Journal of Computer Science

Research Article

Blockchain-Enabled Decisive Red Fox Optimizer-Based Feature Selection With Deep Learning-Based Intrusion Detection System

C. Ananth[1], S. Sathiyarani[1] and N. Mohananthini[2]

[1]*Department of Computer and Information Science, Annamalai University, Annamalainagar, 608002, India*
[2]*Department of Electrical and Electronics Engineering, Muthayammal Engineering College, Rasipuram, 637408, India*

Article history
Received: 19-03-2025
Revised: 18-07-2025
Accepted: 25-07-2025

Corresponding Author:
S. Sathiyarani
Department of Computer and Information Science, Annamalai University, Annamalainagar, 608002, India
Email: sathiyaranis86@gmail.com

Abstract: Recently, Intrusion Detection Systems (IDS) using Deep Learning (DL) models become useful in accomplishing network security. The selected features serve as input to the DL model, which is trained on labelled datasets to learn intrinsic patterns distinguishing malicious from normal network behaviour. DL techniques like Convolutional Neural Networks (CNN) are usually utilized. The seamless combination of Public Blockchain (BC) technology into the IDS working procedure safeguards a tamper-resistant and safe record of intrusion detection results, improving reliability and transparency in cybersecurity processes. BC is combined into the IDS to improve safety and data integrity. Every legalized intrusion event or classification result is recorded in a decentralized and immutable ledger. BC ensures the reliability of the recognition outcomes, averts tampering, and presents a clear and safe record of network actions. This study introduces a BC-enabled decisive red fox optimizer-based feature selection using the DL (BDRFFS-DL) technique to identify intrusions effectively. The BDRFFS-DL technique exploits the Feature Selection (FS) approach to pick a relevant subset of features, thereby improving classification accuracy and decreasing the computation complexity. Initially, Z-score standardization is used for normalizing the input traffic data into a consistent format. The BDRFFS-DL approach utilizes the DRF optimizer to select the finest feature subset to improve the classification performance and resolve the high dimensionality issue. Furthermore, the intrusion detection process is carried out by using the Convolutional Sparse Autoencoder (CSAE) model. Moreover, BC ensures the integrity of detection results and provides a secure record of network actions. An extensive study of the BDRFFS-DL approach using the ToN_IoT dataset illustrated its superior performance, achieving an accuracy of 98.91%, outperforming existing models.

Keywords: Blockchain, Security, Intrusion Detection System, Feature Selection, Deep Learning, Decisive Red Fox Optimizer

Introduction

An IDS is applied to identify network or computer anomalies (Shobana *et al*., 2022). IDSs are considered in numerous methods, among them the most popular techniques such as anomaly- and misuse-assisted IDS. Misuse-based IDS is implemented proficiently to recognize known outbreaks such as snort (Oseni *et al*., 2022). This type of IDS has decreased the false alarm rate (FAR). It cannot identify new attacks that do not distinguish some information in a dataset. An anomaly-based IDS builds a model of consistent behaviour. Then, it splits all crucial abnormalities from this system and considers that abnormality an intrusion (Bahri *et al*., 2023). This kind of IDS can identify unknown and known outbreaks; however, it meets a higher FAR. Numerous Machine Learning (ML) models are employed to reduce FAR. ML is employed to develop an automatic analytical system. This is a method of data analysis (Kumaran and Mohan, 2023). It is one of the subdivisions of Artificial Intelligence (AI) that performs under the notion that a system obtains training, takes decisions, and learns to

recognize the patterns with some involvements of humans (Ferrag *et al*., 2021).

The development of cyberattacks requires new security actions (Saveetha and Maragatham 2022). This research discovers the combination of two cutting-edge technologies, BC and optimum DL, to make an effective defence against intrusions. BC's immutable and decentralized ledger safeguards the reliability and liability of data (Liu *et al*., 2022). Utilizing a distributed ledger increases the security of sensitive data, avoiding unauthorized modifications and safeguarding a tamper-resistant record of actions. DL, fine-tuned through optimization techniques, provides exceptional precision to IDSs. Its capability to distinguish intricate patterns and anomalies in network traffic improves the active recognition of possible attacks (Vaiyapuri *et al*., 2024). The incorporation of BC and DL makes a synergistic security network. BC protects data integrity, and DL-driven IDS secures the network against complex intrusions. BC's decentralized feature ensures that security actions must be allocated (Mbaya *et al*., 2023). Integrating BC with the DL will provide various possible advantages in improving the security of network systems. BC presents an immutable and decentralized ledger that could store logs and records connected to network actions and safety measures (Monirah and Ykhlef, 2023). By maintaining intrusion detection and prevention data under a BC, the data is tamper-proof and apparent, safeguarding the integrity of the records.

This study introduces a BC-enabled decisive red fox optimizer-based FS using the DL (BDRFFS-DL) technique to identify intrusions effectively. Initially, Z-score standardization is used for normalizing the input traffic data into a consistent format. The DRF optimizer is employed to select the finest feature subset to improve the classification performance and resolve the high dimensionality issue. Furthermore, the intrusion detection process is carried out by using the Convolutional Sparse Autoencoder (CSAE) model. Moreover, BC ensures the integrity of the detection result and provides a secure record of network actions. The ToN_IoT dataset is used for extensive analysis. The key contribution is listed below:

- Z-score standardization is used to normalize the input traffic data into a uniform scale, which improves consistency across features. This step supports better learning by the model and improves classification accuracy. It plays a major role in data preparation for intrusion detection
- The DRF optimizer addresses the high dimensionality issue by choosing the most informative features from the input data. This significantly improves detection performance while minimizing computational overhead. Concentrating on significant features only strengthens the overall system efficiency
- The CSAE model is implemented to perform intrusion detection by capturing deep spatial features and enforcing sparsity. This enhances the technique's capability to distinguish between normal and malicious traffic. It adds robustness to the detection framework through precise and efficient threat detection
- BC is integrated to preserve the integrity of detection results and securely log all network activities in an immutable manner. This ensures transparency and prevents tampering, strengthening the reliability and accountability of the overall IDS

Literature Review

Alamro *et al*. (2023) introduced a BC-enabled IoT healthcare system employing an ant lion optimizer with a hybrid DL (BHS-ALOHDL) technique. This Neural Network (NN) method executes an ALO-FSS model for generating a sequence of feature vectors. This HDL method combines the LSTM model and CNN features for IDS. In conclusion, the Flower Pollination Approach (FPA) was utilized for optimization. Alkadi *et al*. (2021) developed a Deep BC architecture method. The IDS handled consecutive networking data using a BiLSTM-based DL method. Ethereum is also utilized. (Mansour 2022) proposed an innovative poor and rich optimizer with the DL and BC-based IDS in CPS, named the PRO-DLBIDCPS method. Narayanan and Paul (2023) introduced an innovative model named BC-based federated learning for IDS (BlockFL-IDS). This model utilizes Auction game theory and employs the Base Criterion Method (BCM) technique to protect the channel selection. In Abdel-Basset *et al*. (2022), a FED-IDS technique was developed. A context-aware modifier model is also utilized.

He *et al*. (2022) implemented a conditional GAN (CGAN)-assisted combined IDS with BC-assisted dispersed FL. Poorazad *et al*. (2023) developed an incorporated technique comprising two modules: a CNN-based IDS executed as an SDN utilization and a BC-based model allowing network and application layers protection correspondingly. An essential benefit of the developed technique exists in mutually decreasing the effect of attacks like rule and command injection under SDN-assisted IIoT architectural layers. Alamro *et al*. (2025) proposed the mathematical modelling-based BC with mountain gazelle optimizer and attention to DL for cybersecurity (MGOADL-CS) model to improve drone cybersecurity by integrating BC technology with an Attention Long Short-Term Memory NN (ALSTM-NN) optimized via MGO for accurate detection and classification of cyberattacks in real-time. Perumal *et al*. (2024) proposed an Enhanced Metaheuristics with a DL Method for BC-based Cybersecurity Solution (EMDLM-BCCS) methodology by integrating BC technology with

Extreme Learning Machine (ELM) optimized by elite-oppositional grasshopper optimizer approach (EGOA) model for effective DDoS attack detection.

Al Mazroa *et al*. (2025) presented an Automated Cyberattack Detection Utilizing Binary Metaheuristics with DL (ACAD-BMDL) model using Binary Grey Wolf Optimization (BGWO) combined with the enhanced Elman Spike NN (EESNN) and Archimedes Optimizer Approach (AOA) for accurate and efficient threat identification. Dontu *et al*. (2024) presented a decisive red fox with a CNN (DRF-CNN) model to enhance cyberattack detection using DL-based FS and classification for accurate and efficient intrusion detection. Abdullah *et al*. (2025) proposed an ensemble learning model using extreme gradient boosting (XGBoost) to improve detection by accurately classifying network traffic and enhancing healthcare cybersecurity. (Salami *et al*., 2024) introduced hybrid method by utilizing Harris Hawks Optimization (HHO) in detecting attacks within IoT networks by selecting optimal features for classification. Alqahtany *et al*. (2025) proposed an enhanced grey wolf optimizer-based FS (EGWO-FS) model to improve IDS in Internet of Things (IoT) networks by selecting optimal features and using RF for accurate and efficient attack detection. Alabdali and Mashat (2024) proposed BC and federated learning-based deep belief network (BC-FL-DBN) model by integrating LSTM, BC, and Alloy Language for secure and privacy-preserving predictive modelling in social media.

While existing models such as BHS-ALOHDL, PRO-DLBIDCPS, BlockFL-IDS, and FED-IDS have shown robust intrusion detection capabilities, many rely on single-layer optimization or lack real-time adaptability in resource-constrained environments. Various methods like CGAN-integrated IDS and EMDLM-BCCS improve data diversity and attack detection but face difficulty with scalability and latency in distributed networks. Though BC integration strengthens data integrity, models like ACAD-BMDL and EGWO-FS often overlook adaptive trust mechanisms. Ensemble and hybrid FS methods such as DRF-CNN and HHO-based IDS improve detection but may incur high computational costs. The research gap is developing lightweight, adaptive, and real-time IDS frameworks that integrate BC, DL, and metaheuristics without compromising speed, accuracy, or resource efficiency across diverse domains like IoT, CPS, and IoMT.

Methodology

This research introduces an innovative BDRFFS-DL model to identify intrusions effectively. The BDRFFS-DL technique exploits the FS approach to choose relevant feature subset, thereby improving the accuracy and reducing the computational complexity. Figure 1 depicts the complete flow of the BDRFFS-DL technique. The pseudocode of the BDRFFS-DL technique is showcased in Algorithm 1.

Z-Score Normalization

Initially, the BDRFFS-DL model applies Z-score to compute input traffic in a uniform format. This approach standardizes traffic data to zero mean and unit variance, ensuring balanced feature contribution. This model handles extreme values more robustly by relying on statistical distribution. This technique improves the convergence speed and stability of learning algorithms, specifically those sensitive to feature scales, namely NNs and distance-based classifiers. It also enhances the interpretability of the data, making anomalies more distinguishable during detection. Compared to methods like log or decimal scaling, this model maintains the original distribution shape while mitigating the impact of skewed data. Its adaptability across diverse datasets and consistent performance in high-dimensional spaces make it an ideal option for preprocessing in intrusion detection systems.

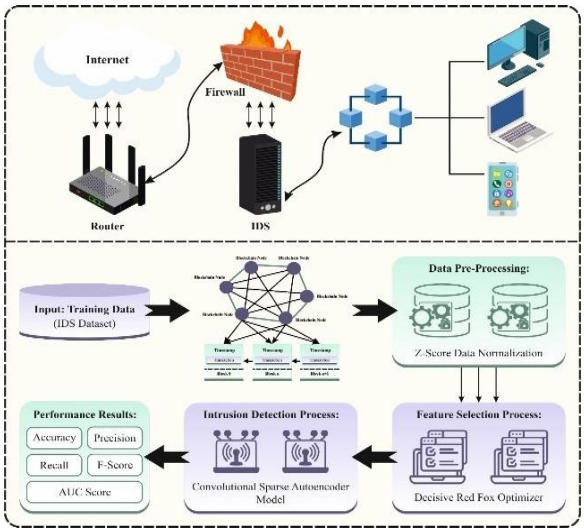

Fig. 1: Overall flow of BDRFFS-DL technique

Algorithm 1: Pseudocode of BDRFFS_DL approach

```
BDRFFS_DL_Intrusion_Detection(input_traffic_data)
:
 Z_score_normalization(input_data):
   # Implement Z-score normalization on the input data
   normalized_traffic =
Z_score_normalization(input_traffic_data)
   # Return the normalized data
DRF_Optimizer(data):
   # Perform the DRF optimizer for FS
   # Choose a feature subset using the optimizer
   selected_features =
DRF_Optimizer(normalized_traffic)
# Return the selected features
CSAE_Intrusion_Detection(features):
```

```
    # Execute the CSAE for intrusion detection
    # Apply the features selected for the detection method
    intrusion_results = CSAE_Intrusion_Detection(selected_features)
    # Return the intrusion detection outcomes
BC_integration(results):
    # Incorporate BC for result integrity
    # Create a secure record of network actions
    # Ensure the security and integrity of the intrusion detection outcomes
```

Z-score normalization plays a vital part in normalizing the input features of the method, safeguarding a reliable scale through different data sources (Cochran *et al*., 2021). By altering the raw data into Z-scores, which signify the number of Standard Deviations (SD) a data point is from the mean, the IDS attains an even distribution of values. This normalization procedure is vital for upholding the reliability of anomaly recognition systems, as it permits the system to separate unusual designs or deviations from the model. The use of BC technology further strengthens the safety of the IDS by certifying a tamper-resistant and clear record of the regularized data, improving the reliability of the IDS mechanism.

BC Integration

Finally, BC is applied to ensure the detection result's integrity and provide a secure record of network actions. Decentralization is the foremost inspiration behind the BC model (Liang *et al*., 2020). The transparent and distributed features of the BC archive mean that the one-node flop will not concern the entire system. BC reformed the structure of the transaction system from a lead to a Point-to-Point (P2P) layout. This altered structure permits dual parties to contract with one another directly with security and encryption depending upon code and system safety. The nodes in the transaction network depend on itself for establishing trust, thus eliminating the need to evaluate third-party validating in this setting. Hyperledger fabric and Ethereum, which share similar core technologies, are the two major platforms for BC. The significant dissimilarity among these platforms lies in the method they are intended for and in the objective users. Smart deals and community BCs are directed at uses that common users utilize. Hyperledger Fabric has a very flexible design that is highly suitable for corporate use. The main intention is to shorten effort and trade procedures utilizing the technology of BC, which helps resolve the inter-firm credit issue. Figure 2 represents the BC framework.

This method applies a private chain to protect communication among agents. The technique combines the embedded and the BC node datasets in a similar agent, initial and ending at the equivalent period. Storing a dataset copy in entire agents will decrease the communicating agent by executing a local hunt of the recently upgraded data

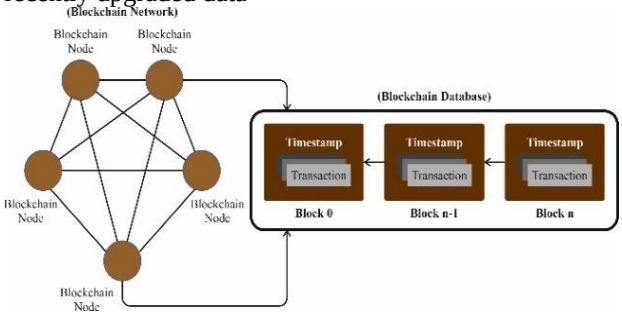

Fig. 2: BC architecture

The recognition and analysis module of the communication agent is a great node for the BC unit. It includes the complete BC ledger and ensures all nodes in the system can obtain and attach the precise copy. Other agents in every module are permitted as light nodes, and the link to an agent is a parent node. The BC unit is utilized to validate and control the behaviours of agents and is also used to construct faith in systems in which several parties are involved. Furthermore, data from messages of communication is utilized for analyzing assaults and enhancing agents by using Reinforcement Learning (RL).

DRF-Based FS

The BDRFFS-DL technique applies the DRF optimizer to select an optimum feature subset. This model effectually handles high-dimensional data by utilizing the merits of decision forests to evaluate feature importance. Unlike conventional methods that may depend on simple statistical measures, DRF considers intrinsic interactions between features, improving the selection of the most relevant subset. This results in an improved performance and reduced overfitting. Compared to other optimizers, DRF presents faster convergence and scalability to massive datasets, thus facilitating real-time detection. Additionally, it balances exploration and exploitation effectively, ensuring a comprehensive search of the feature space. Overall, DRF optimizes accuracy and computational effectiveness, making it an ideal for FS in complex network settings.

After attaining the balanced data from the prior stage, the DRF optimizer method was implemented to choose the optimum feature to increase the accuracy and training speed of IDS (Rabie *et al*., 2024). The classical IDS framework introduces Different metaheuristic optimization techniques to improve network safety. However, the main issues are related to factors such as over-fitting, complicated computation operations, slow processes, and reduced convergence rates. This approach is widely applied in safety applications to resolve complex optimizer problems. The DRF is the recent optimizer

method with several advantages over other techniques. It consists of reduced local optimum, lower computation complexity, avoiding stacking of algorithm under optimizer, and fast convergence. The study uses this algorithm to enhance the data features based on the optimum output. Furthermore, this technique assists in simplifying the classification process with an improved recognition rate.

This technique can tune the parameters of a balanced IoT. In general, foxes are small and medium-sized, omnivorous animals that belong to the Canidae genera. Furthermore, the foxes are distinguished from other members of giant dogs or their families. The hunting habits of RFs motivates this model. During hunting, the RF gets closer to the target, hides in bushes, and then attacks the prey. This method integrates exploration and exploitation abilities similar to other metaheuristics approaches. During this method, the parameter initialization is carried out depending on the group of arbitrary individuals as defined in Eqs. (1-2):

$$P = [p_0, p_1 \dots p_{n-1}] \tag{1}$$

$$(P)^i = \left[(p_0)^i, (p_1)^i \dots (p_{n-1})^i\right] \tag{2}$$

On the other hand, i implies the populations from the searching space. Afterwards, a better performance was obtained from the search space by utilizing the global optimum function. At this point, the Euclidean distance was executed to get a better result by employing the following method:

$$E\left(((P)^i)^k, (P_{best})^k\right) = \sqrt{((P)^i)^k - (P_{best})^k)} \tag{3}$$

In this case, k signifies the iteration counts, P_{best} refers to the best optimal, and E stands for the Euclidean distance. Accordingly, better performance is employed to migrate every candidate, as expressed:

$$\left((P)^i\right)^k = ((P)^i)^k + rsign((P_{best})^k - \left(((p)^i)^k\right) \tag{4}$$

Whereas r implies the random number within an interval of [0-1], which is an arbitrarily elected scaling parameter that is fixed. After moving to the finest location, once the fitness value at their novel locations is developed, individuals remain there or can return to their new places. This demonstrates how the family members arrive home later on an expedition and explain to the others somewhere to search. Once there is a possibility of discovering food, it will stay to search; or else, it would arrive home with empty-hand". In every cycle of DRF, these processes stand in for presented global hunts.

Additionally, the candidates' novel place can present an appropriate choice, or the previous place will still occur. The RF method detects the target using a DRF model, which incorporates a random value ω between 0 and 1:

$$\begin{cases} Move\ forward\ if, \omega > 3/4 \\ Stay\ hidden\ if, \omega > 3/4 \end{cases} \tag{5}$$

$$\omega = \begin{cases} h \times \frac{\sin(\delta_0)}{\delta_0} & if\ \delta_0 \neq 0 \\ \tau & if\ \delta_0 = 0 \end{cases} \tag{6}$$

Where h stands for an arbitrary number in 0 and 0.2, δ_0 refers to the arbitrary number within an interval of $[0,2\pi]$ assumed as the Fox observation viewpoint, and τ implies the arbitrary value from zero to one:

$$\begin{cases} p_0^{new} = h \times \omega \times \cos(\delta_1) + p_0^{actual} \\ p_1^{new} = h \times \omega \times \sin(\delta_1) + h \times \omega \times \cos(\delta_2) + p_1^{actual} \\ p_1^{new} = h \times \omega \times \sin(\delta_1) + h \times \omega \times \sin(\delta_2) + h \times \omega \times \cos(\delta_3) + p_2^{actual} \\ \vdots \\ p_{n-1}^{new} = h \times \omega \times \sum_{t=1}^{n-2} \sin(\delta_1) + h \times \omega \times \cos(\delta_{n-1}) + p_{n-2}^{actual} \\ p_{n-1}^{new} = h \times \omega \times \sin(\delta_1) + h \times \omega \times \sin(\delta_2) + \cdots + h \times \omega \times \sin(\delta_{n-1}) + p_{n-\alpha}^{actual} \end{cases} \tag{7}$$

The population's worst members are removed to continue a stable population size, and several new members are added. Afterwards, the two optimum members are recognized at iteration k, and their centre was evaluated as:

$$C_e^k = \frac{1}{2}\left(P(1)\right)^k - \left(P(2)\right)^k \tag{8}$$

At this point, a parameter φ among (0 and 1) was employed for all the iterations that certain alternates from the iteration according to the following model:

$$\begin{cases} new\ nomadic\ individual\ if, \varphi > 0.45 \\ reproduction\ \ \ if, \varphi \leq 0.45 \end{cases} \tag{9}$$

According to this process, the random places are upgraded from the search space, and the novel members are included by utilizing the subsequent method:

$$(P^{rp})^k = \frac{\varphi}{2}\left(P(1)\right)^k - \left(P(2)\right)^k \tag{10}$$

This function acquires the mimicked individual, and the finest P_{best} is given back as the output. This work was employed to optimally select the features to train the optimizer's data instances.

In the DRF method, the intentions are combined into a solitary intent data such that a present weight identifies every goal prominence (Mafarja *et al*., 2023). This study implements an FF that integrates both objectives of FS, as shown in Eq. (11):

$$Fitness(X) = \alpha \cdot E(X) + \beta * \left(1 - \frac{|R|}{|N|}\right) \tag{11}$$

Here, $E(X)$ is the classifier error rate for the chosen features X, and Fitness(X) is its fitness value. $|R|$ and $|N|$ are the chosen numbers and original features. α\alphaα (in

[0,1] weights classification error, while $\beta = (1 - \alpha)$ weights feature reduction.

Classification using the CSAE model

The intrusion detection process is carried out using the CSAE model for classification. This technique is selected for its ability to automatically learn deep hierarchical features while enforcing sparsity, which assists in capturing the most informative patterns in network traffic data. Compared to conventional classifiers, CSAE outperforms in handling high-dimensional and complex data by extracting robust spatial features without heavy manual feature engineering. Its sparse coding promotes model generalization and reduces overfitting, crucial for accurately detecting varied intrusion types. Unlike standard autoencoders, the convolutional architecture preserves spatial relationships, improving detection sensitivity. Additionally, CSAE is more resilient to noise and anomalies, improving overall classification reliability in dynamic network environments. This combination of deep feature extraction and sparsity makes CSAE a powerful model for intrusion detection tasks. Fig. 3 represents the architecture of CSAE.

A supervised model is a data-driven Feature Learning (FL) approach that updates the weight connection through forward and backward training (Mohana and Subashini, 2023). Compared to the supervised method, unsupervised learning openly obtains an unlabelled input dataset and learns applicable features. This technique considerably decreases the workload for a labelling dataset.

Unsupervised AE (UAE), consisting of an encoder, a hidden (latent) space, and a decoder, efficiently detects intrusions. AEs are primarily used for feature extraction and dimensionality reduction. They reconstruct an output that closely resembles the original input data, capturing crucial patterns to facilitate accurate detection. The encoder converts the input dataset into code of the HL by $code(c) = f(w.x + b)$, where f depicts an activation function, w shows the weight, x refers to the input value, and b indicates a bias. The decoder recreates the output from the code of HL by $x' = f'(w'.c + b')$ and evaluates the mean squared value between reconstructed output and input through the cost $cost = \min \sum_{i=1}^{n} |x' - x|^2$.

A Convolutional AE (CAE) is a variation of the CNN designed to preserve the spatial relationships within the input data. This architecture automatically extracts relevant features and discovers underlying patterns without manual intervention. The encoder compresses the input feature map through convolutional layers, while the decoder reconstructs the output using transposed convolution (deconvolution) layers, enabling effective data representation and reconstruction. Furthermore, the reconstructed fault of the convolution encoder and decoder is evaluated like the typical AE. The significant components of CSAE are the convolution layer, pooling layer, neuron size, sparsity, filter size, and ReLU function. This model comprises three deconvolution blocks of a decoder and four convolution blocks of an encoder, each with batch normalization and convolution layer and filter size (3×3), which is used for generalizing the network's learning process. Then, the max pooling (2×2 kernel size) layer with sparsity is applied for down-sampling the feature maps of the convolution encoder. Now, the sparsity highlights the pertinent feature for learning. The convolution layer and activation are added to the batch normalization, the convolution decoder. After the two convolution blocks, an up-sampling layer (2×2 kernel size) is used.

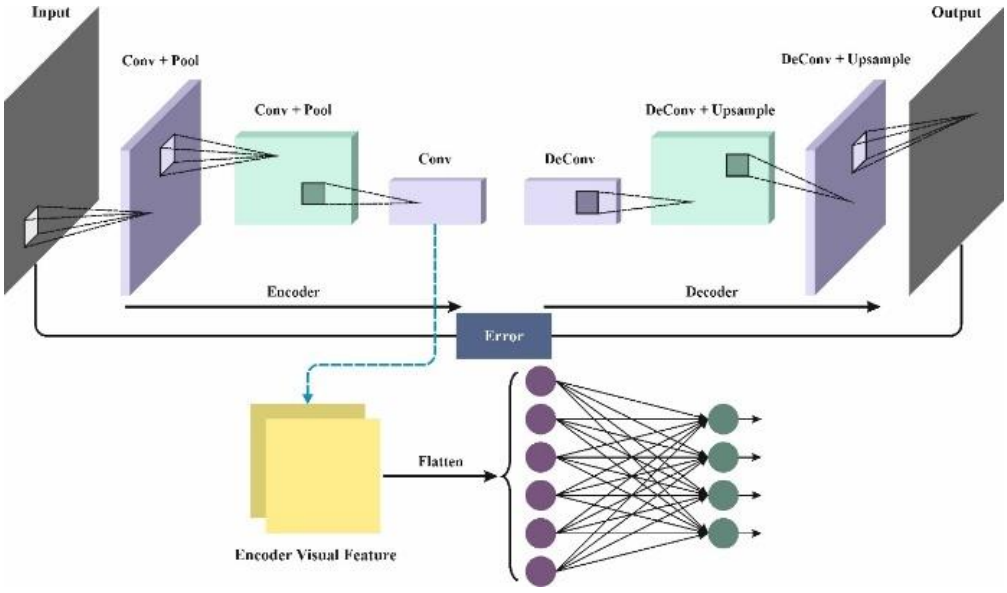

Fig. 3: Architecture of CSAE

Firstly, the inputs are encoded with a pixel patch $x_i, i = 1,2 \ldots x_n$ and multiplied with neuron $weight\ sw_j$, where j is applied to compute the convolution layer. Lastly, the output layer 0_{ij} is evaluated as $o_{ij} = f(w_j . x_i + b)$. Next, the output from the convolution decoder is described by $x_i' = f'(w_j' . 0_{ij} + b)$. Lastly, reconstruction error is computed by $CSA = \frac{1}{P}\sum_{i=1}^{p} \| x_i - x_i' \|$, where p refers to a reconstructed operation of convolution kernel size with dxd, where $d \leq pixels$.

Results Analysis

The BDRFFS-DL technique in examined in this section. The method runs on Python 3.6.5 with an i5-8600k CPU, 4GB GPU, 16GB RAM, 250GB SSD, and 1TB HDD, using a 0.01 learning rate, ReLU, 50 epochs, 0.5 dropout, and batch size 5. In Table 1 and Fig. 4, the Execution Time (ET) of the BDRFFS-DL technique is examined under varying numbers of transactions (Tx) and nodes. The results show that the BDRFFS-DL technique acquires effectual EXET values. With 100 Txs, the BDRFFS-DL technique presents minimal EXET of 17s, 30s, 143s, and 289s under 20-80 nodes, respectively. Additionally, with 200 Txs, the BDRFFS-DL model delivers the least EXET of 26s, 52s, 420s, and 617s below 20-80 nodes, correspondingly. Meanwhile, with 300 Txs, the BDRFFS-DL method presents the least EXET of 56s, 102s, 627s, and 962s under 20-80 nodes, respectively.

Table 2 and Fig. 5 signify the Transaction Mining Time (TMT) comparison outputs of the BDRFFS-DL technique illustrating the enhanced outcomes with the least TMT values. The BDRFFS-DL technique consistently outperforms other models, achieving the lowest TMT values of 0.00058 seconds at 5 Txs, 0.00084 seconds at 15 Txs, and 0.00088 seconds at 25 Txs, compared to higher values from Pow, ePow, and BHS-ALOHDL.

(1) The detection results of the BDRFFS-DL model are verified by employing the ToN_IoT dataset. It holds 50000 instances with dual classes, as demonstrated in Table 3. The BDRFFS-DL approach has selected 28 features from the 44 features.

Table 1: ET analysis of BDRFFS-DL technique under various transactions and nodes

ET (Sec)				
Tx	20 Nodes	40	60	80
100	17	30	143	289
150	24	36	302	439
200	26	52	420	617
250	54	78	516	910
300	56	102	627	962

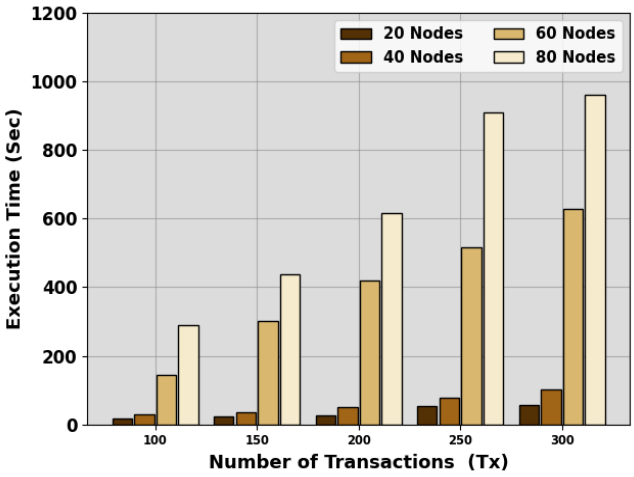

Fig. 4: ET analysis of BDRFFS-DL technique under various nodes

Table 2: TMT analysis of BDRFFS-DL technique under various transactions

TMT (Sec)				
No. of Transactions (Tx)	Pow	ePoW	BHS-ALOHDL	BDRFFS-DL
5	0.00222	0.00146	0.00108	0.00058
10	0.00280	0.00161	0.00099	0.00050
15	0.00266	0.00201	0.00094	0.00084
20	0.00254	0.00174	0.00099	0.00047
25	0.00276	0.00181	0.00091	0.00088

Figure 6 presents the classifier outputs of the BDRFFS-DL approach under all two classes using test dataset. Figs. 6a-6b depicts the confusion matrix at 70:30 of TRAP/TESP. Likewise, Fig. 6c-d validates the PR and ROC study of the BDRFFS-DL model. The figure illustrates greater results with the most excellent ROC values.

The detection results of the BDRFFS-DL approach are inspected with 70:30 of TRAP/TESP in Table 4 and Fig. 7. With 70:30 of TRAP/TESP, the BDRFFS-DL approach attains an average $accu_y$ of 98.80% and 98.91%, $prec_n$ of 98.80% and 98.91%, $reca_l$ of 98.80% and 98.91%, F_{score} of 98.80% and 98.91%, AUC_{score} of 98.80% and 98.91%, and Kuppa of 98.87% and 98.95.

The $accu_y$ curves for TRA and validation (VL) illustrated in Fig. 8. Both TRA/TES $accu_y$ steadily improve with growing epochs, showing the ability of the model in learning patterns and generalize well to unseen data.

Table 4: Detection output of BDRFFS-DL technique with 70:30 of TRAP/TESP

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	AUC_{Score}	Kuppa
TRAP (70%)						
Normal	99.04	98.58	99.04	98.81	98.80	98.88
Attack	98.57	99.03	98.57	98.80	98.80	98.86
Average	98.80	98.80	98.80	98.80	98.80	98.87
TESP (30%)						
Normal	99.16	98.67	99.16	98.91	98.91	98.92
Attack	98.67	99.16	98.67	98.92	98.91	98.97
Average	98.91	98.91	98.91	98.91	98.91	98.95

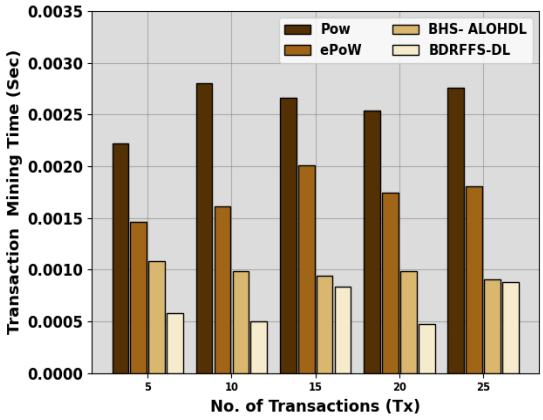

Fig. 5: TMT analysis of BDRFFS-DL technique under various transactions

Table 3: Dataset description

Classes	Instance Numbers
Normal	25000
Attack	25000
Overall Instances	50000

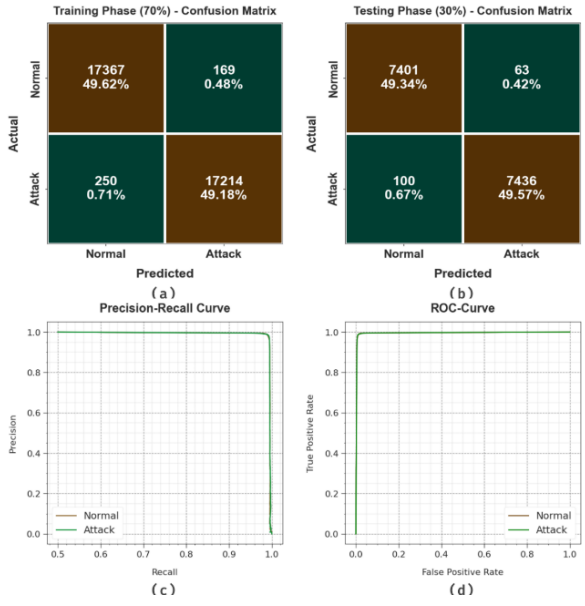

Fig. 6: Classifier result of (a-b) confusion matrices and (c-d) PR and ROC curves

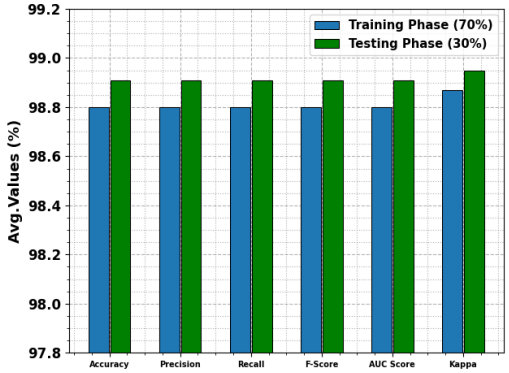

Fig. 7: Average of BDRFFS-DL technique with 70:30 of TRAP/TESP

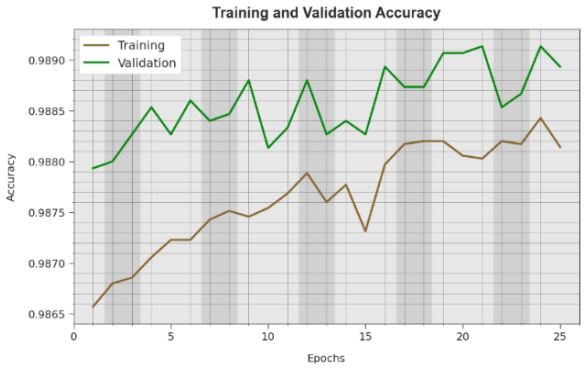

Fig. 8: $Accu_y$ the curve of the BDRFFS-DL method

Figure 9 outlines the TRA/TES loss for the BDRFFS-DL technique across diverse epochs. The TRA loss steadily lessens as the weight is refined, illustrating effective learning. The BDRFFS-DL model consistently improves parameters to minimize the gap between actual and predicted TRA labels.

Table 5 and Fig. 10 depict the comparison assessment of the BDRFFS-DL model (Alamro *et al.*, 2023). Based on $accu_y$, the BDRFFS-DL model reaches an improved $accu_y$ of 98.91% while the IDS, DT, RF, NB, and BiLSTM techniques obtain decreased $accu_y$ of 98.43%, 96.49%, 97.86%, 96.84%, and 96.36%.

Meanwhile, based on $prec_n$, the BDRFFS-DL approach ranges enhanced $prec_n$ of 98.91% while the IDS, DT, RF, NB, and BiLSTM techniques get reduced

$prec_n$ of 98.08%, 98.28%, 98.39%, 96.74%, and 97.71%. Furthermore, based on F_{score}, the BDRFFS-DL technique attains an enhanced F_{score} of 98.91%, where the IDS, DT, RF, NB, and BiLSTM techniques gain diminished F_{score} of 98.71%, 96.24%, 98.67%, 97.15%, and 97.99%. These outcomes displayed the better performance of the BDRFFS-DL method.

Table 6 and Fig. 11 specify the Computational Time (CT) evaluation of the BDRFFS-DL approach with existing models. The BDRFFS-DL approach demonstrates the fastest CT with 4.01 seconds, indicating superior efficiency. In contrast, the IDS model records the highest CT at 12.56 seconds, illustrating it is the most time-consuming. Decision Tree (DT) and Random Forest (RF) follow with CT values of 7.62 and 6.78 seconds, respectively, giving a moderate performance. Naïve Bayes (NB) exhibits a CT of 11.47 seconds while Bi-LSTM takes 8.91 seconds, requiring more time than RF but less than the IDS model.

Table 7 and Fig. 12 demonstrate the ablation study of the BDRFFS-DL methodology with existing models. The BDRFFS-DL methodology demonstrated superior performance, achieving an $accu_y$ of 98.91%, $prec_n$ of 98.91%, $reca_l$ of 98.91%, and F_{score} of 98.91%, indicating highly balanced and consistent results across all metrics. In comparison, the CSAE and DRF models attained lesser values. These results highlight the reliability and robustness of the BDRFFS-DL model in handling classification tasks.

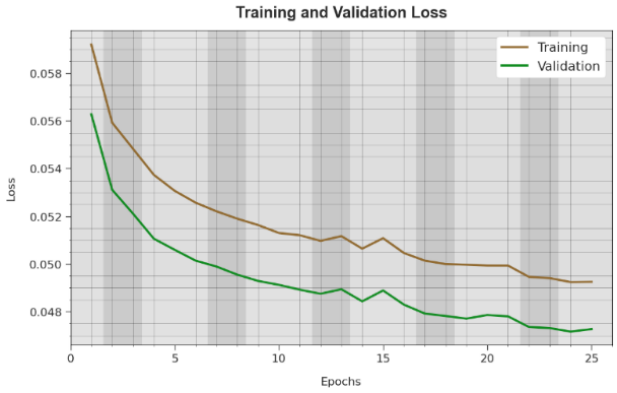

Fig. 9: Loss curve of the BDRFFS-DL method

Table 5: Comparison evaluation of BDRFFS-DL approach with existing models

Techniques	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
BDRFFS-DL	98.91	98.91	98.91	98.91
IDS	98.43	98.08	98.67	98.71
DT	96.49	98.28	97.47	96.24
RF	97.86	98.39	96.50	98.67
NB	96.84	96.74	98.54	97.15
BiLSTM	96.36	97.71	98.22	97.99

Table 6: CT analysis of BDRFFS-DL approach with existing methods

Methods	CT (sec)
BDRFFS-DL	4.01
IDS Model	12.56
DT	7.62
RF	6.78
NB	11.47
Bi-LSTM	8.91

Table 7: Result evaluation of the ablation study of BDRFFS-DL model

Techniques	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
BDRFFS-DL	98.91	98.91	98.91	98.91
CSAE	98.30	98.33	98.20	98.20
DRF	97.61	97.82	97.67	97.55

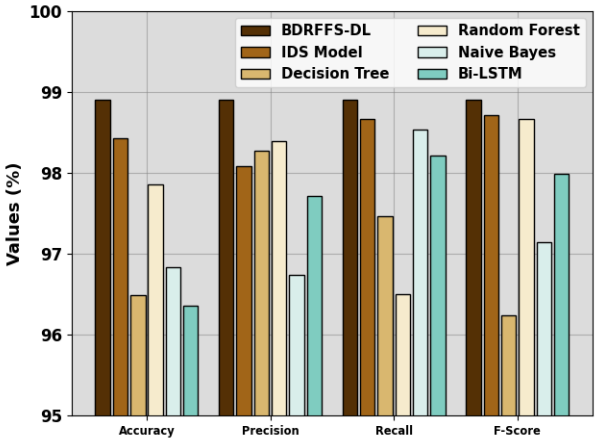

Fig. 10: Comparison evaluation of BDRFFS-DL approach with existing models

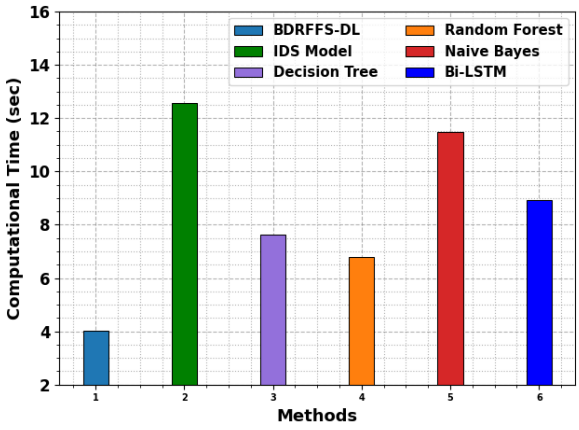

Fig. 11: CT analysis of BDRFFS-DL approach with existing methods

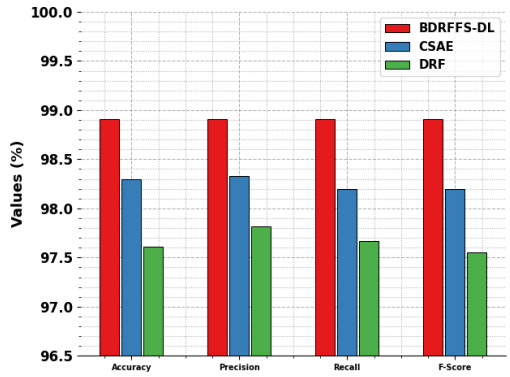

Fig. 12: Result analysis of the ablation study of BDRFFS-DL approach

Conclusion

This research presents a novel BDRFFS-DL model for the effective identification of intrusions. The BDRFFS-DL technique exploits the FS approach to pick a relevant subset of features, thereby improving classification accuracy and decreasing the computation complexity. Initially, Z-score standardization is applied. To improve the classification performance and resolve the high dimensionality problem, the BDRFFS-DL technique applies a DRF optimizer to choose the finest feature subset. Lastly, the intrusion detection process is carried out using the CSAE model. Furthermore, BC is applied to ensure the detection result's integrity and provide a secure record of network actions. An extensive study of the BDRFFS-DL approach using the ToN_IoT dataset illustrated its superior performance, achieving an accuracy of 98.91%, outperforming existing models. The limitations of the BDRFFS-DL technique comprise limited evaluation under real-time network conditions and restricted scalability across heterogeneous environments. The use of static datasets may not fully capture evolving attack patterns, leading to potential performance degradation in dynamic scenarios. Furthermore, the reliance on complex models can result in high computational overhead, making deployment challenging for resource-constrained devices. There is also insufficient focus on interpretability, which affects trust and adoption in critical sectors. Integration with privacy-preserving mechanisms remains minimal, raising concerns in sensitive applications. Future works may explore lightweight model architectures, adaptive learning mechanisms, real-time benchmarking, enhanced interpretability, and secure collaborative detection frameworks across distributed environments.

Acknowledgment

Thank you to the publisher for their support in the publication of this research article. We are grateful for the resources and platform provided by the publisher, which have enabled us to share our findings with a wider audience. We appreciate the efforts of the editorial team in reviewing and editing our work, and we are thankful for the opportunity to contribute to the field of research through this publication.

Funding information

The corresponding author states on behalf of all authors that they did not receive any funds for this project.

Author's Contributions

C. Ananth: Contributed to the conceptualization and methodology design of the study, formulating the core research idea and framework.

S. Sathiyarani: Carried out the data analysis, refined the overall concept, and was primarily responsible for manuscript writing, review, and editing, ensuring coherence and technical accuracy.

N. Mohananthini: Was involved in data collection, preparation of datasets, and drafting sections of the manuscript, providing essential support in organizing and presenting the research findings.

Ethics

No ethics approval is required.

Conflicts of Interest

The authors declare no conflict of interest.

Competing Interests

The authors declare no competing interest.

Data Availability Statement

The ToN_IoT dataset that support the findings of this study are openly available at https://research.unsw.edu.au/projects/toniot-datasets.

References

Abdel-Basset, M., Moustafa, N., Hawash, H., Razzak, I., Sallam, K. M., & Elkomy, O. M. (2022). Federated Intrusion Detection in Blockchain-Based Smart Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems*, *23*(3), 2523–2537. https://doi.org/10.1109/tits.2021.3119968

Abdullah, A. S., Sunil, H. J., & Nazmudeen, M. S. H. (2025). A New Model to Evaluate Signature and Anomaly Based Intrusion Detection in Medical IoT System Using Ensemble Approach. *SN Computer Science*, *6*(4), 347. https://doi.org/10.1007/s42979-025-03875-9

Al Mazroa, A., Albogamy, F. R., Khairi Ishak, M., & Mostafa, S. M. (2025). Boosting Cyberattack Detection Using Binary Metaheuristics With Deep Learning on Cyber-Physical System Environment. *IEEE Access*, *13*, 11280–11294. https://doi.org/10.1109/access.2025.3526258

Alabdali, A. M., & Mashat, A. (2024). A novel approach toward cyberbullying with intelligent recommendations using deep learning based blockchain solution. *Frontiers in Medicine*, *11*. https://doi.org/10.3389/fmed.2024.1379211

Alamro, H., Maray, M., Aljabri, J., Alahmari, S., Abdullah, M., Alqurni, J. S., Alotaibi, F. A., & Mohamed, A. A. (2025). Mathematical modelling-based blockchain with attention deep learning model for cybersecurity in IoT-consumer electronics. *Alexandria Engineering Journal*, *113*, 366–377. https://doi.org/10.1016/j.aej.2024.11.016

Alamro, H., Marzouk, R., Alruwais, N., Negm, N., Aljameel, S. S., Khalid, M., Hamza, M. A., & Alsaid, M. I. (2023). Modeling of Blockchain Assisted Intrusion Detection on IoT Healthcare System Using Ant Lion Optimizer With Hybrid Deep Learning. *IEEE Access*, *11*, 82199–82207. https://doi.org/10.1109/access.2023.3299589

Alkadi, O., Moustafa, N., & Turnbull, B. (2021). *A Collaborative Intrusion Detection System Using Deep Blockchain Framework for Securing Cloud Networks*. 553–565. https://doi.org/10.1007/978-3-030-55180-3_41

Alqahtany, S. S., Shaikh, A., & Alqazzaz, A. (2025). Enhanced Grey Wolf Optimization (EGWO) and random forest based mechanism for intrusion detection in IoT networks. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-024-81147-x

Bahri, M. A. E., Jemili, F., & Korbaa, O. (2023). Towards Deep Learning and Blockchain-based Intrusion Detection System. *2023 International Conference on Cyberworlds (CW)*, 357–364. https://doi.org/10.1109/cw58918.2023.00063

Cochran, J. M., Leproux, A., Busch, D. R., O'Sullivan, T. D., Yang, W., Mehta, R. S., Police, A. M., Tromberg, B. J., & Yodh, A. G. (2021). Breast cancer differential diagnosis using diffuse optical spectroscopic imaging and regression with z-score normalized data. *Journal of Biomedical Optics*, *26*(02), 026004. https://doi.org/10.1117/1.jbo.26.2.026004

Dontu, S., Addula, S. R., Kumar Pareek, P., Vallabhaneni, R., & Fallah, M. H. (2024). A Feature Selection based Decisive Red Fox Algorithm with Deep Learning for Protecting Cybersecurity Network. *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, 1–7. https://doi.org/10.1109/iacis61494.2024.10721671

Ferrag, M. A., Shu, L., Djallel, H., & Choo, K.-K. R. (2021). Deep Learning-Based Intrusion Detection for Distributed Denial of Service Attack in Agriculture 4.0. *Electronics*, *10*(11), 1257. https://doi.org/10.3390/electronics10111257

He, X., Chen, Q., Tang, L., Wang, W., & Liu, T. (2023). CGAN-Based Collaborative Intrusion Detection for UAV Networks: A Blockchain-Empowered Distributed Federated Learning Approach. *IEEE Internet of Things Journal*, *10*(1), 120–132. https://doi.org/10.1109/jiot.2022.3200121

Kumaran, N., & Mohan, J. S. S. (2024). BRDO: Blockchain Assisted Intrusion Detection Using Optimized Deep Stacked Network. *Cybernetics and Systems*, *55*(8), 2071–2092. https://doi.org/10.1080/01969722.2023.2175153

Liang, C., Shanmugam, B., Azam, S., Karim, A., Islam, A., Zamani, M., Kavianpour, S., & Idris, N. B. (2020). Intrusion Detection System for the Internet of Things Based on Blockchain and Multi-Agent Systems. *Electronics*, *9*(7), 1120. https://doi.org/10.3390/electronics9071120

Liu, L., Tsai, W.-T., Bhuiyan, Md. Z. A., Peng, H., & Liu, M. (2022). Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum. *Future Generation Computer Systems*, *128*, 158–166. https://doi.org/10.1016/j.future.2021.08.023

Mafarja, M., Thaher, T., Al-Betar, M. A., Too, J., Awadallah, M. A., Abu Doush, I., & Turabieh, H. (2023). Classification framework for faulty-software using enhanced exploratory whale optimizer-based feature selection scheme and random forest ensemble learning. *Applied Intelligence*, *53*(15), 18715–18757. https://doi.org/10.1007/s10489-022-04427-x

Monirah, A. A., & Ykhlef, M. (2023). DeepBlock: a Collaborative Intrusion Detection Framework Based on Blockchain and Deep Learning. *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA)*, 180–185. https://doi.org/10.1109/bcca58897.2023.10338903

Mansour, R. F. (2022). Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment. *Scientific Reports*, *12*(1), 12937. https://doi.org/10.1038/s41598-022-17043-z

Mbaya, E. B., Adetiba, E., Badejo, J. A., Wejin, J. S., Oshin, O., Isife, O., Thakur, S. C., Moyo, S., & Adebiyi, E. F. (2023). SecFedIDM-V1: A Secure Federated Intrusion Detection Model With Blockchain and Deep Bidirectional Long Short-Term Memory Network. *IEEE Access*, *11*, 116011–116025. https://doi.org/10.1109/access.2023.3325992

Mohana, M., & Subashini, P. (2023). *Convolutional Sparse Autoencoder for Emotion Recognition*. *164*, 3–15. https://doi.org/10.1007/978-3-031-27762-7_1

Narayanan, U., & Paul, V. (2023). Twin chain: A Blockchain based Federated Learning Intrusion Detection System using Optimized Backpropagation based Neural Network for Edge Assisted IoT Networks. https://doi.org/10.21203/rs.3.rs-3214924/v1

Oseni, A., Moustafa, N., Creech, G., Sohrabi, N., Strelzoff, A., Tari, Z., & Linkov, I. (2023). An Explainable Deep Learning Framework for Resilient Intrusion Detection in IoT-Enabled Transportation Networks. *IEEE Transactions on Intelligent Transportation Systems*, *24*(1), 1000–1014. https://doi.org/10.1109/tits.2022.3188671

Perumal, E., Arulanthu, P., Ramachandran, R., & Singh, R. (2024). Enhanced Metaheuristics with Deep Learning Model for Blockchain Assisted Cyber Security Solution in Internet of Things Environment. *2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)*, 1–7. https://doi.org/10.1109/ic-etite58242.2024.10493229

Poorazad, S. K., Benzaïd, C., & Taleb, T. (2023). Blockchain and Deep Learning-Based IDS for Securing SDN-Enabled Industrial IoT Environments. *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, 2760–2765. https://doi.org/10.1109/globecom54140.2023.10436839

Rabie, O. B. J., Selvarajan, S., Hasanin, T., Alshareef, A. M., Yogesh, C. K., & Uddin, M. (2024). A novel IoT intrusion detection framework using Decisive Red Fox optimization and descriptive back propagated radial basis function models. *Scientific Reports*, *14*(1), 386. https://doi.org/10.1038/s41598-024-51154-z

Salami, Y., Ebazadeh, Y., Hamrang, M., & Allahbakhshi, N. (2024). A Novel Approach for Intrusion Detection System in IoT Using Correlation-Based Hybrid Feature Selection and Harris Hawk Optimization Algorithm. *Journal of Optimization of Soft Computing (JOSC*, *2*(3), 7–21.

Saveetha, D., & Maragatham, G. (2022). Design of Blockchain enabled intrusion detection model for detecting security attacks using deep learning. *Pattern Recognition Letters*, *153*, 24–28. https://doi.org/10.1016/j.patrec.2021.11.023

Shobana, M., Shanmuganathan, C., Challa, N. P., & Ramya, S. (2022). An optimized hybrid deep neural network architecture for intrusion detection in real-time IoT networks. *Transactions on Emerging Telecommunications Technologies*, *33*(12). https://doi.org/10.1002/ett.4609

Vaiyapuri, T., Sbai, Z., Alaskar, H., & Ali, N. (2021). Deep Learning Approaches for Intrusion Detection in IIoT Networks Opportunities and Future Directions. *International Journal of Advanced Computer Science and Applications*, *12*(4). https://doi.org/10.14569/ijacsa.2021.0120411