frac{\chi_i - lb}{ub - lb} \tag{9}$$

$$\delta_2 = \frac{ub - x_i}{ub - lb} \tag{10}$$

$$\delta_k = \begin{cases} [(2r) + (1-2r) * (1-\delta_1)^{\eta m+1}]^{\frac{1}{\eta_m + 1}^{-1}}, r \le 0.5 \\ 1 - [2(1-r) + 2(r-0.5) * (1-\delta_2)^{\eta m+1}]^{\frac{1}{\eta_m + 1}}, \; otherwise \end{cases} \tag{11}$$

$$x_i = x_i + \delta_k(ub - lb) \tag{12}$$

where *ub* and *lb* define the upper and lower boundaries of the search spaces. *r* signifies the arbitrary number amongst zero and one. η_m refers the distribution exponential that is a non-negative number. Since it is clear that the previous formula, HDPM is exploring the total search space.

In contrast to the classical ECOA, in which the update of solutions takes place in the search area in the direction of continuous value location. However, in the BECOA, the searching area can be defined by *n* dimension Boolean lattice. In addition, the solutions get updated using the corner of a hypercube. Moreover, for selecting the features, 1 represents the selection of features, otherwise 0. In addition, the BECOA derived a fitness function in determining the solutions for maintaining a tradeoff between a pair of objectives, as given in Eq. (13):

$$fitness \ = \alpha \Delta_R(D) + \beta \frac{|Y|}{|T|} \tag{13}$$

$\Delta_R(D)$ denotes the error of the classifier, $|Y|$ represents the subset size, and $|T|$ indicates the total number of features that exist in the dataset. Besides, α signifies a variable $\in [0,\ 1]$ related to the weight of the classification error level, and $\beta = 1 - \alpha$ symbolizes the significance of reduction feature.

2.2 Optimal DNN Based Intrusion Detection and Classification

At this stage, the chosen features are passed into the DNN model for intrusion classification. The DNN is an ANN that consists of input, hidden, and output layers. The hidden layer applies a group of non-linear functions and it can be demonstrated as follows [17]:

$$Z = sig(W * x + bias) \tag{14}$$

where *x* refers the input of all nodes, *W* and bias signifies the weight as well as bias vectors correspondingly and *sig* implies the sigmoid activation functions, for instance, $\frac{1}{1+e^{-x}}$. During the presented optimizing DNN, 2 hidden layers are assumed and for minimizing the MAE of DNN, optimum selective of weight matrices are required in order, at this point SAR has been employed. The searching and rescuing function has important 2 stages, for instance, social as well as individual phases. In the searching procedure, the set members collect the clues. The clues left under the search by group members were saved from the memory matrix (O) but the human place is saved from the place matrix (W). The clue matrix *B* with size N^*D that has of left clues and the human places are expressed as:

$$B = \begin{bmatrix} W \\ O \end{bmatrix} = \begin{bmatrix} W_{11} & \cdots & W_{1D} \\ \vdots & \ddots & \vdots \\ W_{N1} & \cdots & W_{ND} \\ O_{11} & \cdots & O_{1D} \\ \vdots & \ddots & \vdots \\ O_{N1} & \cdots & O_{ND} \end{bmatrix} \tag{15}$$

The 2 steps of human search are demonstrated as follows. i) Social step: The search way has provided by $SD_i = (W_i - B_k)$ where $k \neq i$. A novel solution has been created utilizing the formula.

$$W_{ij}^{'} = \begin{cases} \begin{cases} B_{ij} + r_1(W_{ij} - B_{ij}),\ if\ f(B_i) > f(W_i) \\ W_{ij} + r_1(W_{ij} - B_{ij}),\ otherwise \end{cases} & if\ r_2 > SE \\ W_{ij},\ otherwise \end{cases} \tag{16}$$

At this point $f(B_i)$ & $f(W_i)$ denotes the FF values to B_i & W_i, r_1 and r_2 indicates the arbitrary numbers from the range [−1, 1] and [0, 1], the SE is technique parameter range amongst zero and one.

ii) Individual step: According to the present place humans identify its novel place and novel place of i^{th} human is provided as [18]:

$$W_i^{'} = W_i + r_3(B_k - B_m), i \neq k \neq m \tag{17}$$

Every solution is placed from the solution spaces, once the novel place is outer the solution space then it can be enhanced utilizing the formula

$$W_{ij}^{\wedge} = \begin{cases} \dfrac{w_{i,j} + w_j^{\max}}{2} & if\ w_{ij}^{\wedge} > w_j^{\max} \\ \dfrac{w_{i,j} + w_j^{\min}}{2} & if\ w_{ij}^{\wedge} < w_j^{\min} \end{cases} \tag{18}$$

where $W_j^{\max}$ and W_j^{min} implies the maximal as well as minimal threshold. The performance of determining the global optimum solution has improved by providing memory upgrade formulas

$$ME_n = \begin{cases} w_i & if\ f(W_i^{'}) > f(W_i) \\ ME_n & otherwise \end{cases} \tag{19}$$

$$W_i = \begin{cases} W_i^{'} & if\ f(W_i^{'}) > f(W_i) \\ W_i & otherwise \end{cases} \tag{20}$$

where ME_n is n_{rh} has saved clue place from the memory matrix and n refers the arbitrary integer number ranging amongst [1, N]. During the clue search procedure, once optimum clues are not initiated nearby the present place a specific amount of searches, human goes to novel place. For modeling, this, primary, the USN is fixed 0 to all humans.

$$USN_i = \begin{cases} USN_i + 1 & if\ f(W_i^{'}) > f(W_i) \\ 0 & otherwise \end{cases} \tag{21}$$

Once the USN value is superior to the maximal unsuccessful searching number, the human becomes an arbitrary place from the searching space utilized in Eq. (21), and the value of USN_i is fixed 0 to that human.

$$w_{ij} = w_j^{\min} + r_4(w_j^{\max} - w_j^{\min}); i = 1, \ldots..D \tag{22}$$

where r_4 ranges from the interval *zero* and one.

2.3 Process Involved in BEICS

The BC [19] is a major component of the integrity verification system. The primary concept is to offer a solution in which that every flow produced from the controller is saved in a verifiable and immutable dataset. The BC includes a series of blocks interconnected to one another via hash values. At the BC network, the users contain a pair of keys namely private key for signing the BC transaction and public key for representing the irreplaceable address. The client signed a transaction by the use of private key and transmit it to the other ones in the network for verification. Once the broadcasting block gets verified, it is added to the BC. If it is saved, the data in the provided blocks could not be modified with no changes of all succeeding blocks. Besides, the data is present in many hosts concurrently, therefore, the modifications can be discarded by the peer hosts. Here, a private BC has been presented in contrast to a public BC. The private BC decides who can get participated in the network and represented actions as well as permissions allotted identifiable applicants. Therefore, it limits the need for consensus mechanisms like Proof of Work. Fig. 2 shows the structure of BC.

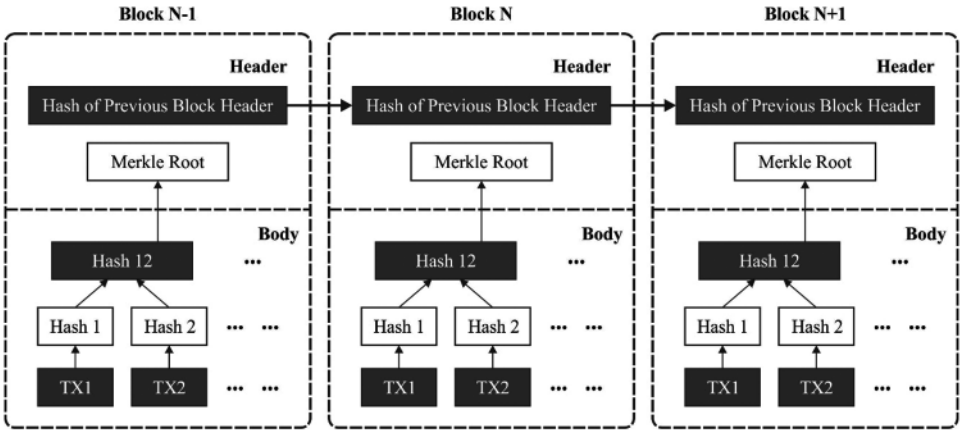

Figure 2: Structure of BC

3 Experimental Validation

In this section, the performance validation of the BDLE-CDE technique takes place using benchmark dataset [20], which comprises 1000's different classes of events. The dataset contains binary (Natural and Attack) and multiclass (No event, Natural, and Attack) labels. Tab. 1 provides a detailed result analysis of the BDLE-CDE technique on the binary class dataset.

Table 1: Results analysis of proposed BDLE-CAD model on binary class dataset

Binary dataset	Precision	Recall	Specificity	Accuracy	F-Score
Subdata-1	96.89	97.47	99.02	98.88	97.10
Subdata-2	97.02	97.95	99.35	98.39	97.05
Subdata-3	98.23	96.98	98.90	98.62	97.94
Subdata-4	96.56	97.83	99.12	98.45	97.97
Subdata-5	96.91	96.67	98.95	98.75	96.77
Subdata-6	96.53	97.76	99.17	98.49	97.06
Subdata-7	97.45	96.70	99.27	98.30	96.52
Subdata-8	97.01	97.71	99.30	98.39	97.42
Subdata-9	97.34	97.17	99.34	98.72	97.87
Subdata-10	97.80	97.97	99.37	98.49	97.23
Subdata-11	97.37	97.00	99.05	98.93	97.48
Subdata-12	98.27	97.98	98.99	98.74	97.57
Subdata-13	97.58	97.72	99.23	98.93	97.01
Subdata-14	98.37	96.76	99.36	98.91	97.89
Subdata-15	97.76	97.04	99.28	98.51	96.90
Average values	97.41	97.38	99.18	98.63	97.32

Fig. 3 offers a brief $prec_n$ and $reca_l$ analysis of the BDLE-CDE technique under distinct subdata on binary class dataset. The figure revealed that the BDLE-CDE technique has attained increased values of $prec_n$ and $reca_l$. For instance, with subdata-1, the BDLE-CDE technique has offered $prec_n$ and $reca_l$ of 96.89% and 97.47% respectively. Meanwhile, with subdata-10, the BDLE-CDE technique has provided $prec_n$ and $reca_l$ of 97.80% and 97.97% respectively. Eventually, with subdata-15, the BDLE-CDE technique has demonstrated $prec_n$ and $reca_l$ of 97.76% and 97.04% respectively.

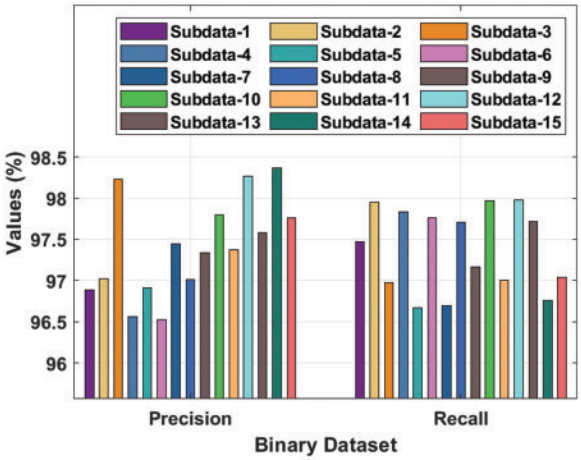

Figure 3: Pre_n and Rec_l analysis of BDLE-CDE technique on binary dataset

Fig. 4 exhibits a detailed $spec_y$ and F_{score} analysis of the BDLE-CDE technique under distinct subdata on binary class dataset. The figure shows that the BDLE-CDE technique has accomplished superior values of $spec_y$ and F_{score}. For instance, with subdata-1, the BDLE-CDE technique has demonstrated $spec_y$ and F_{score} of 99.02% and 97.10% respectively. Moreover, with subdata-10, the BDLE-CDE technique has gained $spec_y$ and F_{score} of 99.37% and 97.23% respectively. Furthermore, with subdata-15, the BDLE-CDE technique has reached $spec_y$ and F_{score} of 99.28% and 96.90% respectively.

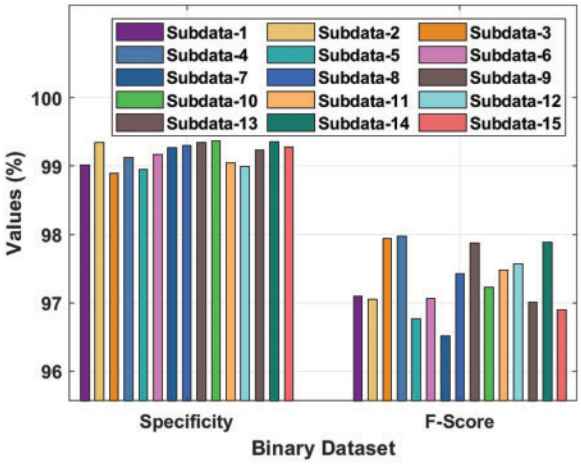

Figure 4: $Spec_y$ and F_{score} analysis of BDLE-CDE technique on binary dataset

Fig. 5 portrays the $accu_y$ analysis of the BDLE-CDE technique on the test binary dataset. The results show that the BDLE-CDE technique has gained a lower $accu_y$ of 98.30% on subdata-7 and higher $accu_y$ of 98.91% on subdata-14. Therefore, it is ensured that the BDLE-CDE technique has effectually classified binary classes.

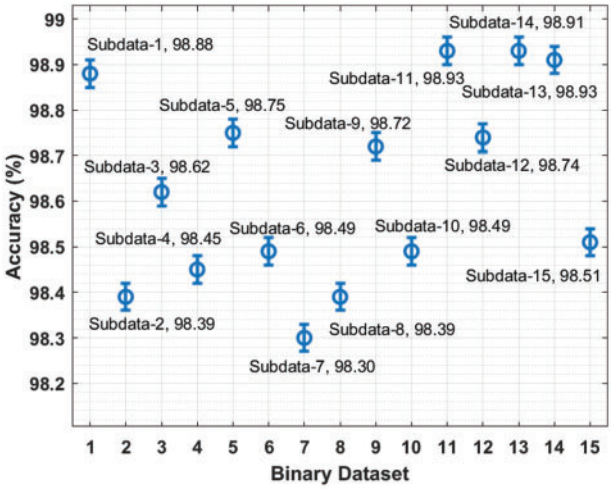

Figure 5: *Accu*$_y$ analysis of BDLE-CDE technique on binary dataset

Tab. 2 offers a comprehensive comparison study of the BDLE-CDE technique on the multi class dataset.

Table 2: Results analysis of proposed BDLE-CAD model on multiclass dataset

Multiclass dataset	Precision	Recall	Specificity	Accuracy	F-Score
Subdata-1	79.00	92.09	93.46	93.08	80.55
Subdata-2	82.98	91.57	92.93	93.79	80.39
Subdata-3	81.62	89.72	93.56	92.41	82.51
Subdata-4	81.80	89.97	93.59	93.98	82.46
Subdata-5	79.47	89.53	93.13	91.50	81.49
Subdata-6	83.20	92.29	93.46	91.23	79.74
Subdata-7	80.69	92.85	92.78	92.22	83.19
Subdata-8	83.50	90.56	93.96	93.24	80.08
Subdata-9	80.11	91.45	93.87	92.38	80.67
Subdata-10	83.37	92.39	93.79	93.05	79.83
Subdata-11	78.88	91.34	93.28	93.16	82.26
Subdata-12	82.56	89.28	93.04	92.53	82.75
Subdata-13	83.49	89.57	93.59	93.59	80.15
Subdata-14	83.37	89.56	93.40	91.01	79.79
Subdata-15	78.62	89.25	93.75	92.21	82.46
Average values	81.51	90.76	93.44	92.63	81.22

Fig. 6 showcases a brief $prec_n$ and $reca_l$ analysis of the BDLE-CDE technique under distinct subdata on multi class datasets. The figure discovered that the BDLE-CDE technique has attained increased values of $prec_n$ and $reca_l$. For instance, with subdata-1, the BDLE-CDE technique has presented $prec_n$ and $reca_l$ of 79% and 92.09% respectively. Meanwhile, with subdata-10, the BDLE-CDE technique has delivered $prec_n$ and $reca_l$ of 83.37% and 92.39% respectively. Finally, with subdata-15, the BDLE-CDE technique has demonstrated $prec_n$ and $reca_l$ of 78.62% and 89.25% respectively.

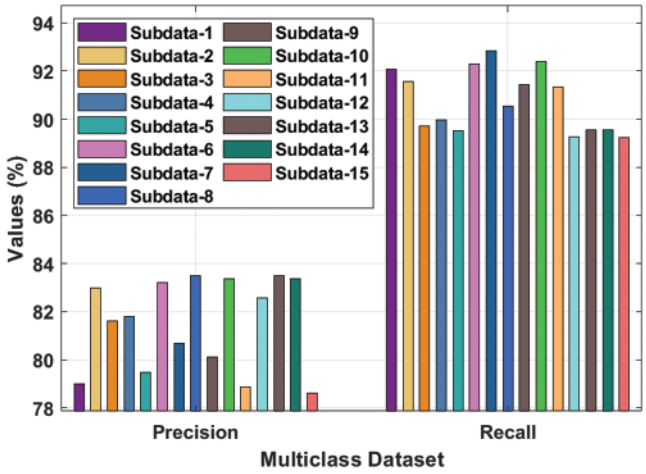

Figure 6: Pre_n and Rec_l analysis of BDLE-CDE technique on multiclass dataset

Fig. 7 reveals a detailed $spec_y$ and F_{score} analysis of the BDLE-CDE technique under distinct subdata on multi class datasets. The figure displayed that the BDLE-CDE technique has resulted in maximum values of $spec_y$ and F_{score}. For instance, with subdata-1, the BDLE-CDE technique has demonstrated $spec_y$ and F_{score} of 93.46% and 80.55% respectively. Moreover, with subdata-10, the BDLE-CDE technique has gained $spec_y$ and F_{score} of 93.87% and 80.67% respectively. Furthermore, with subdata-15, the BDLE-CDE technique has reached $spec_y$ and F_{score} of 93.75% and 82.46% respectively.

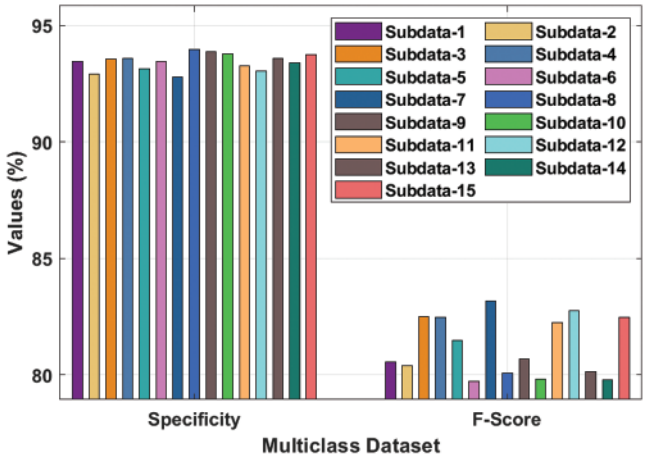

Figure 7: $Spec_y$ and F_{score} analysis of BDLE-CDE technique on multiclass dataset

Fig. 8 shows the $accu_y$ analysis of the BDLE-CDE technique on the test binary dataset. The figure reported that the BDLE-CDE technique has gained a lower $accu_y$ of 91.01% on subdata-14 and higher $accu_y$ of 93.98% on subdata-4. Therefore, it is ensured that the BDLE-CDE technique has effectually classified multiple classes.

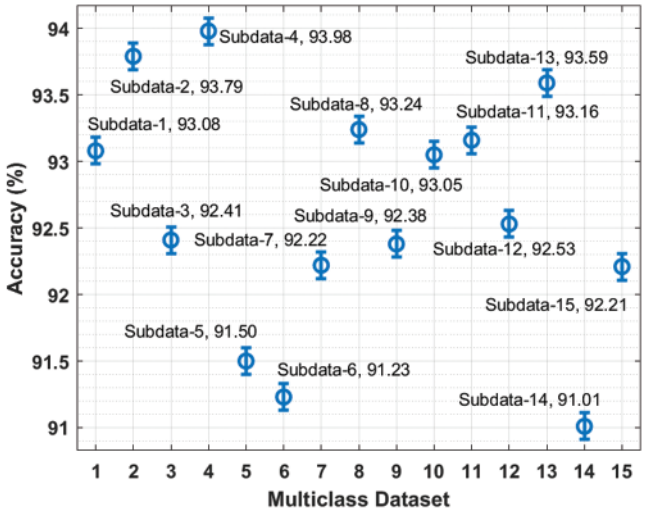

Figure 8: $Accu_y$ BDLE-CDE technique on binary dataset

Tab. 3 offers a detailed comparative study of the BDLE-CDE technique with recent methods [21]. A comparative classification result analysis of the BDLE-CDE technique on the binary class dataset is depicted in Fig. 9. The results exposed that the Nearest Neighbor (NN), random forest (RF), and SVM models have obtained lower $accu_y$ of 71.56%, 80.61%, and 78.84% respectively. At the same time, the KNN, Adaboost+JRip, and JRip models have obtained moderate $accu_y$ values of 95.49%, 95.56%, and 90.10%. However, the BDLE-CDE technique has resulted in increased $accu_y$ of 98.63%.

Table 3: Comparative accuracy analysis of BDLE-CAD model on binary and multiclass dataset

Methods	Binary class	Multi class
BDLE-CAD	98.63	92.63
KNN	95.49	87.66
Nearest neighbor	71.56	77.33
Random forest	80.61	80.51
SVM	78.84	78.56
JRip	90.10	90.09
Adaboost+JRip	95.56	91.44

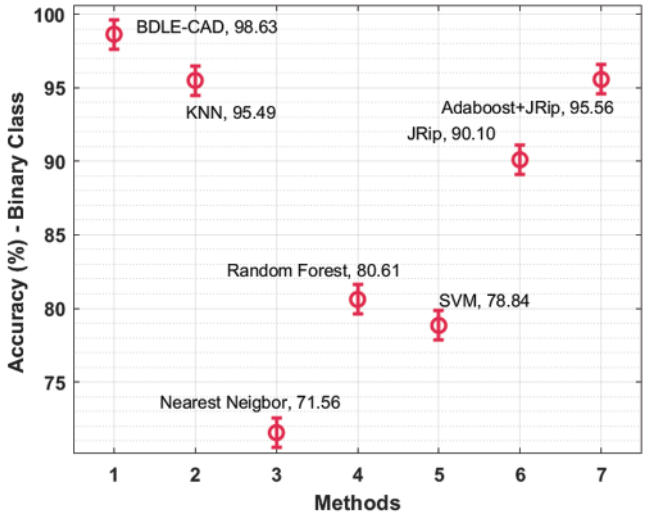

Figure 9: Comparative $Accu_y$ analysis of BDLE-CDE technique on binary dataset

Detailed multiclass performance analysis of the BDLE-CDE technique on the multi class dataset is offered in Fig. 10. The experimental values illustrated that the Nearest Neighbor (NN), random forest (RF), and SVM models have gained reduced $accu_y$ of 77.33%, 80.51%, and 78.56% respectively. Moreover, the KNN, Adaboost+JRip, and JRip models have obtained moderate $accu_y$ values of 87.66%, 91.44%, and 90.09%. However, the BDLE-CDE technique has accomplished superior $accu_y$ of 92.63%. From these results and discussion, it can be ensured that the BDLE-CDE technique has the ability to attain maximum performance over the other compared methods.

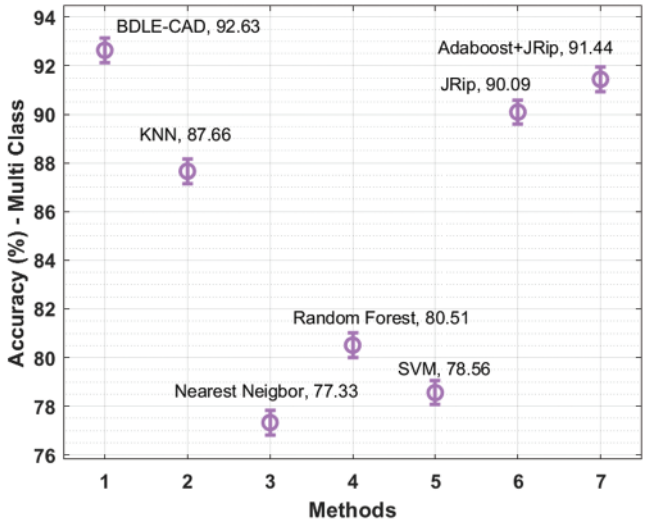

Figure 10: Comparative $Accu_y$ analysis of BDLE-CDE technique on multiclass dataset

4 Conclusion

In this study, a new BDLE-CAD technique has been developed to identify the existence of intrusions in critical infrastructures. The proposed BDLE-CAD technique encompasses ECOA-FS technique for the selection of optimal subset of features. Moreover, the DNN with SAR optimizer is can be used as a classifier and the BEICS has been presented to defend over the misrouting attacks. The experimental result analysis of the BDLE-CAD technique takes place and the results are inspected under varying aspects. The simulation analysis pointed out the supremacy of the BDLE-CAD technique over the recent state of art techniques with the accomplished superior $accu_y$ of 92.63%. Therefore, the BDLE-CAD technique can be utilized as a proficient tool to detect intrusions in the network. In future, clustering and outlier detection approaches can be designed to boost the detection performance.

Acknowledgement: The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the Project Number (IFPIP-145-351-1442) and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

Funding Statement: This project was supported financially by Institution Fund projects under Grant No. (IFPIP-145-351-1442).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Otoum, I. A. Ridhawi and H. Mouftah, "Securing critical IoT infrastructures with blockchain-supported federated learning," *IEEE Internet Things Journal*, pp. 1–1, 2021, https://doi.org/10.1109/JIOT.2021.3088056.

[2] Y. Qi, L. Tian, Y. Zhou and J. Yuan, "Mobile edge computing-assisted admission control in vehicular networks: The convergence of communication and computation," *IEEE Vehicular Technology Magazine*, vol. 14, no. 1, pp. 37–44, 2019.

[3] D. Feng, C. She, K. Ying, L. Lai, Z. Hou *et al.,* "Toward ultrareliable low-latency communications: Typical scenarios, possible solutions, and open issues," *IEEE Vehicular Technology Magazine*, vol. 14, no. 2, pp. 94–102, 2019.

[4] I. A. Ridhawi, S. Otoum, M. Aloqaily, Y. Jararweh and T. Baker, "Providing secure and reliable communication for next generation networks in smart cities," *Sustainable Cities and Society*, vol. 56, pp. 102080, 2020.

[5] Y. Wu, H. Dai and H. Wang, "Convergence of blockchain and edge computing for secure and scalable iiot critical infrastructures in industry 4.0," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2300–2317, 2021.

[6] K. Yu, L. Tan, X. Shang, J. Huang, G. Srivastava *et al.,* "Efficient and privacy-preserving medical research support platform against covid-19: A blockchain-based approach," *IEEE Consumer Electronics Magazine*, vol. 10, no. 2, pp. 111–120, 2021.

[7] M. Chen, Y. Jiang, N. Guizani, J. Zhou, G. Tao *et al.,* "Living with I-fabric: Smart living powered by intelligent fabric and deep analytics," *IEEE Network*, vol. 34, no. 5, pp. 156–163, 2020.

[8] K. Yu, L. Tan, M. Aloqaily, H. Yang and Y. Jararweh, "Blockchain-enhanced data sharing with traceable and direct revocation in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7669–7678, 2021.

[9] J. M. Mcginthy and A. J. Michaels, "Secure industrial internet of things critical infrastructure node design," *IEEE Internet Things Journal*, vol. 6, no. 5, pp. 8021–8037, 2019.

[10] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.
[11] A. Gumaei, M. A. Rakhami, M. M. Hassan, P. Pace, G. Alai *et al.,* "Deep learning and blockchain with edge computing for 5g-enabled drone identification and flight mode detection," *IEEE Network*, vol. 35, no. 1, pp. 94–100, 2021.
[12] O. Alkadi, N. Moustafa, B. Turnbull and K. K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks," *IEEE Internet Things Journal*, vol. 8, no. 12, pp. 9463–9472, 2021.
[13] S. K. Singh, Y. S. Jeong and J. H. Park, "A deep learning-based IoT-oriented infrastructure for secure smart City," *Sustainable Cities and Society*, vol. 60, pp. 102252, 2020.
[14] K. Zhang, Y. Zhu, S. Maharjan and Y. Zhang, "Edge intelligence and blockchain empowered 5g beyond for the industrial internet of things," *IEEE Network*, vol. 33, no. 5, pp. 12–19, 2019.
[15] M. Khishe, M. Nezhadshahbodaghi, M. R. Mosavi and D. Martin, "A weighted chimp optimization algorithm," *IEEE Access*, pp. 1–1, 2021, http://dx.doi.org/10.1109/ACCESS.2021.3130933.
[16] D. Wu, W. Zhang, H. Jia and X. Leng, "Simultaneous feature selection and support vector machine optimization using an enhanced chimp optimization algorithm," *Algorithms*, vol. 14, no. 10, pp. 282, 2021.
[17] C. Muppala and V. Guruviah, "Detection of leaf folder and yellow stemborer moths in the paddy field using deep neural network with search and rescue optimization," *Information Processing in Agriculture*, vol. 8, no. 2, pp. 350–358, 2021.
[18] A. Shabani, B. Asgarian, S. A. Gharebaghi, M. A. Salido and A. Giret, "A new optimization algorithm based on search and rescue operations," *Mathematical Problems in Engineering*, vol. 2019, pp. 1–23, 2019.
[19] A. Derhab, M. Guerroumi, A. Gumaei, L. Maglaras, M. A. Ferrag *et al.,* "Blockchain and random subspace learning-based ids for sdn-enabled industrial IoT security," *Sensors*, vol. 19, no. 14, pp. 3119, 2019.
[20] S. Abe, Y. Uchida, M. Hori, Y. Hiraoka and S. Horata, "Cyber threat information sharing system for industrial control system (ICS)," in *2018 57th Annual Conf. of the Society of Instrument and Control Engineers of Japan (SICE)*, Nara, pp. 374–379, 2018.
[21] R. C. B. Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari *et al.,* "Machine learning for power system disturbance and cyber-attack discrimination," in *2014 7th Int. Symp. on Resilient Control Systems (ISRCS)*, Denver, CO, USA, pp. 1–8, 2014.