E-ISSN 2586-9027
Homepage : https://tci-thaijo.org/index.php/SciTechAsia Science & Technology Asia
Vol.31 No.1 January - March 2026 Page: [192-210]
Original research article

OIDS-CS: An Efficient Optimal Intrusion Detection System for Cyber Security using Hybrid Artificial Intelligence

Yogomaya Mohapatra*, Archana Rout, Pravat Kumar Routray

Department of Computer Science and Engineering, Siksha 'O' Anusandhan University, Odisha 751030, India

Received 28 August 2025; Received in revised form 5 February 2026
Accepted 16 February 2026; Available online 27 March 2026

ABSTRACT

Cybersecurity systems face significant challenges in intrusion detection due to high false alarm rates and the inability to accurately detect evolving attack patterns in large-scale network traffic. To address this problem, this paper proposes an Optimal Intrusion Detection System for Cybersecurity (OIDS-CS) based on a hybrid artificial intelligence framework. The proposed OIDS-CS framework for DDoS detection consists of three main stages: preprocessing, feature selection, and intrusion detection and classification. In the preprocessing stage, the network traffic data are cleaned to remove noise and redundancy, improving the quality of the input for subsequent analysis. In the feature selection stage, the extracted features are optimized using the Improved Buzzard Optimization (IBO) algorithm, which minimizes correlation among features and ensures that only the most significant and discriminative features are retained for DDoS detection. Finally, the Residual Artificial Neural Network (RANN) is employed for intrusion detection and classification. The optimized features are used as input to the RANN, which predicts whether a DDoS attack is present or not. The outputs are classified into two categories: DDoS present or DDoS not present. This structured approach not only reduces computational complexity but also improves detection accuracy and robustness against evolving DDoS attack patterns.

Keywords: Cyber security; Classification; DDoS; Detection; IDS; Intrusion

1. Introduction

In internet-connected systems, cybersecurity refers to the set of practices and technologies used to protect hardware, software, networks, and data from cyberattacks, damage, or unauthorized access. It

***Corresponding author:** mohapatrayogomaya@gmail.com **doi:** xx.xxxxx/scitechasia.xxxx.xx

focuses on safeguarding electronic systems and digital information against threats such as hacking, malware, viruses, and other malicious activities [1]. Cybersecurity also addresses privacy and confidentiality issues arising from the extensive use of digital technologies and online platforms. In today's digital era, the rapid growth of internet usage and interconnected systems has significantly increased the frequency and sophistication of cyberattacks and cybercrime [2].

Cybersecurity plays a vital role in protecting sensitive and personal information, including financial records, personal identities, and confidential business data, from unauthorized access, theft, or misuse. Moreover, it helps secure critical infrastructure such as power grids, transportation systems, and communication networks against cyber threats that may cause service disruption or physical damage [3]. Overall, cybersecurity is essential to ensure the confidentiality, integrity, and availability (CIA) of information and systems in the presence of evolving cyber threats.

Network security is a crucial subdomain of cybersecurity that focuses on protecting an organization's information technology (IT) infrastructure and communication networks from unauthorized access, misuse, damage, or disruption. It involves the implementation of technical and administrative controls to prevent unauthorized modification, disclosure, or destruction of data and network resources. The primary objective of network security is to preserve the confidentiality, integrity, and availability of organizational data while ensuring the privacy and protection of legitimate users.

Intrusion in computer networks refers to unauthorized access or malicious activities performed within a network environment [4]. Attackers may exploit various techniques such as hacking, phishing, malware injection, or social engineering to compromise network security. Network intrusions can result in data loss, service disruption, system compromise, or unauthorized disclosure of sensitive information. Therefore, continuous monitoring and robust security mechanisms are required to detect and prevent intrusion attempts effectively [5].

A distributed denial-of-service (DDoS) attack is a severe form of cyberattack aimed at disrupting the normal operation of a network, server, or application by overwhelming it with a massive volume of traffic [6]. This malicious traffic is typically generated using a large number of compromised systems, commonly referred to as a botnet, with the intention of exhausting network or system resources and denying service to legitimate users [7]. DDoS attacks can severely impact organizational operations, causing financial losses, reputational damage, and service outages, making them a critical cybersecurity concern [8].

Several approaches have been proposed for detecting DDoS attacks, including traffic analysis, packet inspection, behavioral analysis, signature-based detection, rate-limiting techniques, and artificial intelligence (AI) and machine learning-based methods [9]. Combining multiple detection strategies often improves detection accuracy and robustness [10]. However, many existing approaches suffer from limitations such as high false-positive rates, scalability issues, evasion by sophisticated attacks, increased complexity, and limited visibility in large-scale networks.

Intrusion Detection Systems (IDS) [11]–[13] are widely used security mechanisms designed to identify unauthorized access, misuse, or malicious activities in com-

puter systems and networks. IDS monitors network traffic, system logs, and other relevant data sources to detect abnormal or suspicious behavior. IDS can be classified as host-based or network-based, and as rule-based or anomaly-based systems. In recent studies, IDS have been employed extensively for detecting DDoS attacks and other network intrusions.

Several intelligent and hybrid intrusion detection approaches have been reported in the literature to mitigate DDoS attacks. For example, fuzzy logic and Q-learning–based IDS frameworks provide adaptive decision-making capabilities but often suffer from increased computational complexity and limited scalability in large-scale networks [14]. Automated security architectures improve responsiveness; however, they rely heavily on predefined policies and lack robustness against evolving attack patterns [15]. Feature ranking and cumulative ranking algorithms enhance cost-effective traffic classification, but their performance degrades when handling high-dimensional or imbalanced datasets [16, 17]. Self-adaptive detection techniques such as MM-CUSUM support protocol-independent DDoS detection, yet they are sensitive to threshold selection and may generate higher false alarms under dynamic traffic conditions [18]. Endpoint optimization-based SON solutions focus on source-side mitigation of flooding attacks; however, their effectiveness is limited in distributed environments and they require extensive coordination among network nodes [19]. Similarly, bio-inspired anomaly-based approaches like BIFAD enable early detection of application-layer DDoS attacks, but they depend on handcrafted features and exhibit reduced generalization capability under diverse and large-scale attack scenarios [20]. These limitations motivate the need for a more robust, scalable, and feature-optimized intrusion detection framework, which the proposed approach aims to address.

Our contributions. For further enhancement in cyber security, efficient optimal IDS technique is proposed for cyber security using hybrid artificial intelligent technique (OIDS-CS).

1. An improved buzzard optimization (IBO) algorithm is used for feature optimization which selects the optimal best features to reduce the data dimensionality issues.

2. Residual artificial neural network (RANN) is introduced for the intrusion detection and classification which present in the given traffic traces.

3. Our proposed OIDS-CS technique is validated by using the benchmark datasets, such as DARPA1998, DARPA LLS DDoS-1.0, CI-CIDS2017, NSL-KDD, and KDD cup, and the simulation results compared with existing IDS systems to validate the performance of proposed OIDS-CS technique.

The remainder of this paper is organized as follows. Section II reviews related IDS techniques for DDoS attack detection. Section III describes the problem formulation and system design. Section IV presents the proposed OIDS-CS methodology. Section V discusses the experimental results and comparative analysis. Finally, Section VI concludes the paper and outlines future research directions.

2. Related Works

Recent studies have explored various IDS techniques for detecting Dis-

tributed Denial of Service (DDoS) attacks using machine learning, deep learning, and optimization-based approaches. Hezavehi et al. [21] introduced anomaly-based IDS using a third-party auditor for cloud environments, achieving low computational overhead and fast response time; however, its dependence on external auditors' limits scalability. Dasari et al. [22] proposed a meta-heuristic association scale with a drift-based ensemble classifier to handle feature deviation in large-scale transactions, but threshold selection remains sensitive to data distribution changes. Daneshgadeh et al. [23] developed an online DDoS detection framework using statistical tests and kernel-based learning, which effectively detects zero-day attacks, though its multi-stage processing increases computational complexity.

Bhandari et al. [24] presented a D-CAD framework deployed at the ISP level, combining entropy and divergence measures to distinguish malicious traffic, but its performance is constrained to SDN-based environments. Gupta et al. [25] proposed a two-layer LSTM-based IDS with improved attack classification accuracy; nevertheless, the use of oversampling increases training time. Kushwah et al. [26] introduced a SaE-ELM-based detection system optimized to mitigate overfitting, achieving high accuracy across multiple datasets, though its generalization to real-time traffic remains unverified. Cil et al. [27] applied deep neural networks for DDoS detection and achieved high accuracy on CICDDoS2019, but classification performance degraded for minority attack classes.

Nascimento et al. [28] proposed a non-intrusive DDoS detection approach using hardware performance counters, reducing reliance on external datasets, yet its applicability is limited to enterprise server environments. Correa et al. [29] evaluated machine learning-based DDoS detection in cloud–edge–fog environments and demonstrated better performance than signature-based IDS, though accuracy remained moderate under bandwidth constraints. Almiani et al. [30] introduced a Kalman back-propagation neural network for IoT-based 5G networks, achieving low false alarm rates; however, its adaptability to rapidly evolving attack patterns is limited.

Although existing IDS approaches demonstrate promising performance, most suffer from high false alarm rates, scalability issues, dataset dependency, or limited adaptability to evolving DDoS attacks. These limitations motivate the development of a robust, optimized, and scalable IDS framework capable of improving detection accuracy while reducing false positives and computational overhead.

3. Problem Methodology and System Architecture

3.1 Problem methodology

Recent studies, such as Dora et al. [31], have demonstrated that hybrid deep learning models combined with optimization algorithms can improve DDoS detection accuracy. Their CP-GWO-based CNN–OLSTM framework effectively selects optimal features and mitigates overfitting, achieving notable performance gains on benchmark datasets. However, such approaches remain limited by centralized training, high false alarm rates, restricted adaptability to evolving attack patterns, and scalability issues when handling high-dimensional and large-scale network traffic.

In general, existing intrusion detection systems (IDS) for DDoS attacks suffer from several key limitations: (i) high false positive and false negative rates, (ii) re-

liance on hand-crafted or static feature sets, (iii) overfitting caused by high data dimensionality, (iv) limited capability to adapt to new and unseen attack behaviors, and (v) high computational overhead that restricts scalability in real-time and large-scale network environments. Moreover, most existing methods are trained in a centralized manner, making them unsuitable for distributed or privacy-sensitive environments.

To overcome these limitations, this work proposes an Optimal Intrusion Detection System for Cybersecurity (OIDS-CS) that differs from existing approaches in the following aspects. First, the data are preprocessed to remove noise and redundant features, which helps improve model training and reduces overfitting. Second, an improved buzzard optimization (IBO) algorithm is introduced for feature optimization, which effectively reduces dimensionality while minimizing overfitting and computational cost. Third, a Residual Artificial Neural Network (RANN) is utilized for intrusion detection and classification, enabling deeper feature learning and improved detection of complex and evolving DDoS attack patterns. Unlike conventional IDS models, the proposed OIDS-CS framework is designed to adapt automatically to changing traffic trends and handle multiple subclasses of DDoS attacks with enhanced accuracy and robustness.

Based on these motivations, the main objectives of the proposed OIDS-CS framework are summarized as follows:

- To develop a real-time malicious traffic prediction model capable of distinguishing normal and abnormal network behavior.
- To improve DDoS detection accuracy using a hybrid deep learning and optimization-based framework.
- To enable adaptive learning for evolving network traffic and attack patterns.
- To validate the proposed model across multiple subclasses of DDoS attacks.
- To evaluate the effectiveness of the proposed system using comprehensive error and quality performance metrics.

3.2 System architecture of proposed OIDS-CS technique

The proposed OIDS-CS technique consists of a set of processes, which are described in Fig. 1. Initially, various datasets related to DDoS attacks are collected, including DARPA1998, KDD cup, CICID2017, NSL-KDD, and DARPA LLS DDoS-1.0. After the data collection process, pre-processing is applied. The preprocessing, which includes data cleaning, data normalization, and data integration to deal with missing or irrelevant data, is performed on the collected network traffic traces. An improved bat optimization (IBO) algorithm is used to select the optimal features from the input. An IBO algorithm is responsible for data dimensionality reduction and solves the over-fitting problems with the help of standard feature optimization. The selected features are trained with the help of a standard layer architecture in the IDS scheme; here, we need a proper neural network to detect and classify the exact status of the DDoS class. Here, we utilized the Recurrent Artificial Neural Network (RANN) for the detection and classification of DDoS attacks in the given traffic flow. The selected optimal features are used as inputs to the RANN to train either ”DDoS present” or ”DDoS not present” will appear on the network’s output.

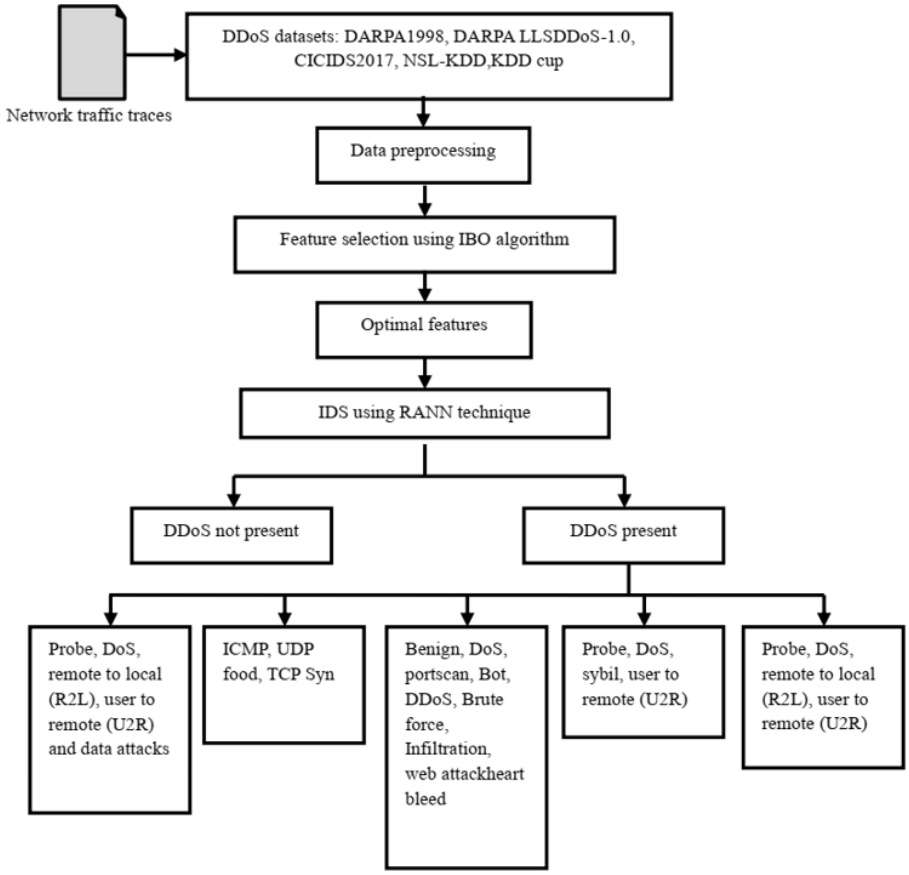

Fig. 1. System architecture of proposed OIDS-CS.

4. Proposed Methodology

The proposed OIDS-CS framework for DDoS detection consists of three main stages: preprocessing, feature selection, and intrusion detection and classification. In the preprocessing stage, the network traffic data are cleaned to remove noise and redundancy, improving the quality of the input for subsequent analysis. In the feature selection stage, the extracted features are optimized using the Improved Buzzard Optimization (IBO) algorithm, which minimizes correlation among features and ensures that only the most significant and discriminative features are retained for DDoS detection. Finally, the Residual Artificial Neural Network (RANN) is employed for intrusion detection and classification. The optimized features are used as input to the RANN, which predicts whether a DDoS attack is present or not. The outputs are classified into two categories: DDoS present or DDoS not present. This structured approach not only reduces computational complexity but also improves detection accuracy and robustness against evolving DDoS attack patterns.

4.1 Pre-processing

Preprocessing is a critical step in network traffic classification, as it ensures that raw data is cleaned, normalized, and transformed into a suitable format for deep learning models. Proper preprocessing improves

model performance by reducing noise, handling missing values, and standardizing feature representations. During preprocessing, the network traffic features are first transformed using one-hot encoding and then normalized to ensure consistent feature scaling. Before pre-processing, the CIC-IDS2017 dataset is divided into three mutually exclusive subsets: training, validation, and testing. Specifically, 70% of the data is used for training, 15% for validation, and the remaining 15% for testing. The training set is utilized to learn the model parameters, while the validation set is employed for hyperparameter tuning and to prevent overfitting. The test set is reserved exclusively for final performance evaluation and is not used during model training or optimization. This data partitioning strategy ensures an unbiased assessment of the proposed intrusion detection framework.

4.1.1 One-hot processing

The dataset contains three symbolic data types: flag, service, and protocol type. These features are mapped into binary vectors using one-hot encoding. The CIC-IDS- 2017 dataset is transformed using the one-hot encoding technique to convert numerical features into symbolic characteristics. For example, the second feature of the CIC-IDS-2017 dataset sample represents a protocol type. A type may consist of one of three: tcp, udp, or icmp. The one-hot encoding method converts categorical data into binary vector representations that a computer can handle, with TCP encoded as [1,0,0], UDP as [0,1,0], and ICMP as [0,0,1].

4.1.2 Resampling

To address the class imbalance present in the CIC-IDS2017 dataset, a data balancing strategy is applied during preprocessing. Minority attack samples are augmented using oversampling techniques to ensure a more balanced class distribution, thereby preventing bias toward majority classes during model training.

4.1.3 Normalization processing

The original data's value might be excessively high, which results in issues like "large numbers to eat decimals," uneven weights, and data processing failures, among others. We utilize a common Scaler for classifying ongoing data into the [0, 1] range. Normalization removes any effect of the unit of measurement during practice, increasing the reliance of the outcome on the fundamental components of the data. The equation is shown in Eq. (2.1).

$$A_{new} = \frac{A_{current} - A_{min}}{A_{max}}, \qquad (4.1)$$

where A_{new} represents the Normalized feature, $A_{current}$ represents the Current feature, A_{min} represents the lowest possible value feature for the relevant section and A_{max} represents the highest possible value feature for the relevant section.

4.2 Feature selection using the Improved Buzzard Optimization algorithm

Feature selection plays a crucial role in improving detection accuracy by reducing data dimensionality, minimizing overfitting, and enhancing model interpretability. In this work, feature selection is performed to identify the most discriminative features for effective DDoS attack detection.

An Improved Buzzard Optimization (IBO) algorithm is employed to select optimal features from the input dataset. Buzzard Optimization is a swarm intelligence–based algorithm inspired by the collective food-searching behavior of birds, where candidate solutions iteratively update their positions based on individual and global

best solutions. To enhance convergence efficiency and solution quality, the proposed IBO introduces an improved balance between exploration and exploitation, enabling faster convergence and better search capability in high-dimensional feature spaces.

The IBO-based feature optimization effectively selects salient feature points by evaluating detector responses using a moving window mechanism, while maintaining invariance to scale, rotation, and affine transformations. This optimized feature subset significantly reduces computational complexity and improves the performance of the subsequent intrusion detection and classification stages. The conventional nonlinear diffusion is characterized as,

$$\frac{\partial l}{\partial s} = Div(C(y, x, s), \nabla l). \quad (4.2)$$

The conductivity, divergence denotes as C and Div, respectively.

4.3 Solution initialization

Solution initialization is an important process in all optimization algorithms. In this stage, the input features are treated as candidate solutions. The search space is assumed to be large and is represented in a D-dimensional space. Accordingly, the position vector of the j-th particle in the D-dimensional search space is defined as follows:

$$l_j = (L_{j1}, L_{j2}, L_{j3}, ..., L_{jD}). \quad (4.3)$$

The ability vector known as the C-vector is made up of the ability to taste and smell particles. The C_j a definition of the j-th particle's vector:

$$C_j = (C_{j1}, C_{j2}, C_{j3}, ..., C_{jD}). \quad (4.4)$$

The following $C^*_{h,best}$ is a definition of the ideal position for the i particle:

$$C^*_{j,best} = (C^*_{j1}, C^*_{j2}, C^*_{j3}, ..., C^*_{jd}). \quad (4.5)$$

The position that is best throughout the particle is $C^*_{h,best}$; which appears as follows:

$$C^*_{h,best} = (C^*_{h1}, C^*_{h2}, C^*_{h3}, ..., C^*_{hd}). \quad (4.6)$$

The new position updating process considers several iterations to reach the optimal solution, in the initial iteration (S = 1) to obtain the optimal position for all particles.

$$C^*_{j,best} = l_j(s) \quad j = 1, 2, 3, ..., D. \quad (4.7)$$

Fitness calculation: Following the initialization step, the proposed IBO algorithm evaluates the quality of all candidate solutions. Each generated solution is subjected to a fitness evaluation process, where the fitness value is computed based on the classification accuracy achieved by the corresponding model. Higher classification accuracy indicates better fitness of the solution. Accordingly, the fitness function used in the IBO framework is defined as follows:

$$Fitness = \text{Max}(Accuracy). \quad (4.8)$$

4.4 Updating process

After fitness calculation, we update the solution using IBO operations. Two numbers, rand1 and rand2, are chosen at random with a uniform distribution and a value between 0 and 1. $C_j(s-1)$ denotes the optimal solution for the vector to desire termination and $L_j(s-1)$ in iteration (s 1), is the Position vector. The following equation is used to update each particle's ability vector.

$$C_1(s) = \alpha_1 c(s-1) + \alpha_2^* rand^*(C^*_{j,best} - L_j(s-1)), \quad (4.9)$$

where $C_1(s)$ by considering the problem, $\alpha_1, \alpha_2, \beta, \gamma$ are experimentally determined.

The $\alpha_1, \alpha_2, \beta, \gamma$. Taking into account the issue, experimental methods are used to determine coefficients. However, in general, 1 ought to be less than one due to the divergence and constant increase in $C(s)$ at higher values. Also, keep in mind that, although theoretically, we compute the next step solution through the following rule of zero eliminated condition with $C(s)$ fluctuation. Problems will arise if the coefficient's small value (1) is chosen due to the fact that utilizing large values for these two coefficients causes the particle to sharply deviate from its own path; therefore, they should not be considered to be very large. A threshold for ability is calculated with the help of the following sigmoidal function:

$$T(c_j(s) = \frac{1}{1 + exp(-C_j(s))}. \quad (4.10)$$

Lastly, the following could be used to determine each particle's binary position:

$$l_j(s) = \begin{cases} 1, & \text{if } \rho_j < t(c_j(s)); \\ 0, & \text{if } \rho_j \geq t(c_j(s)), \end{cases} \quad (4.11)$$

where, ρ_j is fixed as a common value within the limit of 0 to 1. The proposed IBO algorithm selects the optimal features for a better detection rate. Those selected features have been verified through the prevalidation process, which is done by the classifier. The particle's length, which is a random binary value, is the maximum number of features. Algorithm 2 describes the working process of feature optimization using IBO.

Algorithm 2: Feature optimization using IBO.

Input : Extracted features, termination condition	
Output: Optimal selected features	
1.	Initialize the random population
2.	Define standard nonlinear diffusion $\frac{\partial l}{\partial s} = Div(C(y, x, s), \nabla l)$.
3.	Define C_j vector of the j-th particle $C_j = (C_{j1}, C_{j2}, C_{j3}, ..., C_{jD})$
4.	If $j = 0$ and $i = 1$
5.	Compute optimal solution to update the i particle is $C^*_{j,best} = (C^*_{j1}, C^*_{j2}, C^*_{j3}, ..., C^*_{jd})$
6	Compute binary position of each particle $l_j(s) = \begin{cases} 1, & \text{if } \rho_j < t(c_j(s)); \\ 0, & \text{if } \rho_j \geq t(c_j(s)), \end{cases}$
7.	Update the final best solution
8.	End

4.5 Intrusion detection using a residual artificial neural network

After feature selection, the selected features are given to the input of the intrusion detection process. Intrusion detection and classification aim to identify malicious network activities, such as DDoS attacks, by analyzing traffic patterns and assigning them to either normal or attack classes. In this work, a RANN is employed for effective intrusion detection.

RANN enhances the learning capability of conventional artificial neural networks by incorporating residual connections between hidden layers, which mitigate the vanishing gradient problem and facilitate stable training of deep networks. These connections allow feature representations from earlier layers to be directly propagated to deeper layers, enabling the model to learn complex and non-linear traffic patterns more effectively.

Compared to traditional ANN-based IDS models, RANN demonstrates improved convergence speed, reduced overfitting, and better generalization performance, particularly in high-dimensional network traffic data. The network is trained using forward and backpropagation mechanisms with consistent parameter configurations to reduce computational complexity and improve training efficiency. Continuous mon-

itoring of network deviations further enhances detection accuracy and robustness against evolving DDoS attack patterns. The layer is designed as follows:

$$\hat{x}^{(j)} = f(w, a, y^{j}). \tag{4.12}$$

The network's weight matrices are denoted as W and b, where the variable j ranges from 1 to M. The cross-entropy loss function 0 is employed during forward propagation to assess the accuracy of the predictions made for each batch of samples, by comparing the predicted labels to the true labels.

$$\Gamma(w, a) = -\frac{1}{M}\sum_{j=1}^{M}(x^{(j)})\log[\hat{x}^{(j)}] + \mu\sum\|w\|^{2}. \tag{4.13}$$

The regularization component for the network's weights is expressed as $\mu\sum\|w\|^{2}$, where $Q\sum\|w\|^{2}$ is a coefficient that determines the strength of the regularization, and is the sum of squares of the weight values. During the back propagation phase, an adaptive moment estimation optimization algorithm is utilized to optimize the RANN parameters. This optimization approach is more effective compared to the traditional stochastic gradient descent algorithm, especially when handling large datasets. As an illustration, let's consider the optimization of the weight w_l. In iterations, the optimization process involves determining the gradient of the loss function 0 with respect to w_l.

$$h_{s}^{L} = \frac{\partial\Gamma(w, a)}{\partial W^{L}}. \tag{4.14}$$

Update the biased estimates of the first and second raw moments.

$$\begin{cases} M_{S}^{L} = \beta_1 \cdot M_{s-1}^{L} + (1-\beta_1)\cdot h_{s}^{l} \\ V_{S}^{L} = \beta_2 \cdot M_{s-2}^{L} + (1-\beta_2)\cdot h_{s}^{l} \end{cases} \tag{4.15}$$

Update the parameters

$$W_{s+1}^{L} = W_{s}^{L} - Lr\cdot\frac{M_{s}^{L}}{\sqrt{s_{s}^{L}}}. \tag{4.16}$$

The exponential decay rates are defined as 1=0.9 and 2=0.999, while the learning rate is set at Lr=0.001. l represents the layer number where the weight w_l is situated. Upon completion of the training process, the performance of the RANN model is evaluated by calculating its accuracy rate (AR). The AR metric indicates the model's prediction accuracy.

$$Br = \frac{K}{N}\times 100\%, \tag{4.17}$$

where n is the total number of test samples and k is the number of samples that have been correctly identified. The analysis reveals the following expression for the RANN-based modulation recognition algorithm because the computation process is somewhat independent of the fitness functions. The method starts by looking at small random values before training the synaptic weights. Estimating the total error E can be done with the RANN adaptive training method.

$$E_i(S) = D_i(S) - o_i(S). \tag{4.18}$$

As observed, an additional input line with a value of 1 is added to take the bias into account. The following equation typically describes the unit transfer function F as a logistic sigmoid:

$$F(Y) = \frac{1}{1+e^{-y}}. \tag{4.19}$$

Dynamic back-propagation is used to train the network. The assumption that the initial state of the network is independent of its initial weights is the foundation of the gradient descent learning algorithm.

$$I(S+1) = [E(S+1)]^{1/2}. \tag{4.20}$$

The cumulative output error time for all nodes in the current stack can be calculated by iterating through the nodes.

$$E_K = \sum_{j=1}^{Mtr} o_j - Z_{K_j}. \qquad (4.21)$$

HereZ_{K_j} represents the obtained output. Algorithm 3 describes the working process of intrusion detection and classification using the RANN technique.

Algorithm 3: Intrusion detection and classification using RANN technique.

Input: optimal features, number of layers, termination condition.
Output: DDoS present, DDoS not present

1. Initialize the random population
2. Define initial fitness $\hat{x}^{(j)}$ is $\hat{x}^{(j)} = f(w, a, y^j)$
3. The gradient of loss function 0 with respect to w $h_s^L = \frac{\partial \Gamma(w,a)}{\partial W^L}$.
4. If $j = 0$ and $i = 1$
5. The compute accuracy rate (AR) is used to measure performance $Br = \frac{K}{N} \times 100\%$
6 Compute the model independent of the initial weights $E(S+1) = \frac{D(S+1)}{x(S+1)}$
7. Find the best output solution
8. End

5. Results and Discussion

In this section, we talk about the results of the simulation and compare the proposed and existing state-of-the-art IDS techniques with respect to the different benchmark datasets. Our OIDS-CS technique is implemented on the Google Colab simulation with the Python programming language. Our OIDS-CS technique is validated through the benchmark datasets, DARPA1998, DARPA LLS DDoS-1.0, CICIDS2017, NSL-KDD, and KDD cup. The simulation results of our OIDS-CS technique are compared with the existing IDS techniques, GWO-O-LSTM [32], PSO-O-LSTM [33], MFO-O-LSTM [34], WOA-O-LSTM [35], and CP-GWO-O-LSTM [31], with respect to accuracy, precision, recall, specificity, F-measure, false positive rate (FPR), and false negative rate (FNR). Experimental used hyper parameter is presented in Table 1.

Table 1. Hyper parameter values.

Parameter	Suggested Value
Number of hidden layers	5
Number of neurons per layer	64
Activation function	ReLU for hidden layers, Softmax for output
Learning rate	0.001
Optimizer	Adam
Batch size	32
Epochs	100
Dropout rate	0.2
Training	80%
Testing	20%

5.1 Dataset description

The results of the simulations show that the proposed OID-CS method performs better than the existing state-of-the-art IDS techniques in terms of accuracy, precision, recall, F-measure, specificity, FPR, and FNR on the benchmark datasets, DARPA1998, KDD cup, CICID2017, NSL-KDD, and DARPA LLS DDoS-1.0. The data concerning this are summarized in Table 1. For each dataset, the number of traffic flows used for training and testing is provided, as well as the total number of traffic flows. These datasets are used to evaluate and compare the performance of different intrusion detection systems.

1. DARPA1998 is a benchmark dataset that has been used to evaluate the performance of intrusion detection systems (IDS). This dataset has been created by the Defense Advanced Research Projects Agency (DARPA) and is commonly used in computer

security research. The dataset contains normal and abnormal (intrusive) network traffic data that can be used to evaluate the accuracy and performance of IDS. The data collected in the DARPA1998 dataset is collected from a military network and represents a real-world scenario that can be used to evaluate the performance of different intrusion detection systems.

2. DARPA LLS DDoS-1.0 is a dataset used for evaluating and comparing the performance of DDoS attack detection techniques. It was created by DARPA for the purpose of advancing the state of the art in intrusion detection. The dataset consists of network traffic data collected from a variety of sources and contains both normal and attack traffic, allowing researchers to evaluate and compare the performance of different DDoS detection techniques.

3. The CICID2017 dataset contains benign network traffic, as well as the latest common attacks, which accurately reflect real-world data (PCAPs). The analysis of the network traffic was performed using the CICFlowMeter tool, resulting in labeled flows based on time stamps, source and destination IP addresses, source and destination ports, protocols, and attack type. The CSV version of CICID2017 consists of 8 files with a total of 2,830,743 rows, each with 79 features. Each row of the dataset is labeled as either ”Benign” or one of 14 different attack types.

4. An enhanced version of the KDD’99 dataset, the NSL-KDD dataset, aims to address some of the limitations of the original dataset. Despite some remaining limitations, the NSL-KDD dataset is widely used as a benchmark for network-based IDS due to a lack of publicly available datasets. Researchers use this dataset to compare the performance of different IDS.

5. The data set for the third international knowledge discovery and data mining tools competition is from the DD cub mining tools competition, which was held in conjunction with KDD-99. The competition task was to build a network intrusion detector, a predictive model capable of distinguishing between ’bad’ connections, called intrusions or attacks, and ’good’ normal connections. A standard set of auditable data can be found in this database, which simulates a wide range of intrusions in a military network environment.

Table 2. Summary of dataset description.

Dataset	Number of traffic flows		
	Training	Testing	Total
DARPA1998	2466929	1099731	3566660
DARPA LLS DDoS-1.0	1024858	856457	1881315
CICID2017	2264594	566149	3566660
NSL-KDD	125973	22544	148517
KDD cup	1074992	311029	1386021

5.2 Comparative analysis

In this subsection, we describe the comparative analysis of proposed and existing state-of-the-art IDS techniques for the DARPA1998 for detecting DDoS attacks. A comparison of IDS is presented in Table 2. The measures used to evaluate the performance of these techniques are accuracy, precision, recall, specificity, F-measure, false positive rate (FPR), and false negative rate (FNR). From the table, it is evident that the proposed OID-CS technique outperforms the existing techniques

in terms of accuracy, with a 98.967% accuracy rate compared to the highest accuracy rate of 96.522% achieved by the CP-GWO-O-LSTM technique. In terms of precision, the OID-CS technique has a precision rate of 0.453%, which is higher than the precision rate of the existing techniques, with the highest precision rate of 0.500% achieved by the PSO-O-LSTM and MFO-O-LSTM techniques. The recall rate of the OID-CS technique is 98.978%, which is higher than the recall rate of the existing techniques, with the highest recall rate of 98.782% achieved by the CP-GWO-O-LSTM technique. The specificity rate of the OID-CS technique is 94.568%, which is higher than the specificity rate of the existing techniques, with the highest specificity rate of 51.613% achieved by the GWO-O-LSTM technique. The F-measure of the OID-CS technique is 98.812%, which is higher than the F-measure of the existing techniques, with the highest F-measure of 97.646% achieved by the PSO-O-LSTM technique. In terms of FPR, the OID-CS technique has an FPR of 0.011%, which is lower than the FPR of the existing techniques, with the lowest FPR of 0.012% achieved by the CP-GWO-O-LSTM technique.

Finally, FNR of the OID-CS technique is 0.011%, which is lower than the FNR of the existing techniques, with the lowest FNR of 0.012% achieved by the CP-GWO-O-LSTM technique. Overall, the proposed OID-CS technique demonstrates superior performance compared to the existing IDS techniques in terms of the F-measure, FPR, and FNR, as well as accuracy, precision, recall, and specificity.

A comparison of various intrusion detection system (IDS) techniques for the DARPA LLS DDoS-1.0 dataset is shown in Table 3. The evaluation measures are accuracy, precision, recall, specificity, the F-measure, the False Positive Rate (FPR), and the False Negative Rate (FNR). The OID-CS (proposed) method has the highest accuracy of 98.689%, followed by CP-GWO-O-LSTM with 95.942%. The other IDS techniques have accuracy values ranging from 94.928% to 95.652%. In terms of precision, the OID-CS (proposed) method has the highest value of 98.978%, followed by CP-GWO-O-LSTM with 97.876%. The other IDS techniques have precision values ranging from 97.338% to 97.724%. The OID-CS (proposed) method also has the highest recall value of 98.879%, followed by CP-GWO-O-LSTM with 98.323%. The other IDS techniques have recall values ranging from 97.117% to 97.872%. The specificity of the OID-CS (proposed) method is 97.564%, followed by CP-GWO-O-LSTM with 50.000%. The other IDS techniques have specificity values of 48.387% and 50.000%. The F-measure of the OID-CS (proposed) method is 98.978%, followed by CP-GWO-O-LSTM with 97.876%. The other IDS techniques have F-measure values ranging from 97.338% to 97.724%. The FPR of the OID-CS (proposed) method is 98.678%, followed by PSO-O-LSTM and WOA-O-LSTM with 97.576%. The other IDS techniques have FPR values ranging from 97.432% to 97.727%. Finally, the FNR of the OID-CS (proposed) method is 0.015, followed by CP-GWO-O-LSTM with 0.017. The other IDS techniques have FNR values ranging from 0.021% to 0.029%. Based on these results, we can conclude that the OID-CS (proposed) method outperforms the other IDS techniques in terms of accuracy, precision, recall, specificity, F-measure, FPR, and FNR.

The data in Table 4 compares the performance of different IDS techniques using the CICID2017 dataset. The measures used

Table 3. Comparative analysis of IDS techniques for DARPA1998 dataset.

IDS techniques	Measures (%)					FPR	FNR
	Accuracy	Precision	Recall	Specificity	F-measure		
GWO-O-LSTM	95.072	97.710	97.117	51.613	97.412	0.484	0.029
PSO-O-LSTM	95.507	97.572	97.720	50.000	97.646	0.500	0.023
MFO-O-LSTM	95.217	97.565	97.416	50.000	97.490	0.500	0.026
WOA-O-LSTM	95.072	97.713	97.121	50.000	97.416	0.500	0.029
CP-GWO-O-LSTM	96.522	97.594	98.782	51.515	98.185	0.485	0.012
OIDS-CS (proposed)	98.967	98.647	98.978	94.568	98.812	0.453	0.011

to evaluate the techniques are accuracy, precision, recall, specificity, F-measure, FPR, and FNR. In general, the proposed OID-CS method has the highest accuracy with 98.771%, followed by CP-GWO-O-LSTM with 96.522%. The WOA-O-LSTM and PSO-O-LSTM techniques have similar accuracy levels of 95.217% and 95.652% respectively.

The GWO-O-LSTM and MFO-O-LSTM techniques have the lowest accuracy levels of 95.072% and 94.928%, respectively. The OID-CS method also has the highest recall rate with 98.799% and the highest specificity rate with 97.356%. The CP-GWO-O-LSTM method has the highest precision rate with 98.185%. In terms of F-measure, the OID-CS method has the highest score with 98.970, followed by CP-GWO-O-LSTM with 98.185. The other techniques have lower F-measure scores, with the lowest score belonging to WOA-O-LSTM with 97.727. The False Positive Rate (FPR) for OID-CS is 98.879%, which is higher than CP-GWO-O-LSTM with 97.594%. The False Negative Rate (FNR) is the lowest for OID-CS with 98.799%, and the highest for MFO-O-LSTM with 97.117%. In conclusion, the OID-CS method has the best overall performance among the IDS techniques compared in the CICID2017 dataset.

In table 5, the performance of different IDS techniques is evaluated using various measures like accuracy, precision, recall, specificity, and F-measure on NSL-KDD dataset. The results show that the OID-CS technique has the highest accuracy with 98.548%. It also has the highest recall with 98.999% and highest precision with 98.396%. However, it has the lowest specificity with 97.235% compared to the other techniques. GWO-O-LSTM has an accuracy of 95.072%, recall of 97.117%, precision of 97.412% and specificity of 51.613%. PSO-O-LSTM has an accuracy of 95.362%, a recall of 97.420%, a precision of 97.568%, and a specificity of 51.613%. MFO-O-LSTM has an accuracy of 95.217%, a recall of 97.273%, a precision of 97.494%, and a specificity of 50%. WOA-O-LSTM has an accuracy of 95.072%, a recall of 97.121%, a precision of 97.416%, and a specificity of 50%. CP-GWO-O-LSTM has an accuracy of 96.377%, a recall of 98.630%, a precision of 98.107% and a specificity of 51.515%. Comparing the results of all the techniques, OID-CS has the highest accuracy, recall, and precision, but has the lowest specificity. In terms of qualitative analysis, the OID-CS (proposed) technique stands out among all the other techniques with the highest accuracy, recall, and precision. It also has the highest F-measure of 0.011. The GWO-O-LSTM, PSO-O-LSTM, MFO-O-LSTM, WOA-O-LSTM, and CP-GWO-O-LSTM techniques

Table 4. Comparative analysis of IDS techniques for DARPA LLS DDoS-1.0 dataset.

IDS Techniques	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	F1-score (%)	FPR (%)	FNR (%)
GWO-O-LSTM	95.652	97.576	97.872	50.000	97.724	50.000	2.128
PSO-O-LSTM	95.652	97.576	97.872	50.000	97.724	50.000	2.128
MFO-O-LSTM	94.928	97.561	97.117	48.387	97.339	51.613	2.883
WOA-O-LSTM	95.652	97.727	97.727	50.000	97.727	50.000	2.273
CP-GWO-O-LSTM	95.942	97.432	98.323	50.000	97.876	50.000	1.677
OIDS-CS (proposed)	98.689	98.678	98.879	97.564	98.678	2.436	1.121

yield similar results, with slight differences in accuracy, recall, precision, and specificity. Overall, our proposed OID-CS is the best-performing technique in terms of accuracy, recall, precision, and F-measure, but it has the lowest specificity. The other techniques have similar results with a slight difference in their performance.

The results in Table 6 show the comparison of different IDS techniques applied to the KDD cup dataset. The measures used are accuracy, precision, recall, specificity, F-measure, FPR, and FNR. According to the table, the proposed OID-CS method has the highest accuracy at 98.978%, followed by CP-GWO-O-LSTM with 96.377%. The FPR and FNR for OID-CS are the lowest compared to other methods, at 98.645% and 98.897%, respectively. In terms of precision, OID-CS has the highest value at 98.789%. In general, the results show that the proposed OID-CS method outperforms other techniques in terms of accuracy, precision, and FPR. This demonstrates the effectiveness of the OID-CS method in detecting intrusion in the KDD cup dataset. It appears that our proposed OID-CS technique consistently outperforms the other IDS techniques across all the datasets in terms of accuracy, precision, recall, specificity, and F-measure. The FPR and FNR values of the OID-CS technique are also lower compared to other IDS techniques, which indicates that it has a lower rate of false positives and false negatives. It is important to note that the results presented in these tables should be taken with caution, as the results of the analysis may be influenced by factors such as the size of the datasets, the types of attacks included in the datasets, and the method used for evaluating the IDS techniques. Further research and experimentation may be necessary to confirm the effectiveness of the OID-CS technique in real-world applications. Table 7 presents a comparative performance evaluation of different IBO-based intrusion detection techniques on three benchmark datasets: CICIDS2017, NSL-KDD, and DDoS-1.0. The models are evaluated using standard classification metrics, namely accuracy, precision, and recall. As observed, the proposed RANN-IBO approach consistently achieves superior performance across all datasets, demonstrating improved detection capability and better generalization compared to traditional SVM, FLS, ANN, and LSTM models optimized with IBO.

5.3 Discussion

The comparative analysis conducted across multiple benchmark datasets—including DARPA1998, DARPA LLS DDoS-1.0, CICID2017, NSL-KDD, and KDD Cup—demonstrates the consistent superiority of the proposed OIDS-CS framework over existing state-of-the-art IDS techniques. Across all datasets, OIDS-CS achieves higher accuracy, precision, recall, specificity, and F-measure, while simultaneously maintaining lower false positive and false negative rates. These results indicate that the proposed model is more reliable in distinguishing mali-

Table 5. Comparative analysis of IDS techniques for CICID2017dataset.

IDS Techniques	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	F1-score (%)	FPR (%)	FNR (%)
GWO-O-LSTM	95.217	97.713	97.269	51.613	97.491	48.387	2.731
PSO-O-LSTM	95.217	97.717	97.273	50.000	97.495	50.000	2.727
MFO-O-LSTM	95.072	97.561	97.264	50.000	97.412	50.000	2.736
WOA-O-LSTM	95.652	97.579	97.876	48.387	97.727	51.613	2.124
CP-GWO-O-LSTM	96.522	97.594	98.782	51.515	98.185	48.485	1.218
OIDS-CS (proposed)	98.771	98.879	98.799	97.356	98.767	2.644	1.201

Table 6. Comparative analysis of IDS techniques for NSL-KDD dataset.

IDS Techniques	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	F1-score (%)	FPR (%)	FNR (%)
GWO-O-LSTM	95.072	97.710	97.117	51.613	97.414	48.387	2.883
PSO-O-LSTM	95.362	97.717	97.420	51.613	97.569	48.387	2.580
MFO-O-LSTM	95.217	97.717	97.273	50.000	97.495	50.000	2.727
WOA-O-LSTM	95.072	97.713	97.121	50.000	97.416	50.000	2.879
CP-GWO-O-LSTM	96.377	97.590	98.630	51.515	98.107	48.485	1.370
OIDS-CS (proposed)	98.548	98.879	98.999	97.235	98.939	2.765	1.001

Table 7. Comparative analysis of IDS techniques for KDD cup dataset.

IDS Techniques	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	F1-score (%)	FPR (%)	FNR (%)
GWO-O-LSTM	95.217	97.717	97.273	50.000	97.494	50.000	2.727
PSO-O-LSTM	95.072	97.713	97.121	50.000	97.416	50.000	2.879
MFO-O-LSTM	95.072	97.561	97.264	50.000	97.412	50.000	2.736
WOA-O-LSTM	95.720	97.561	97.264	50.000	97.412	50.000	2.736
CP-GWO-O-LSTM	96.377	97.447	98.782	48.485	98.110	51.515	1.218
OIDS-CS (proposed)	98.978	98.645	98.897	97.379	98.771	2.621	1.103

Table 8. Comparative Performance Analysis of IBO-Based IDS Techniques on Benchmark Datasets.

Techniques	CICID2017			NSL-KDD			DDoS-1.0		
	Accuracy	Precision	Recall	Accuracy	Precision	Recall	Accuracy	Precision	Recall
SVM_IBO	94.12	95.38	94.97	92.84	94.10	93.52	93.26	94.72	94.18
FLS_IBO	95.03	96.41	95.86	93.91	95.22	94.67	94.38	95.61	95.07
ANN_IBO	95.72	97.05	96.48	94.63	96.01	95.44	95.16	96.34	95.82
LSTM_IBO	96.38	97.59	98.63	95.72	97.11	96.84	96.27	97.48	97.06
RANN + IBO (Proposed)	98.98	98.65	98.90	97.89	98.32	98.11	98.55	98.88	99.00

cious traffic from legitimate traffic and significantly reduces false alarms, which is a major limitation of traditional IDS approaches.

The improved performance of OIDS-CS can be attributed to its integrated design. The multi-scale federated learning mechanism enables effective extraction of discriminative features from distributed traffic sources while preserving data privacy and improving generalization. The Improved Buzzard Optimization (IBO) algorithm further enhances performance by selecting an optimal subset of features, thereby reducing data dimensionality, computational overhead, and overfitting. Finally, the RANN strengthens intrusion detection and classification by enabling deep feature learning with stable convergence, making the model robust to complex and evolving DDoS attack patterns.

From a real-time deployment perspective, OIDS-CS is well-suited for practical cybersecurity environments. The optimized feature set minimizes processing latency, while the residual learning structure accelerates inference and ensures stable detection under high-volume traffic conditions. In addition, the federated learning framework allows the model to adapt continuously to changing network behaviors without requiring centralized data collection, making it scalable for large and heterogeneous network infrastructures. These

characteristics enable OIDS-CS to operate effectively in real-time intrusion detection scenarios, even under high-density DDoS traffic.

Overall, the experimental results confirm that the proposed OIDS-CS framework not only achieves superior detection accuracy across diverse datasets but also offers enhanced robustness, scalability, and real-time adaptability. These advantages make OIDS-CS a promising and practical solution for modern cybersecurity systems facing increasingly sophisticated DDoS attacks.

6. Conclusion

This work addressed key limitations of existing intrusion detection systems, particularly high false alarm rates, poor scalability, data dimensionality issues, and limited adaptability to evolving DDoS attack patterns. Through this study, it is learned that effective intrusion detection requires not only powerful classifiers but also a well-coordinated pipeline for feature extraction, optimization, and classification.

The proposed OIDS-CS framework demonstrates that combining multi-scale federated learning with optimization-driven feature selection significantly improves the quality of learned representations while preserving scalability and reducing redundant information. The use of Improved Buzzard Optimization (IBO) highlights the importance of intelligent feature optimization in mitigating overfitting and reducing computational complexity, which are common challenges in high-dimensional network traffic data. Furthermore, the adoption of a Residual Artificial Neural Network (RANN) confirms that residual learning mechanisms are effective in stabilizing deep model training and enhancing detection reliability for complex and non-linear attack behaviors.

Another important lesson from this research is that hybrid artificial intelligence models, when properly integrated, can outperform single-technique IDS solutions by balancing detection accuracy with robustness and adaptability. The proposed approach also shows that privacy-aware and distributed learning strategies, such as federated learning, are practical and beneficial for modern cyber-security environments.

Overall, this study demonstrates that addressing IDS challenges holistically—through feature learning, optimization, and robust classification—leads to more reliable and scalable intrusion detection systems. The proposed OIDS-CS framework provides a solid foundation for future IDS research and can be extended to handle other attack types and real-world deployment scenarios.

References

[1] Jiang B, Yang J, Ding G, Wang H. Cyber-physical security design in multimedia data cache resource allocation for industrial networks. IEEE Trans Ind Inform. 2019;15(12):6472-80.

[2] Khalili MM, Naghizadeh P, Liu M. Designing cyber insurance policies: The role of pre-screening and security interdependence. IEEE Trans Inf Forensics Secur. 2018;13(9):2226-39.

[3] Zhang Y, Krishnan VVG, Pi J, Kaur K, Srivastava A, Hahn A, et al. Cyber physical security analytics for transactive energy systems. IEEE Trans Smart Grid. 2019;11(2):931-41.

[4] Liang G, Weller SR, Zhao J, Luo F, Dong ZY. A framework for cyber-topology attacks: Line-switching and new attack scenarios. IEEE Trans Smart Grid. 2017;10(2):1704-12.

[5] Chattopadhyay A, Mitra U. Security against false data-injection attack in cyber-physical systems. IEEE Trans Control Netw Syst. 2019;7(2):1015-27.

[6] Dong S, Sarem M. DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks. IEEE Access. 2019;8:5039-48.

[7] Abou El Houda Z, Khoukhi L, Hafid AS. Bringing intelligence to software defined networks: Mitigating DDoS attacks. IEEE Trans Netw Serv Manag. 2020;17(4):2523-35.

[8] Doshi K, Yilmaz Y, Uludag S. Timely detection and mitigation of stealthy DDoS attacks via IoT networks. IEEE Trans Dependable Secure Comput. 2021;18(5):2164-76.

[9] Doriguzzi-Corin R, Millar S, Scott-Hayward S, Martinez-del-Rincon J, Siracusa D. LUCID: A practical, lightweight deep learning solution for DDoS attack detection. IEEE Trans Netw Serv Manag. 2020;17(2):876-89.

[10] Khan IA, Pi D, Khan ZU, Hussain Y, Nawaz A. HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems. IEEE Access. 2019;7:89507-21.

[11] Mamolar AS, Pervez Z, Calero JMA, Khattak AM. Towards the transversal detection of DDoS network attacks in 5G multi-tenant overlay networks. Comput Secur. 2018;79:132-47.

[12] Sahay R, Blanc G, Zhang Z, Debar H. ArOMA: An SDN based autonomic DDoS mitigation framework. Comput Secur. 2017;70:482-99.

[13] Parida S, Panchal B. An efficient dynamic load balancing algorithm using machine learning technique in cloud environment. Int J Sci Res Sci Eng Technol. 2018;4:1184-6.

[14] Sherazi HHR, Iqbal R, Ahmad F, Khan ZA, Chaudary MH. DDoS attack detection: A key enabler for sustainable communication in internet of vehicles. Sustain Comput Inform Syst. 2019;23:13-20.

[15] Mamolar AS, Salva-Garcia P, Chirivella-Perez E, Pervez Z, Calero JMA, Wang Q. Autonomic protection of multi-tenant 5G mobile networks against UDP flooding DDoS attacks. J Netw Comput Appl. 2019;145:102416.

[16] Deka RK, Bhattacharyya DK, Kalita JK. Active learning to detect DDoS attack using ranked features. Comput Commun. 2019;145:203-22.

[17] Hosseini S, Azizi M. The hybrid technique for DDoS detection with supervised learning algorithms. Comput Netw. 2019;158:35-45.

[18] Jing X, Yan Z, Jiang X, Pedrycz W. Network traffic fusion and analysis against DDoS flooding attacks with a novel reversible sketch. Inf Fusion. 2019;51:100-13.

[19] Monge MAS, Gonzalez AH, Fernandez BL, Vidal DM, Garcia GR, Vidal JM. Traffic-flow analysis for source-side DDoS recognition on 5G environments. J Netw Comput Appl. 2019;136:114-31.

[20] Sreeram I, Vuppala VPK. HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm. Appl Comput Inform. 2019;15(1):59-66.

[21] MahdaviHezavehi S, Rahmani R. An anomaly-based framework for mitigating effects of DDoS attacks using a third party auditor in cloud computing environments. Cluster Comput. 2020;23(4):2609-27.

[22] Dasari DB, Edamadaka G, Chowdary CS, Sobhana M. Anomaly-based network intrusion detection with ensemble classifiers and meta-heuristic scale in traffic

flow streams. J Ambient Intell Humaniz Comput. 2021;12:9241-68.

[23] Cakmakci SD, Kemmerich T, Ahmed T, Baykal N. Online DDoS attack detection using Mahalanobis distance and Kernel-based learning algorithm. J Netw Comput Appl. 2020;168:102756.

[24] Bhandari A, Kumar K, Sangal AL, Behal S. An anomaly based distributed detection system for DDoS attacks in Tier-2 ISP networks. J Ambient Intell Humaniz Comput. 2021;12:1387-406.

[25] Gupta N, Jindal V, Bedi P. LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system. Comput Netw. 2021;192:108076.

[26] Kushwah GS, Ranga V. Optimized extreme learning machine for detecting DDoS attacks in cloud computing. Comput Secur. 2021;105:102260.

[27] Cil AE, Yildiz K, Buldu A. Detection of DDoS attacks with feed forward based deep neural network model. Expert Syst Appl. 2021;169:114520.

[28] doNascimento PP, Pereira P, Mialaret JM, Ferreira I, Maciel P. A methodology for selecting hardware performance counters for supporting non-intrusive diagnostic of flood DDoS attacks on web servers. Comput Secur. 2021;110:102434.

[29] Correa JH, Ciarelli PM, Ribeiro MR, Villaca RS. ML-based DDoS detection and identification using native cloud telemetry macroscopic monitoring. J Netw Syst Manag. 2021;29:1-28.

[30] Almiani M, AbuGhazleh A, Jararweh Y, Razaque A. DDoS detection in 5G-enabled IoT networks using deep Kalman backpropagation neural network. Int J Mach Learn Cybern. 2021;12:3337-49.

[31] Dora VRS, Lakshmi VN. Optimal feature selection with CNN-feature learning for DDoS attack detection using meta-heuristic-based LSTM. Int J Intell Robot Appl. 2022;6(2):323-49.

[32] Mirjalili S, Mirjalili SM, Lewis A. Grey wolf optimizer. Adv Eng Softw. 2014;69:46-61.

[33] Liu Z, He Y, Wang W, Zhang B. DDoS attack detection scheme based on entropy and PSO-BP neural network in SDN. China Commun. 2019;16(7):144-55.

[34] Chaithanya PS, Gauthama Raman MR, Nivethitha S, Seshan KS, Sriram VS. An efficient intrusion detection approach using enhanced random forest and moth-flame optimization technique. In: Computational Intelligence in Pattern Recognition: Proceedings of CIPR 2019. Singapore: Springer; 2020. p.877-84.