Hybrid chaotic bat artificial bee colony algorithm assisted hybrid machine learning based intrusion detection system

Vasanth Nayak[1, 2], Sumathi Pawar[3,*], Sunil Kumar B. L.[4]

[1]Research Scholar, Department of Computer Science and Engineering, Nitte (Deemed to be University) NMAM Institute of Technology, Nitte (DU), SH1, Karkala, Karnataka 574110, India

[2]Department of ISE, Canara Engineering College, Mangaluru, Karnataka 574219, India

[3]Associate Professor, Department of Information Science and Engineering, NMAMIT Nitte (DU), Karkala, Karnataka 574110, India

[4]Associate Professor, Department of Computer Science and Engineering, Canara Engineering College, Mangaluru, Karnataka 574219, India

Email: Vasanth.nayak@canaraengineering.in; drsumathi@nitte.edu.in; sunil.bl@canaraengineering.in

Abstract

Network intrusions are becoming more common, resulting in significant privacy violations, financial losses, and the illegal transfer of sensitive information. Numerous intrusion strategies pose a threat to data, computer resources, and networks. While hackers may focus on obtaining trade secrets, private information, or confidential data that can then be disclosed for illegal purposes, each type of intrusion aims to achieve a distinct objective. False attack detection by security systems and changing threat environments create challenges such as delayed identification of true attacks and long-term financial harm. This paper presents a novel hybrid optimization algorithm-assisted deep learning model for accurately identifying intrusion types and enhancing network security. Initially, input information is composed from openly obtainable datasets. The input data is cleaned, normalized, and standardized to produce accurate results. An improved synthetic minority oversampling technique (ISMOTE) for data balance reduces the method's overfitting problem. Then, the Chaotic Bat Artificial Bee Colony optimization algorithm (CBABCOA) is used to identify critical features and reduce feature dimensionality issues. HSVM-XGBoost (Hybrid Kernel Support Vector Machine-Extreme Gradient Boosting) is used for intrusion detection and classification. The Chaotic Binary Horse Optimization Algorithm (CBHOA) is used for hyper parameter tuning. This method makes use of the CIC UNSW-NB15 Augmented dataset, the CICIDS 2019 data set, and the NSL-KDD information set. The proposed method achieves better than the other method.

Keywords: Intrusion; DL; Hybrid optimization; Efficient; Dynamic; Cyber threats; Network security

1. Introduction

The proliferation of smart devices, driven by advances in communication technology and mobile device hardware, has significantly improved the intelligence and convenience of everyday life. Furthermore, technological advancement has resulted in advancements in a variety of industries, including healthcare, transportation, and industry [1]. However, the widespread use of these technologies has also raised concerns about network security. Data security and protecting digital life have become major concerns due to the increased vulnerability to cyber threats. Network safety relies severely on IDS. An IDS continuously analyses network traffic for unusual activities, alerting administrators or performing countermeasures when potential intrusions are identified [2-3].

Compared to traditional firewalls, IDSs can detect signs of various attacks earlier and provide proactive protection against cyber threats. IDSs assist in protecting important assets by maintaining the obtainability, concealment, and veracity of hosts and systems [4]. The two chief kinds of network intrusion discovery algorithms are anomaly and misuse recognition. By comparing unusual action to a predetermined model of typical behaviour, which is often based on well-known assault patterns, misuse detection identifies abnormal activity. The goal of this strategy is to maximize

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

true positives and reduce false positives. Therefore, anomaly detection sets a baseline for typical network traffic and warns of any changes as possible intrusions. Although this method can detect known and unknown threats, it may generate false alarms [5-6].

Researchers have examined the potential benefits of using ML and DL approaches to address the difficulties in creating trustworthy IDSs [7-8]. In many cases, ML approaches can yield more reliable and representative features than manual ones, resulting in better performance. In intrusion detection, DL-based methods have become more and more common. These include RNN, GRU (gated recurrent units), LSTM, CNN, and hybrid models [9-10]. However, the enormous dimensionality of the datasets necessary to train these models is a substantial challenge, potentially increasing training time and decreasing classification accuracy due to redundant information.

1.1 Motivation

Several current models related to IDS are examined. Despite their superior performance, the existing models are limited in their ability to detect infiltration. The drawbacks of current models include data imbalance, difficulty in detecting newly revealed attacks, parameter issues, and longer detection times when dealing with highly dynamic and developing cyber threats. These issues are caused by the suggested model's suppression of the constraints. As a result, this study introduces an efficient, unique hybrid optimization algorithm-assisted DL model for detecting intrusion classes and increasing network security.

- To pre-process the input data by employing data cleaning, normalization, and standardization for producing accurate results.
- To present an improved synthetic minority oversampling technique (ISMOTE) for data balance reduces overfitting.
- To introduce a chaotic bat Artificial Bee Colony optimization algorithm (CBABCOA) for selecting essential features and reducing feature dimensionality issues.
- To perform feature extraction using NMF (non-negative matrix factorization) to excerpt applicable topographies.
- To propose a Hybrid Kernel Support Vector Machine- Extreme Gradient Boosting (HSVM-XGBoost) for intrusion detection and classification.
- To use the Chaotic Binary Horse Optimization Algorithm (CBHOA) for hyper parameter tuning.

This paper is divided into five different sections. Various related works on the different techniques are defined in Section 2. The suggested approach overview is in Section 3. The outcome and conversation are labelled in Section 4, and the overall conclusion, upcoming work and references are in Section 5.

2. Related Work

The authors offered a new GJOADL-IDSNS. The GJOADL-IDSNS method's objective is to efficiently recognize and categorize various types of intrusions to accomplish system safety. The input information is initially normalized utilizing the data normalization method [11-13]. GJOA is used to identify the best feature subset based on relevant features. For categorization, the attention-based bi-directional LSTM (A-BiLSTM) model is used in the GJOADL-IDSNS approach. The GJOADL-IDSNS method uses the SSA to tune the hyper parameters of the A-BiLSTM model. Using the CICIDS-2017 dataset, the GJOADL-IDSNS method is evaluated and compared to cutting-edge techniques. The stationary nature of some feature assortment methods may make it challenging to deal with extremely changing and developing cyber threats [14-16].

Researchers created an enhanced Artificial Intelligence approach for effectively identifying and classifying intrusions. Data pre-processing begins with standardization and normalization to increase input quality [17-18]. Then, key features are efficiently selected using Corporate Hierarchy Optimization (CHO). Finally, GEO-SMPIF detects and categorizes optimization-based Golden Eagle Network intrusions. Here, a backpropagation technique is used to tune the precondition parameters, and golden eagle optimization (GEO) is rummage sale to enhance the replica's limitations [19-20]. The UNSW-NB15 and NSL-KDD information sets are utilized to evaluate the system's performance. However, the suggested approach did not balance the input data, which resulted in an overfitting issue [21].

The authors created an efficient intrusion detection system known as the SMSOA-based Deep Q network. The presented system has three stages: detection, feature fusion, and pre-processing. Missing value imputation is used for pre-processing, deep belief networks (DBNs) for feature combination, deep Q networks for ID, and the SMSOA technique for training [22-23]. However, dealing with data imbalance becomes more difficult when utilizing the NSL-KDD dataset to evaluate performance.

The authors offer autonomous IDS that uses ML techniques to efficiently classify intrusions. To eliminate extraneous parameters and missing values, the pre-processing technique uses Min-Max standardization and null charge handling. The ASmoT solves the data imbalance problem by minimizing overfitting concerns and balancing the class. M-SvD (Modified Singular Value Decomposition) was utilized to extract critical attributes during the feature extraction stage [24]. ONgO Algorithm Resistance-based Northern Gaussian optimization is used to select the best features. Finally, an

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

M-MultiSVM is described, which is a soil mesh-assisted multi-layer support vector machine used to classify infiltration data. Here, Mud Ring is utilized to improve the model's limitations. The system's performance is assessed utilizing the UNSW-NB15 and CSE-CIC-IDS 2018 information sets. However, neither before nor after the classification stage were attention processes utilized in this research. In any network situation, the attention mechanism aids detection by concentrating the pertinent portions of the information [25-26].

Th researchers presented DL-based IDS utilizing a chaotic optimization strategy. Data purification as well as M-squared normalization are the first pre-processing steps used to generate accurate results. The Extended Synthetic sampling technique is used to balance the input data. After balancing, kernel-assisted principal component, analysis is performed to extract features, and the Chaotic Honey Badger optimization method is utilized in the feature selection stage to select the optimal feature set. Finally, the Gated Attention Dual LSTM (Dugat-LSTM) model is introduced to categorize various forms of intrusions [27-28]. The TON-IOT and NSL-KDD information sets are utilized to evaluate the system's performance. The Dugat-LSTM model is utilized to achieve the accuracy of the NSL-KDD information set. The method may make it more difficult to detect lately identified assaults via multiple processes.

To recognize potential intimidations in networks, presented a Hybrid DL-Based Network IDS (HDLNIDS). An HDLNIDS collects local features utilizing a CNN and extracts features by means of a deep-layer RNN [29]. This makes the IDS more efficient as well as predictable. The effectiveness of the suggested method is tested with publicly accessible benchmark data from CICIDS-2018. The study's results show that the optional HDLNIDS outdoes the existing intrusion detection methods in relations of detecting malicious attempts [30]. The absence of parameter tuning leads to producing lower performance results. Analysis of prevailing studies is given in Table 1.

Table 1: Analysis of prevailing studies

Author Name Reference	Technique used	Dataset used	Aim	Advantage	Disadvantage
Aljehane et al. (2024)	GJOADL-IDSNS	CICIDS-2017	To effectually identify and classify intrusion types for achieving security of the network	Performs better than alternative models.	It may encounter difficulties managing extremely dynamic and changing cyber threats since certain feature selection techniques are static.
Siva Shankar et al. (2024)	GEO-SMPIF, CHO	NSL-KDD and UNSW-NB15	To improve the presentation and reduce errors in IDS	The model with the best hyper parameter values and the highest degree of detection performance was identified.	The absence of data balancing leads to producing an overfitting issue
Emil Selvan et al. (2024)	SMSOA-based Deep Q network	NSL-KDD	To introduce effective IDS	The goal of attack mitigation is to reduce the quantity of data lost due to attack events.	data imbalanced problems
Turukmane et al. (2024)	ASmoT, M-SvD, ONgO, M-MultiSVM	CSE-CIC-IDS 2018 and UNSW-NB15	To secure the necessary processing capacity and analyse the attacks, automatic abnormality detection systems are needed.	Optimization techniques and a mixture of ML schemes with oversampling approaches produce accurate findings.	Attention processes have not been used in this research before or after the classification stage. In any network setting, the attention mechanism improves detection by helping to concentrate the pertinent portions of the information.
Devendiran et al. (2024)	Dugat-LSTM	TON-IOT and NSL-KDD	To identify network intrusions sufficiently early	Because of the numerous technique developments, the model produces good validation results.	The method might make it more difficult to identify recently identified attacks in numerous processes.
Qazi et al. (2023)	HDLNIDS	CICIDS-2018 data	RNNs and CNNs are used in a deep-layered architecture to identify and categorize harmful data.	Uses a multi-categorization technique to accurately identify and classify all assault types.	The absence of parameter tuning leads to producing lower performance results.

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

2.1 Problem Statement

The static nature of certain feature selection techniques may make it difficult to handle extremely dynamic and changing cyber threats. The static nature of certain feature selection techniques may make it difficult to manage extremely dynamic and changing cyber threats. No attention strategies have been used in this research before or after the classification stage. The method may make it more difficult to identify recently identified attacks in numerous processes. The absence of parameter tuning leads to producing less performance results. Strong IDS are required to handle these problems to protect vital computing capabilities and efficiently assess attacks.

3. Proposed Methodology

Intrusions into networks are becoming more common, resulting in serious privacy violations, financial losses, and the unauthorized transfer of sensitive data. Numerous intrusion strategies pose a threat to data, computer resources, and networks. While hackers may focus on obtaining trade secrets, private information, or confidential data that can then be disclosed for illegal purposes, each type of intrusion aims to achieve a distinct objective. False attack detection by security systems and changing threat environments create challenges such as delayed identification of true attacks and long-term financial harm. To address these issues, robust IDS are necessary to safeguard critical calculating capabilities and effectively analyze attacks. This research proposes a novel hybrid optimization algorithm-assisted deep learning model for accurately detecting intrusion classes and enhancing network security. Initially, input information is collected from openly obtainable information sets. Pre-processing methods like information cleaning, standardization, and standardization are employed to make input data suitable for further analysis. Pre-processed data is subjected to an ISMOTE to balance the data and reduce overfitting. After that, a hybrid optimization algorithm called CBABCOA, which combines the chaotic bat optimization algorithm (CBOA) and the Artificial Bee Colony optimization algorithm (ABCOA), is used to find optimal features. After feature selection, Non-Negative Matrix Factorization (NMF) is used to remove latent features for attack classification. HSVM-XGBoost is introduced for intrusion detection and organization. Finally, the parameter of the model is optimized utilizing the CBHOA to increase performance. Figure 1 elucidates the outline of the anticipated technique.

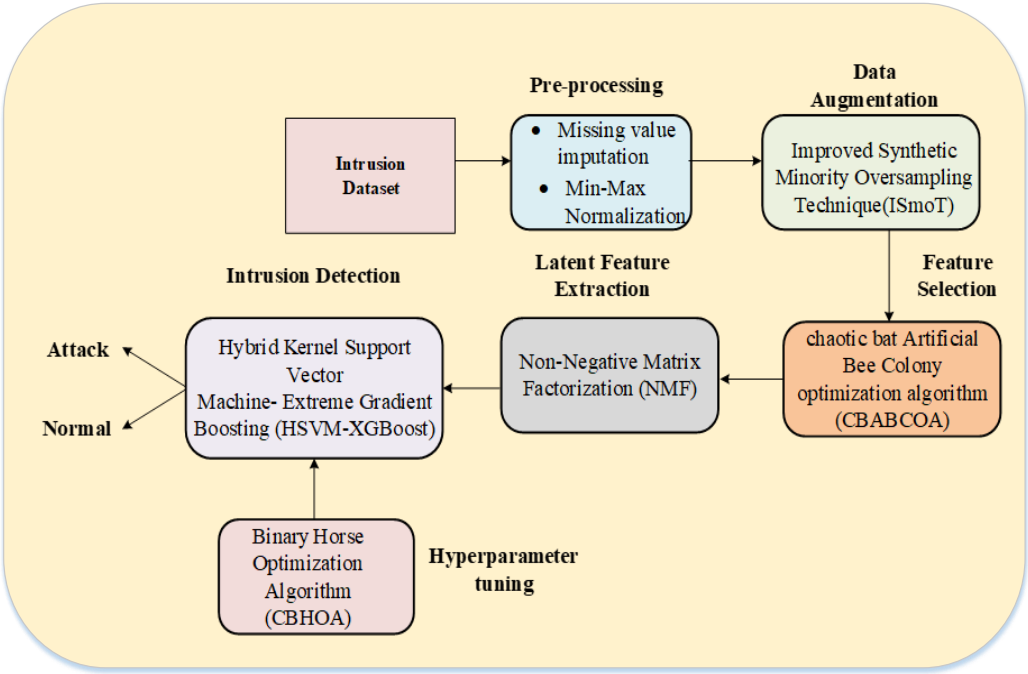

Figure 1. Overview of complete work

3.1 Pre-Processing

To produce accurate results, input data should be pre-processed using data cleaning, normalization, and standardization.

3.1.1 Missing Value Imputation

Imputation (Alkabbani, et al. 2022) of missing data is carried out sequentially, with no entries in any variable. Missing items are used to compute the variable. When the model is being trained, RF is regarded as the target variable. This target variable is predicted by other variables. The RF model is trained using all of the target variable's non-missing inputs, while the trained mode is utilized to replace any missing values.

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

3.1.2 Min-Max Normalization

$$R_{MM}(\lambda)=\frac{R_{tot}(\lambda)-\min(R_{tot}(\lambda))}{\max(R_{tot}(\lambda))-\min(R_{tot}(\lambda))} \quad (1)$$

The algorithm (Witteveen, et al. 2022) scales and offsets each individual recorded reflectance spectrum $R_{tot}(\lambda)$ using its minimum and maximum values.

3.2 Improved Synthetic Minority Oversampling Technique (ISMOTE)

ISMOTE an efficient oversampling technique produces an increase in low-frequency samples that are closely related to low-frequency samples with accidental and linear exclamation. The benefit of the SMOTE procedure creates new samples during the oversampling process rather than duplicating the same samples. Original models that do not make mistakes over time simplify the classifier's sampling and classification processes. However, the SMOTE algorithm is not the only one that wastes computer resources by increasing the number of low-frequency samples while disregarding difficulties such as spatial distribution dispersion and external processing of low-frequency sampling. In this research, a novel local adaptive SMOTE algorithm (ISMOTE)-based adaptive intrusion detection technique is developed. For respectively low-frequency sample (LFS), x chose the situation k nearest neighbours and count the quantity of great frequencies k nearest neighbour models, it is indicated by k_h Then, allowing to the size of k_h assign each LFS to different regions. Different regions have varying degrees of difficulty in classifying LFS. Therefore, different regions use different systems for the LFS process. The following three phases comprise the ISMOTE algorithm.

Step 1: (Regional division).

(a) If $k_h=k$ specifies no compatible models in the adjacent neighbouring countries, such as a low-frequency call of a low-frequency model. Models are outliers hence they are assigned independent points or the IPR (independent point region).

(b) If $(k/2\le k_h<k)$, the amount of great t values suggests that there are higher FS in the nearest neighbours than there are samples overall quantity of samples with low frequencies. In these situations, it is referred to as low frequency and assigns the models' dangerous points to the DPR (danger point domain).

(c) If $(0\le k_h<k/2)$, this directs that the area has more low-frequency samples than high FS. In this instance, models maintain the ideas and split them into a security point domain (SPR) when the frequency is low.

Step 2: (sample generation).

(a) When contrasted to industries with intellectual property, like image processing, the infiltration should not be dismissed as low-frequency sample noise detection. Thus, like the SMOTE algorithm, the example is produced by combining the LFS with the high-frequency samples of the closest neighbours.

$$x_{new}=x+u_{[0,1]}(x_h-x) \quad (2)$$

Where X_{new} newly developed low–frequency model and High-frequency sampling are in IPR, and $u_{[0,1]} \in[0,1]$ is an arbitrary quantity.

(b) Combining high-frequency examples with DPR's LF models results in a high spatial distribution of the LFS set. As a result, a weighted average of every LFS in the class's DPR center is chosen. To reduce the spatial extent circulation of the newly created set of samples, new samples are introduced among the existing ones and the center point to make LFS easier to spot.

$$x_m=\frac{1}{k-k_h}\sum_{i=1}^{k-k_h}x_i \quad (3)$$

$$x_{new}=x+u_{[0,1]}(x_m-x) \quad (4)$$

Here X_m is the unkind of all low-frequency examples in DPR.

Step 3: Remember to include a timestamp for new models derived from IDM. Despite the ISMOTE method's capacity to produce new samples from existing ones, there is no realistic temporal relationship between the two. The article discusses the characteristics of classification, which include the temporal link between network traffic. Therefore, a timestamp must be added to the new collection models.

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

When it comes to creating new samples, the new IPR and DPR models are directly proportional to the original low-frequency models. This indicates that the new models have a stronger temporal relationship and are more closely related to the original low-frequency models in terms of categorization. Thus, if low-frequency samples are input, new ones are generated according to the patterns they generate. Specifically, several new models are successively entered into the IPR generation process while being integrated into the same original samples.

3.3 Chaotic bat optimization algorithm and Artificial Bee Colony optimization algorithm CBA-ABCO

The proposed HCBA-ABCO, which improves search efficiency by replacing solutions with low fitness diversity, should be implemented in the population. BA-ABC algorithm is developed by combining BAT and ABC instruction. Meta-heuristic algorithms inspire the former by nature. It is also inspired by the echolocation behaviour of bats, which use it to detect distance. Bats use short bursts of loud sound to hunt at night and listen for the echo coming back from prey or obstacles. Bats' receiving system allows them to sense the size and position of objects. The BA algorithm has seen extensive use in a diversity of requests, with decoration gratitude and engineering optimization.

On the other hand, the ABC algorithm is based on swarm intelligence and was inspired by honeybee behaviour. The algorithm solution generates an initial population of N (referred to as food resources), randomly distributed, and specifies the swarm size with N. Let X_i be the i_{th} solution and n be the size of the dimension. Every worker bee X_i produce a new possible solution X^* in its current neighbor as follows:

$$v_{j,k} = \phi_{j,k}\left(X_{j,k} - X_{j,i}\right) + X_{j,k} \quad (5)$$

Here X_k is a random possible solution $(i \neq k), k$ depicts a randomly chosen measurement index from the set 1, 2… n, and ϕ has a range of $[-1,1]$. The greedy selection method is used as the new possible solution vi is generated. If vi is fitness-wise superior to its parents X_i, then vi replace X_i; otherwise, there is no change. After the procedure is complete for all worker bees, they perform a dance to communicate food source information to onlooker bees. Honey data collected from all worker bees is evaluated using the amount of honey in each observer bee to select a food source. This selection process takes a probabilistic approach, like roulette wheel selection. The process is detailed as follows:

$$pi = \frac{fit_i}{\sum_{j=1}^{N} fit_i} \quad (6)$$

Where fit_i represents the fitness of the i_{th} swarm solution.

If the maximum iteration number cannot be improved, the food resource is abandoned and discarded. If the rejected source is denoted as X_i, then the scout bee looks for a new basis of food to update X_i using the following process:

$$X_{i,j} = \delta_l^j + r(\delta_u^j - \delta_l^j) \quad (7)$$

Where r is a number arbitrarily created using a normal distribution in the series [0, 1]

Generally, the BA algorithm excels in the search space; however, exploitation becomes a local fascination optimum, which inhibits its ability to conduct effective global searches. Since the BA algorithm relies only on randomness walks, quick integration is not guaranteed. Introducing a major optimization of the programming algorithm to increase the heterogeneity of the risk of trapping at local optima. The step involves integrating the mutation operator from ABC, which accelerates integration. Thus, the difference between BA-ABC and BA algorithms lies in the mutation operator, which generates a new solution for each bat. As a result, the problems of local optima in the BA algorithm are removed, allowing for the exploration of new search locations via the process of mutation of ABC during population optimization.

In the BA-ABC, all stages require additional processes to initialize the population and share information during the meeting. Initially, key parameters such as population size (N), solution space dimension (n), and the maximum number of repetitions are established as the decision criterion. Subsequently, other parameters like $f_i, v_i, A_i, and\ r_i$ are computed. The phase's population initiation, BA phase and ABC grid. Confusion mapping is frequently used in sequences to generate the initial probability in the early stages of the population. The goal is to optimize solutions from a wider search space eligibility of the initial population. The strategy for population loading is described in procedure 1.

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

The original population is produced utilizing the X logistic fuzzy mapping within the search space. The logistics regression function is used here:

$$x(p+1)= x(p)*(p-1)*4 \quad (8)$$

Where p is the iteration number, and the initial value is x (0), selected at random.

After generating the initial population, the algorithm minimizes the standard BA process, optimizes its parameters, and calculates the current position of search agents using steps 9, 10, and 12, as shown in the algorithm and equation (5-7). Algorithm 1 describes the suggested CBA-ABCO algorithm.

Algorithm 1 CBA-ABCO algorithm

1. **Input:** $N, n, f_{\min,} f_{\max}, [\delta_u, ..., \delta_l], it_{\max}, v_i, A_i, r_i, X_{ij}$ **and random number** $(a, b, r_1, r_2, \beta, \phi)$

   N is the number of tasks,

   n is the amount of virtual machines

   $f_{\min,} f_{\max}$ is minimum and maximum load values

   $[\delta_u, ..., \delta_l], it_{\max}, v_i, A_i, r_i, X_{ij}$ these are the parameters of the bat algorithm

   $(a, b, r_1, r_2, \beta, \phi)$ these are random numbers

2. **Output:** X_b
3. **initialization**
4. - Generate initial bat population X_i using chaotic mapping:
5. $X(k+1)=\mathrm{mod}\left(b+X(k)+-\frac{a}{2\Pi}\sin(2\Pi X(k)),1\right)$
6. Evaluate fitness and select current best $X*$
7. **while** $it < it_{\max}$ *do*
8. **Adjust frequency and update velocities:**
9. $f_i = (f_{\max} - f_{\min}) \times \beta + f_{\min}$
10. $V_i^{t+1} = v_i^t + (X_i^t - X*) \times f_i$

    f_i is frequency, V_i is velocity
11. **update position/ solution:**
12. $X_i^{t+1} = X_i^t + v_i^{t+1}$

    Each bat position X_i is updated based on its speed
13. **if** $r_1 > r_i$ *then*
14. – Move agents using updated $f_i, v_i,$ *and* x_i

    The bat moves to the new position updated using frequency, velocity, and position
15. **end if**
16. **Evaluate fitness:**
17. **accept or reject** X_i^{t+1}
18. **if** $r_2 < A_i$ & $f(X_i) \le f(X*)$ *then*
19. $-\uparrow r_i$ *and* $\downarrow A_i$
20. **end if**
21. **Evaluate fitness:**
22. select current best $X*$
23. **Calculate** r **using logistic chaotic mapping:**
24. $X(j+1)=a\times X(j)\times(X(j)-1)$, *while* $X(0)=X*$
25. **Select** X_{ij} **using r**
26. **Mutate search agents:**

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

27. $V_{ij} = X_{ij} + \phi \times (X_{ij} - X_{kj})$
28. **Apply greedy selection**
29. **find new solution, evaluate fitness & select** $X*$
30. **end while**
31. **Return the best solution** $X_{gb} = X*$

This strategy improves exploitation possibilities by allowing for the selection of standards for sustainable environmental solutions and information exchange.

$$X_u = X_o + \in A^t \quad (9)$$

Here X_u is the new state, and X_o is the previous state, $\in$ is a randomly generated number in the series $[-1,1]$, and A^t denotes the bats regular volume at the time t.

If $f(X_i) < f(X*)$ and the randomly generated number $r_2 < A_i$ then consider the new solution valid. Further update A_i and r_i as below:

$$A_i^{t+1} = \alpha \times A_i^t \quad (10)$$

$$r_i^t = r_i^0 \left[1 - e^{-\gamma t}\right] \quad (11)$$

Here A_i^{t+1} and A_i^t are loudness at times $t+1$ and t, respectively; r_i^0 and r_i^t are the pulse rates initially and at time t. As $t \to \infty$, $A_i^t \to 0$ and $r_i^t \to r_i^0$.

The entire exploration and exploitation process, including the BA and ABC phases, is repeated a limited number of times. $it_{\max}$, resulting in the optimal solution. The global search capability is improved by the ABC search equation and the BA search equation (1). Each member has the chance to share information with the audience. It encourages the maintenance of necessary inspection and avoids the problem of exploitation, mitigation and diversification advance integration. Also, it offers a high volume of opportunities to escape and find the global optimum solution. CBA-ABCO is shown in Figure 2.

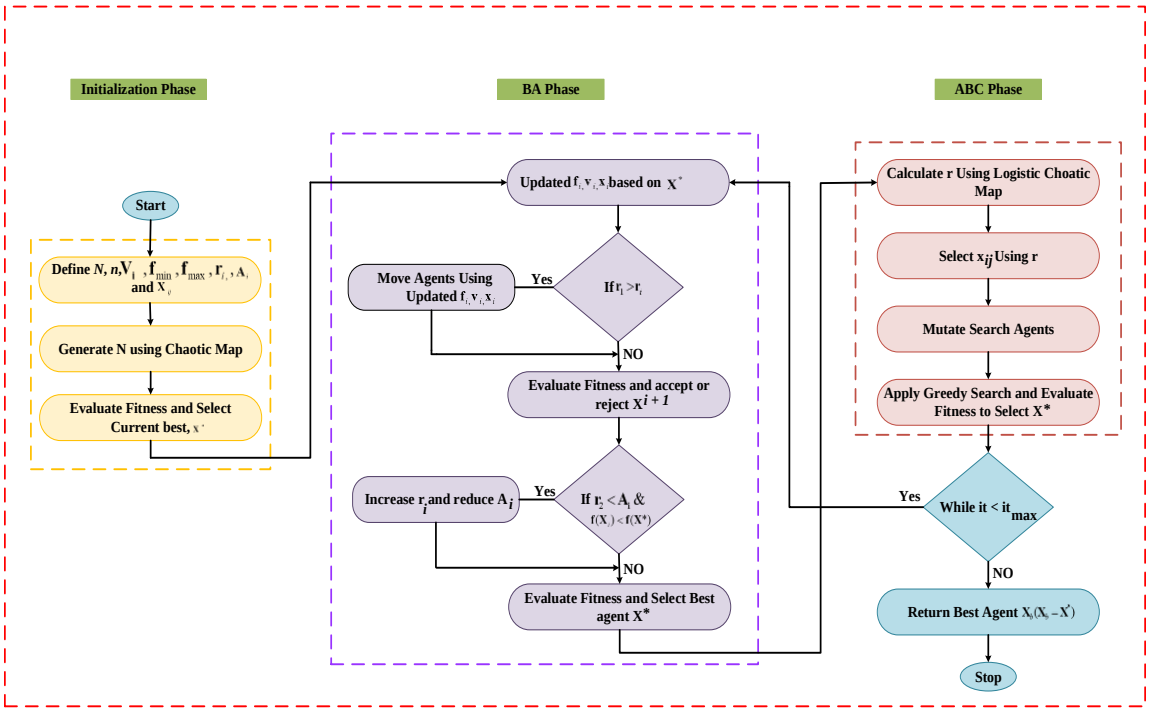

Figure 2. CBA-ABCO

3.4 Non-Negative Matrix Factorization

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

NMF is a matrix analysis technique that will explain each matrix in the following manner.

$$X_{pxq} = W_{pxr} * H_{rxq} \quad (12)$$

NMF is disintegrated into certain data (X) in two matrices $(H \text{ and } W)$ that hold the innovative data in a single artefact of brace media.

3.5 Hybrid Kernel SVM:

SVM is founded on the philosophy of convergent optimization. The primary weight space contains a non-linear SVM classifier, which is described as:

$$y(x) = sign\left[w^T \varphi(x) + b\right] \quad (13)$$

Here $w \in \Re^n, b \in \Re, \varphi(x)$ is the map purpose, which charts χ into a developed dimensional feature interplanetary, the number of dimensions can be unlimited.

Deliberate a usual set of exercise vectors $x_i \in \Re^n \ (i = 1, \ldots, N)$, in two courses and the gauge (feature) course $y_i \in \{-1, 1\}$. Here is the formula for the basic SVM used in classification.

$$\min_{w,b,\xi} \frac{1}{2} w^t \ w + c \ \sum_{K=1}^{N} \xi_k \quad (14)$$

$$s.t \quad yk\left(w^T \varphi(x_k) + b\right) \geq 1 - \xi_k \qquad \xi_k \geq 0, k = 1, \ldots . N, \quad (15)$$

Here ξ_k slack variable is C a confident actual tradeoff is less.

$$\max_{\alpha} -\frac{1}{2} \sum_{k,l=1}^{N} ykyl K\left(x_k, xl\right) \alpha_k \ \alpha_l + \sum_{k=1}^{N} \alpha_k \quad (16)$$

$$s.t \quad \sum_{k=1}^{N} y_k \ \alpha_k = 0, \ \alpha_k \in [0, c], k = 1, \ldots N \quad (17)$$

Here α_k are Lagrange multipliers, and $K(x_k, x_l)$ is the kernel purpose as

$$k\left(x_k, x_l\right) = \varphi\left(x_k\right)^T \varphi\left(x_l\right) \quad (18)$$

After the resolution of the dual problem, the vector w can be expressed as

$$w = \sum y_k \ \alpha_k \ \varphi(x_k) \quad (19)$$

By utilizing primitive double relations. Thus, an equation can be expressed as

$$y(x) = sign\left(w^T \varphi(x) + b\right) = sign\left(\sum_{k=1}^{N} y_k \ \alpha_k \ K(x_k, x) + b\right) \quad (20)$$

Characterization of kernels: The inner product $\phi(x)$ vapnik's introduction to kernel function in 1995 explains how graph function mapping. $K(x_k, x_l)$ converted the linear SVM to a non-linear approach. This is because the result that follows evaluates the map function's internal produces in Hilbert space. The symmetric condition of Hilbert space theory states that there is an extension.

$$K(x, z) = \sum_{K=1}^{\infty} \lambda_k \ \varphi_k(x) \varphi_k(z) \quad (21)$$

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

Here $x, z \in \Re^N$, and $\lambda_k > 0$

Mercer's state dictates that

$$\int k(x,z)g(x)g(z)dxdz \geq 0 \qquad (22)$$

Here $g(\cdot)$ is any square-integrable function

It is noted that the integral is taken over a compact subset of $\Re^N$ and that the kernel function can be represented as an inner product. Additionally, the following claim is equivalent to

First proposition: $K(x,z)$ is a grain purpose if and only if the atmosphere is finite, and x is a finite input space.

$$K(x_k, x_l) = [K(x_k, x_l)]_{k,l=1}^{N} \qquad (23)$$

3.6 Binary Horse Optimization Algorithm

In the extremely uncommon event that classifiers fail to perform with data samples containing only one or no features, the BHOA is fine-tuned to allow for feature selection. Every location is represented by an array of integers ranging from 0 to 1, with at least two 1s. To convert continuous numbers into binary ones, use the following function:

$$s(x) = \begin{cases} 1, & rand < \left| \dfrac{x}{\sqrt{1+x^2}} \right| \\ 0, & otherwise \end{cases}, \qquad (24)$$

Where the function $rand$ proceeds arbitrary ideals from $[0,1]$. The Flowchart of BHOA exposed in figure 3.

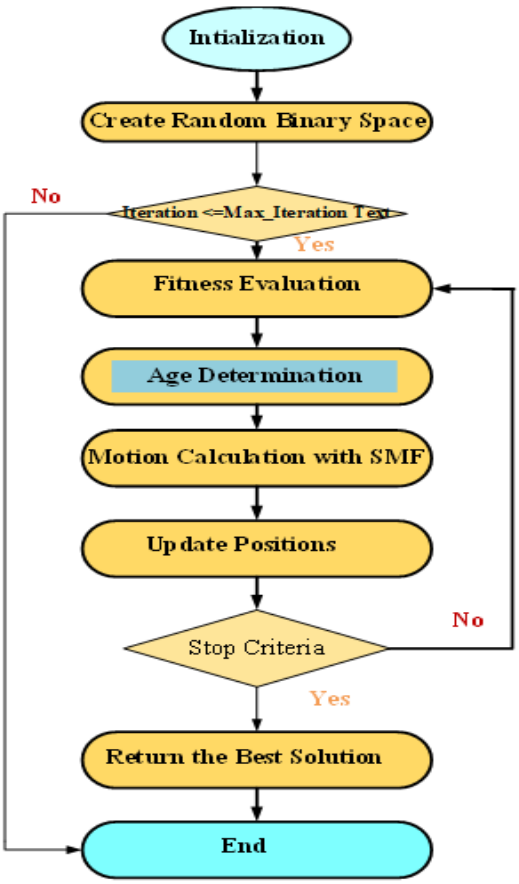

Figure 3. Flowchart of BHOA

4. Result and Discussions

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

The performance of the proposed (CBABCOA) model was assessed utilizing common assessment methods like specificity, f1-score, recall, accuracy, and precision.

4.1 Dataset Explanation

***1. CIC UNSW-NB15 dataset*:** The IXIA Perfect Storm application was used to generate a dataset of contemporary normal and abnormal network circulation. The dataset encompasses both benign traffic and nine occurrence categories. They used the Argus and Bro-IDS tools to extract features from the 100GB of network traffic they had captured over two days. They extracted 47 attributes from categories such as Basic, Content, Time, and other produced characteristics. https://www.unb.ca/cic/datasets/cic-unsw-nb15.html

2. CICIDS 2019 dataset: The CICIDS 2019 information set on Kaggle is a publicly available dataset designed specifically for the evaluation and testing of IDS in network security. It mimics actual network activity and offers a variety of benign and malevolent actions. https://www.kaggle.com/datasets/tarundhamor/cicids-2019-dataset

3. NSL-KDD datasets: In order to eliminate redundant and duplicate records, this dataset is a modernized form of the KDD Cup 1999 dataset. Consequently, there won't be any bias in the categorization models. In adding to "normal" network circulation, NSL-KDD statistics reveal four major intrusions: DoS, R2L, U2R, and probing. The NSL-KDD-Train dataset utilized in this work is 75% trained (125,973 records) and 25% validated (22,544 records). During the training phase of the validation procedure, the models were not overfitted.

https://www.kaggle.com/datasets/hassan06/nslkdd

4.2 Performance Metrics

The proposed model's performance was examined using normal evaluation metrics. These metrics are utilized to analyse the suggested method. Table 2 demonstrations the Performance metrics.

Table 2: Performance metrics

Performance	**Formula**
Accuracy	$\mathrm{Acc}=\frac{\mathrm{T.n}+T.p}{T.n+F.p+F.p+T.p}$
Precision	$precision=\frac{T.p}{T.p+F.p}$
Recall	$recall=\frac{T.p}{T.p+F.n}$
F1 score	$F1-Score=2*\frac{precision*recall}{precision+recall}$
Specificity	$Specificity=\frac{T.p}{T.n+F.p}$
RMSE	$RMSE=\sqrt{\frac{\sum_{i-1}^{n}\left(x_i-x_p\right)^2}{n}}$
MSE	$MSE=\sqrt{\frac{\sum_{i-1}^{n}\left(x_i-x_p\right)^2}{n}}$

4.3 Performance Analysis and Comparison

CIC UNSW-NB15 dataset: The performance of the CBABCOA method is compared to previous methods such as SVM, RF, XGBOOST, and NB. The CBABCOA approach uses the CIC UNSW-NB15 data set for performance analysis. The CBABCOA approach's performance is evaluated using metrics like accuracy, precision, specificity, recall, F1-Score, specificity, RMSE, and MSE. When associated to the current methodology, the CBABCOA technique is more real, as exposed in Figure 4.

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

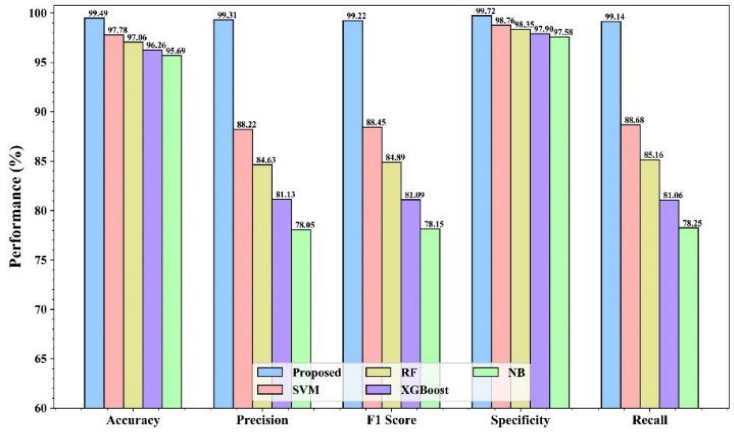

Figure 4. performance metrics of proposed and existing method

The performance of the CBABCOA technique utilizing HSVM-XGBOOST with CBHOA and HSVM-XGBOOST without CBHOA are as follows: with CBHOA, accuracy, precision, specificity, F1Score, recall are high, while without CBHOA, they are low. The error values are low in the CBABCOA technique while utilizing HSVM-XGBOOST with CBHOA and high in HSVM-XGBOOST without CBHOA

The error values are low in the CBABCOA technique while utilizing HSVM-XGBOOST with CBHOA and high in HSVM-XGBOOST without CBHOA, as exposed in Figure 5.

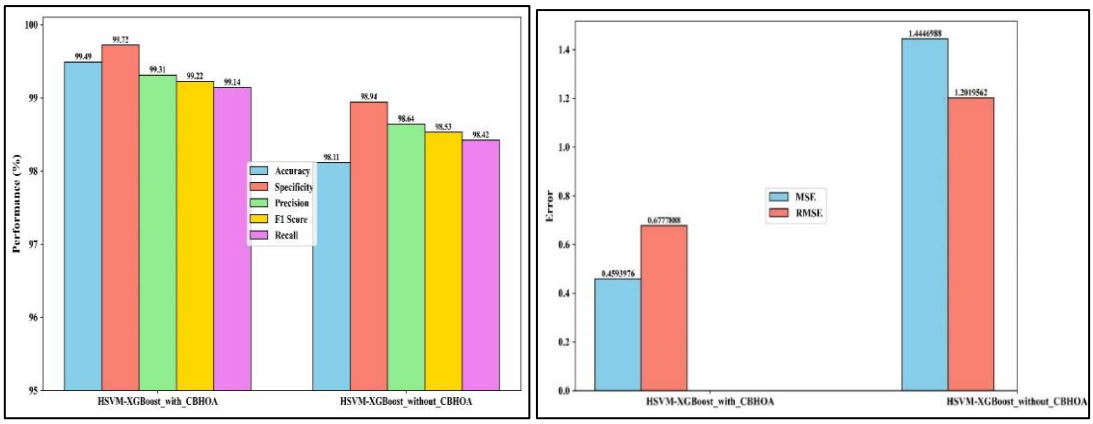

Figure 5. The performance of the projected method using HSVM-XGBOOST with CBHOA and HSVM-XGBOOST without CBHOA

The RMSE and MSE are measured and compared to existing methods such as SVM, RF, XGBOOST, and NB. The CBABCOA approach has a lower error rate than the existing method. Existing methods have strong performance metrics, which are given in Figure 6. Figure 7 demonstrations the ROC Curve.

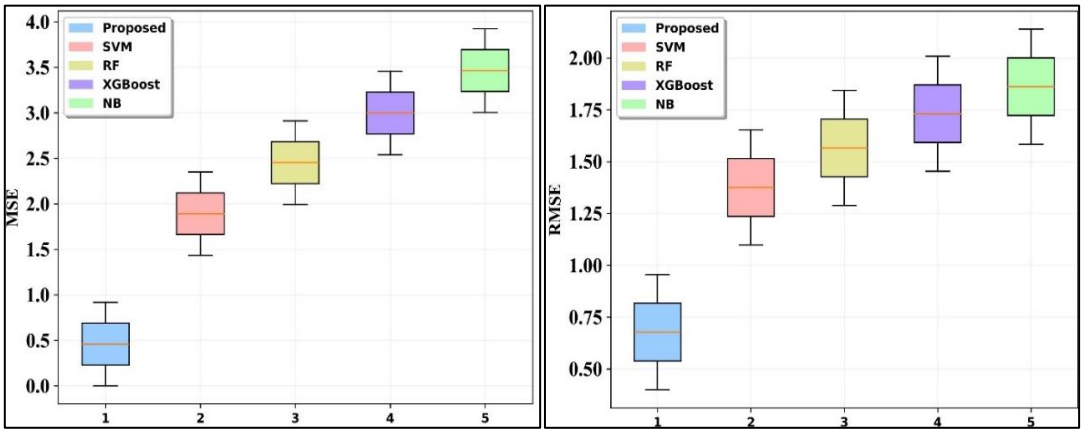

Figure 6. The error values of the proposed and existing method

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

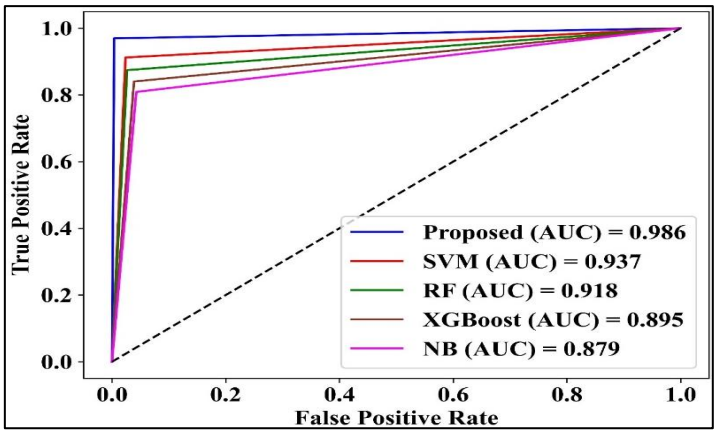

Figure 7. ROC Curve

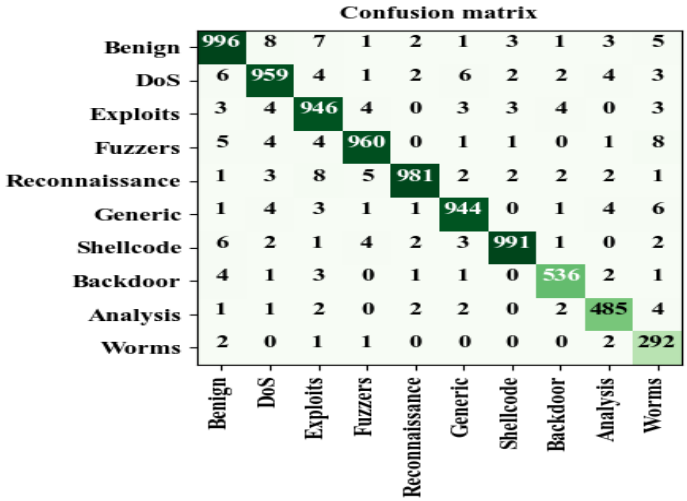

Figure 8. confusion matrix

Figure 8 shows the misperception matrix. A confusion matrix depicts the presentation of a classification perfect in detection numerous types of cyber-attack. Diagonal elements, which reflect valid classifications, typically have high values, indicating great performance in detecting assaults such as benign, DoS, and exploits. However, exploits refer to misclassifications, such as events that are misclassified as fuzzes. While the model has decent overall accuracy, more work is needed to improve its capacity to discriminate specific attack types and eliminate misclassifications. Table 3 demonstrations the comparison table for the suggested as well as current methods.

Table 3: Comparison table for proposed and existing method

Metric	Proposed	SVM	Random Forest (RF)	XGBoost	Naive Bayes (NB)	HSVM-XGBoost without CBHOA
Accuracy	**0.9949**	0.9778	0.9706	0.9626	0.9569	0.9811
Recall	**0.9914**	0.8868	0.8516	0.8106	0.7825	0.9842
Precision	**0.9931**	0.8822	0.8463	0.8113	0.7805	0.9864
F Measure	**0.9922**	0.8845	0.8489	0.8109	0.7815	0.9853
Specificity	**0.9972**	0.9876	0.9835	0.979	0.9758	0.9894
MSE	**0.4594**	1.8924	2.4539	2.9986	3.4648	1.4447
RMSE	**0.6778**	1.3756	1.5665	1.7316	1.8614	1.202

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

CICIDS 2019 dataset: The CBABCOA method's performance is compared to previous approaches such as SVM, RF, and XGBOOST, NB. The CICIDS 2019 data set was used to conduct performance analysis using the suggested approach. When compared to the current methodology, the CBABCOA method is more effective, as exposed in Figure 9.

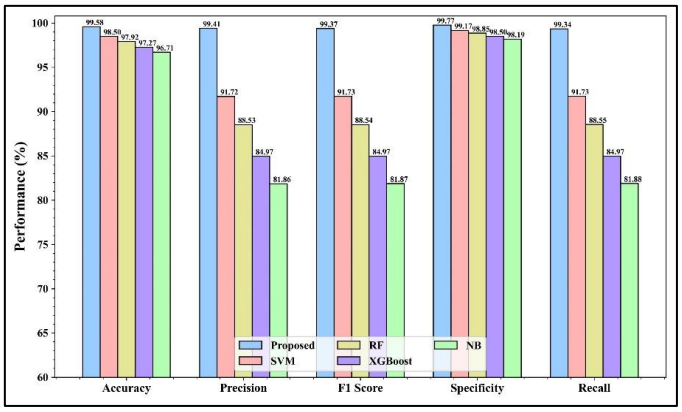

Figure 9. The performance of anticipated and existing technique

The performance of the CBABCOA technique utilizing HSVM-XGBOOST with CBHOA and HSVM-XGBOOST without CBHOA are as follows: with CBHOA, accuracy, precision, specificity, F1Score, recall are high, while without CBHOA, they are low. The error values are low in the CBABCOA technique while utilizing HSVM-XGBOOST with CBHOA and high in HSVM-XGBOOST without CBHOA, as shown in Figure 10.

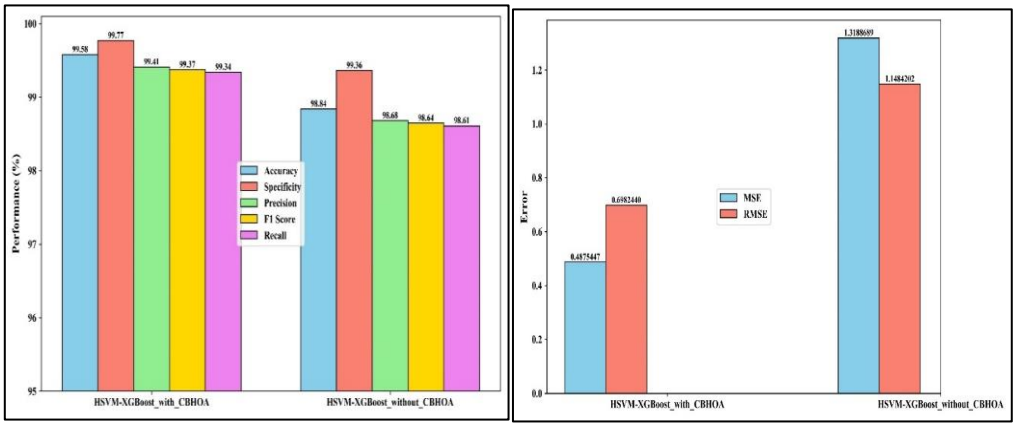

Figure 10. Error and performance metrics

The RMSE and MSE are measured and compared to existing methods such as SVM, RF, XGBOOST, and NB. The recommended technique has a lower error rate than the current method. Existing approaches have excellent performance metrics, as shown in Figure 11.

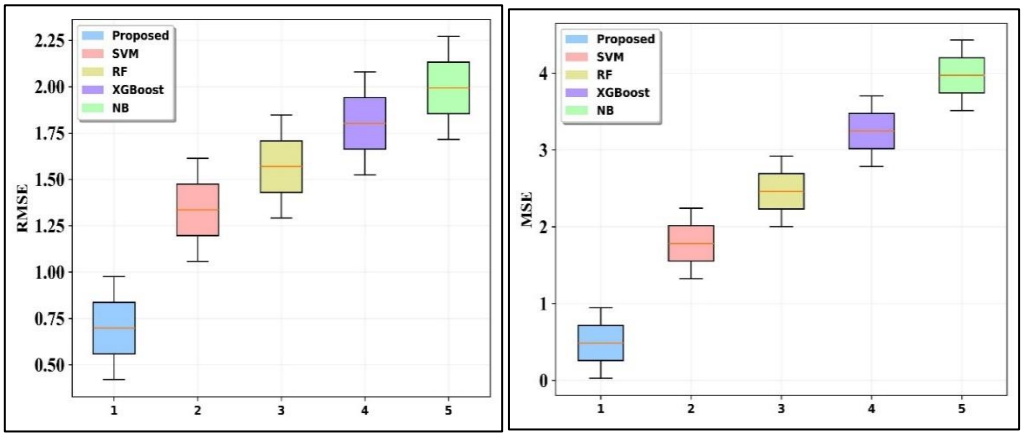

Figure 11. The error values of proposed and existing method

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

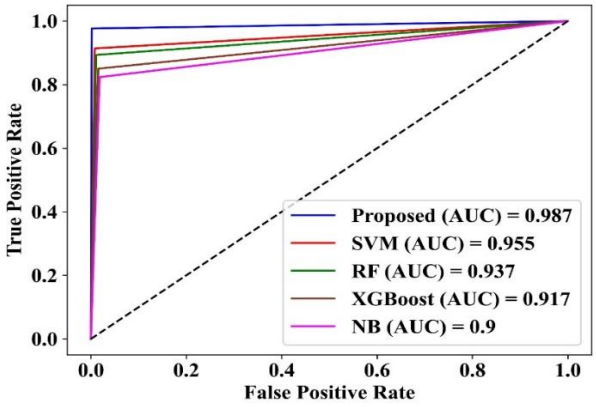

Figure 12. ROC Curve

Figure 12 shows the ROC curves, and it compares the performance of the suggested method to attain better performance than the other model.

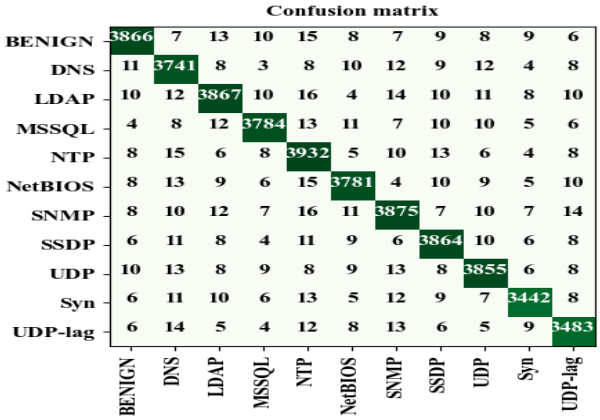

Figure 13. Confusion matrix

Figure 13 demonstrations the confusion matrix for the suggested method and the presentation of the classification model for network traffic. Diagonal elements, usually darker, indicate higher rates of correct classification for each traffic type (e.g., BENIGN, DNS, LDAP). Off-diagonal elements, generally Lighter ones, show misclassifications, which can imply that the model is more prone to errors. The model has promising performance in classifying specific traffic categories. Additional research, including the calculation of metrics like precision, accuracy, recall, and specificity for each class, is required to completely analyse its performance and find areas for improvement. The comparison of suggested and current method performances is exposed in Table 4.

Table 4: Comparison of proposed and existing method performance

Metric	Proposed	SVM	Random Forest (RF)	XGBoost	Naive Bayes (NB)	HSVM-XGBoost without CBHOA
Accuracy	**0.9958**	0.985	0.9792	0.9727	0.9671	0.9884
Recall	**0.9934**	0.9173	0.8855	0.8497	0.8188	0.9861
Precision	**0.9941**	0.9172	0.8853	0.8497	0.8186	0.9868
F Measure	**0.9937**	0.9173	0.8854	0.8497	0.8187	0.9864
Specificity	**0.9977**	0.9917	0.9885	0.985	0.9819	0.9936
MSE	**0.4875**	1.7832	2.4615	3.2458	3.9724	1.3189
RMSE	**0.6982**	1.3354	1.5689	1.8016	1.9931	1.1484

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

NSL-KDD information set: The performance of the CBABCOA technique is likened to that of previous approaches such as SVM, RF, and XGBOOST, NB. The NSL-KDD information set was utilized to analyse performance using the recommended technique. When compared to the current procedure, the CBABCOA method is more efficient. The performance of the suggested approach is shown in Figure 14.

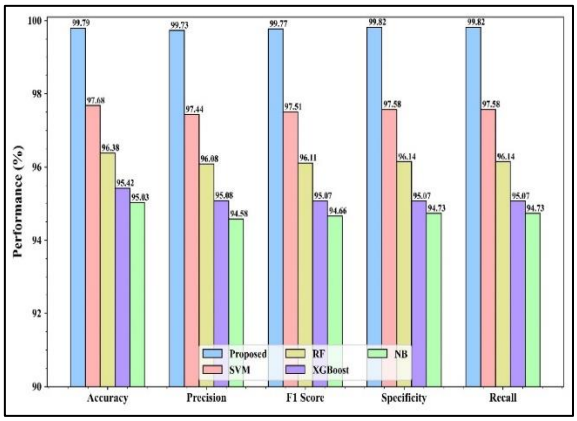

Figure 14. The performance of projected and existing method

The performance of the CBABCOA technique utilizing HSVM-XGBOOST with CBHOA and HSVM-XGBOOST without CBHOA are as follows: with CBHOA, accuracy, precision, specificity, F1Score, recall are high, while without CBHOA, they are low.

Based on an analysis of the error rate, the error values show a low error rate in the suggested method when using HSVM-XGBOOST with CBHOA and a high error rate when using HSVM-XGBOOST without CBHOA, as exposed in Figure 15.

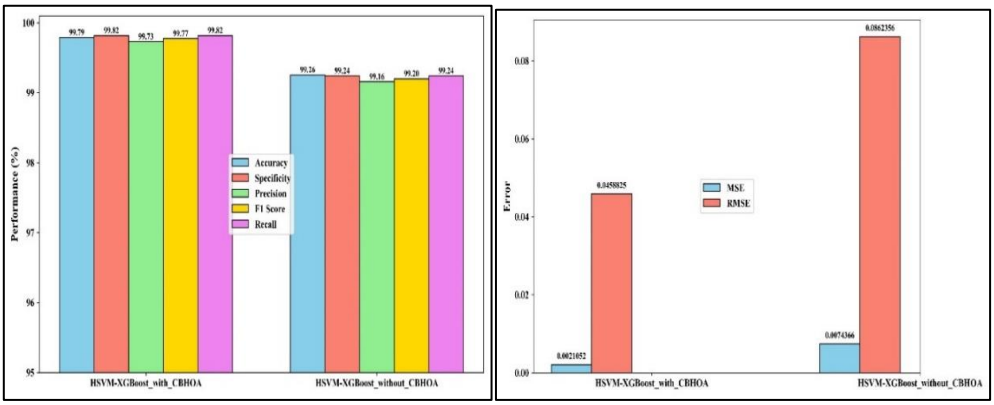

Figure 15. The performance of proposed method using HSVM-XGBOOST with CBHOA and HSVM-XGBOOST without CBHOA

The RMSE and MSE are measured and compared to existing methods such as SVM, RF, XGBOOST, and NB. The optional technique has a lower error rate than the existing method. The ROC and confusion matrix outcomes are given in Figure 16.

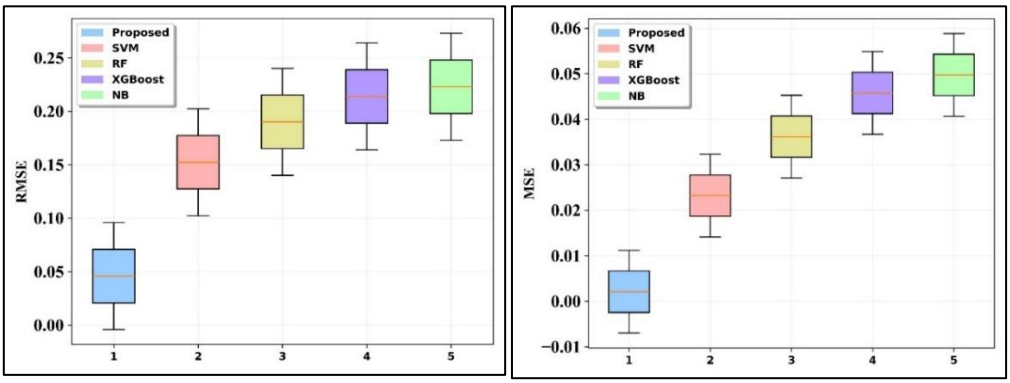

Figure 16. The error values of proposed and existing method

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

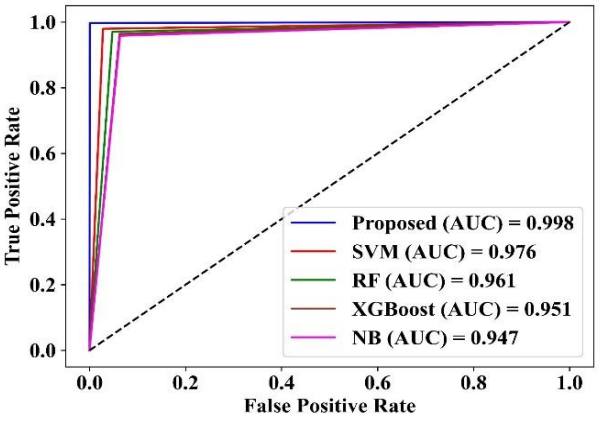

Figure 17. ROC Curve

Figure 17 shows the ROC curves, which compare the presentation of the projected technique to that of the other model.

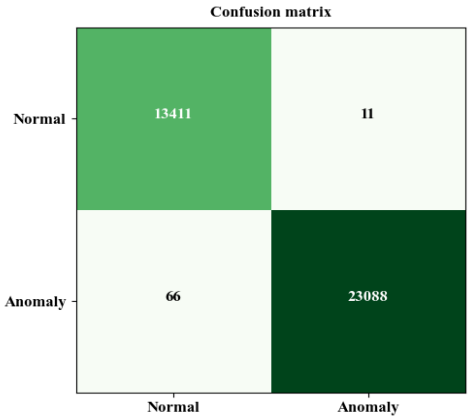

Figure 18. Confusion matrix

Figure 18 shows the confusion matrix. It correctly identifies 13411 as normal and 23088 as abnormal. A comparison of the suggested and current approaches is exposed in Table 5.

Table 5: Judgement of proposed and existing technique performance

Metric	Proposed	SVM	Random Forest (RF)	XGBoost	Naive Bayes (NB)	HSVM-XGBoost without CBHOA
Accuracy	**0.9979**	0.9768	0.9638	0.9542	0.9503	0.9926
Recall	**0.9982**	0.9758	0.9614	0.9507	0.9473	0.9924
Precision	**0.9973**	0.9744	0.9608	0.9508	0.9458	0.9916
F Measure	**0.9977**	0.9751	0.9611	0.9507	0.9466	0.992
Specificity	**0.9982**	0.9758	0.9614	0.9507	0.9473	0.9924
MSE	**0.0021**	0.0232	0.0362	0.0458	0.0497	0.0074
RMSE	**0.0459**	0.1524	0.1902	0.2139	0.223	0.0862

4.4 Discussion

This section contains an exhaustive review of the previous approach's limitations and the new method, as well as the results and proposed rationale based on several assessment and validation experiments. These studies have attained high performance, including drawbacks like in (Aljehane, et al. 2024): The method discussed in this paper struggles with handling dynamic and developing cyber threats because it uses static feature selection techniques. This can lead to poor adaptation as new threats emerge from the proposed method. The new approach adjusts to evolving threats, probably by using more dynamic feature selection methods that are updated in response to fresh information. In (Siva

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

Shankar, et al. 2024): The lack of data balancing can cause overfitting, where the model becomes too tuned to the majority class, missing important patterns in minority classes. Proposed Solution: The proposed method includes data balancing techniques to prevent overfitting and improve generalization.

In (Emil Selvan, et al. 2024): This study highlights problems with imbalanced datasets, where one class (e.g., normal traffic) dominates the data, leading to biased predictions. Proposed Solution: The proposed method addresses these imbalances, likely using techniques like resampling or synthetic data generation. In (Turukmane, & Devendiran, 2024): Previous research did not use attention mechanisms, which are critical for directing on imperative features in the input data, particularly in complex network environments. Proposed Solution: The new approach incorporates attention mechanisms before or after the classification stage to enhance detection accuracy by focusing on the most pertinent parts of the input information. In (Devendiran & Turukmane, 2024): This technique struggles with detecting innovative, previously unknown attacks because it does not dynamically adjust to new data and patterns. Proposed Solution: The proposed method may have mechanisms that allow for more actual adaptation and discovery of emerging intimidations. In (Qazi, et al. 2023): The absence of parameter tuning results in suboptimal performance, as the model's parameters are not optimized for the best possible outcomes. Proposed Solution: The new approach includes parameter tuning to improve performance and ensure the model works at its best.

5. Conclusion

The anticipated method and the previous prototypical are associated in this study. Simulation results established the efficiency of the anticipated method. The previous models were XGBOOST, RF, SVM, and NB. The presentation of the proposed model was appraised by means of commonly used system of measurement such as specificity, accuracy, precision, recall, and F1 score. MSE and RMSE findings are used to determine which strategy performs enhanced. The proposed model has a lower error rate and better presentation, whereas the current technique has a high error rate. The proposed method made use of three sets of datasets: CIC UNSW-NB15, CICIDS 2019, and NSL-KDD. When compared to the current model, the proposed method achieves high accuracy (99.49%, 99.49%, and 99.79%) as well as better performance in precision, f1 score, recall, specificity, and error rate. The future of hybrid ML models for network intrusion detection is promising, with numerous possibilities for exploration. By improving feature selection, real-time adaptability, and explain ability and incorporating modern techniques like transfer learning and behavioural analytics, the next generation of NIDS can be more accurate, scalable, and robust against ever-changing cyber threats.

Funding Data: No funding is provided for the groundwork of document.

References

[1] B. Dappuri and T. G. Venkatesh, "Design and Performance Analysis of Multichannel MAC Protocol for Cognitive WLAN," IEEE Transactions on Vehicular Technology, vol. 67, no. 6, pp. 5317-5330, June 2018, doi: 10.1109/TVT.2018.2812823.

[2] R. Kashyap, "Artificial Intelligence Systems in Aviation," in Cases on Modern Computer Systems in Aviation, T. Shmelova et al., Eds., IGI Global, 2019, pp. 1–26, doi: 10.4018/978-1-5225-7588-7.ch001.

[3] M. R. Shaik and A. S. Reddy, "Optimal placement and sizing of FACTS device to overcome contingencies in power systems," Proc. 2016 Int. Conf. Signal Process., Commun., Power, Embedded Syst. (SCOPES), Paralakhemundi, India, 2016, pp. 838-842, doi: 10.1109/SCOPES.2016.7955559.

[4] V. Roy, H. Amhia, S. Shukla, and A. K. Wadhwani, "An IoT-Based Moving Vehicle Healthcare Service," in IoT in Healthcare Systems: Applications, Benefits, Challenges, and Case Studies, 2023, pp. 177-190, doi: 10.1201/9781003145035-10.

[5] S. Tiwari, C. M. Babu, P. Shanker, K. V. Shahnaz, V. Roy, and R. Kashyap, "Cross-Lingual Transfer Learning in RNNs for Enhancing Linguistic Diversity in Natural Language Processing," in Proc. 2024 Int. Conf. Advances Comput. Res. Sci. Eng. Technol. (ACROSET), 2024, doi: 10.1109/ACROSET62108.2024.10743896.

[6] S. K. Suman et al., "Sign Language Interpreter," in Advances in Cognitive Science and Communications, Springer, ICCCE 2022, pp. 1021-1031, doi: 10.1007/978-981-19-8086-2.

[7] K. Ramu et al., "Deep Learning-Infused Hybrid Security Model for Energy Optimization and Enhanced Security in Wireless Sensor Networks," SN Comput. Sci., vol. 5, no. 848, 2024, doi: 10.1007/s42979-024-03193-6.

[8] R. Kashyap, "Big Data and High-Performance Analyses and Processes," in Spatial Planning in the Big Data Revolution, A. Voghera and L. La Riccia, Eds., IGI Global, 2019, pp. 45–83, doi: 10.4018/978-1-5225-7927-4.ch003.

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025

[9] S. R. Sankranti et al., "Effective IoT-Based Analysis of Photoplethysmography Waveforms for Investigating Arterial Stiffness and Pulse Rate Variability," SN Comput. Sci., vol. 5, no. 5, 2024, doi: 10.1007/s42979-024-02777-6.

[10] K. Ramu et al., "Augmenting Cervical Cancer Analysis with Deep Learning Classification and Topography Selection Using Artificial Bee Colony Optimization," SN Comput. Sci., vol. 5, no. 6, 2024, doi: 10.1007/s42979-024-03040-8.

[11] M. Tamilselvi et al., "WPT: A Smart Magnetic Resonance Technology-Based Wireless Power Transfer System Design for Charging Mobile Phones," in Proc. 2nd Int. Conf. Intell. Innovative Technol. Comput., Electr., Electron. (ICIITCEE), 2024, doi: 10.1109/IITCEE59897.2024.10467828.

[12] M. Tamilselvi et al., "IoT-Based Smart Robotic Design for Identifying Human Presence in Disaster Environments Using Intelligent Sensors," in Proc. 2024 Int. Conf. Autom. Comput. (AUTOCOM), pp. 399-403, 2024, doi: 10.1109/AUTOCOM60220.2024.10486106.

[13] M. J. Basha et al., "Advancements in Natural Language Processing for Text Understanding," E3S Web Conf., vol. 399, 2023, doi: 10.1051/e3sconf/202339904031.

[14] M. Pandey et al., "Blockchain Technology: Applications and Challenges in Computer Science," E3S Web Conf., vol. 399, 2023, doi: 10.1051/e3sconf/202339904035.

[15] R. Pushpakumar et al., "Human-Computer Interaction: Enhancing User Experience in Interactive Systems," E3S Web Conf., vol. 399, 2023, doi: 10.1051/e3sconf/202339904037.

[16] F. R. Willett et al., "High-Performance Brain-to-Text Communication via Handwriting," Nature, vol. 593, no. 7858, pp. 249–254, May 2021, doi: 10.1038/s41586-021-03506-2.

[17] A. Halbouni et al., "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," IEEE Access, vol. 10, pp. 99837-99849, 2022, doi: 10.1109/ACCESS.2022.3207312.

[18] B. Latha et al., "Hand Gesture and Voice Assistants," E3S Web Conf., vol. 399, 2023, doi: 10.1051/e3sconf/202339904050.

[19] R. Gorli et al., "Towards Optic Enlightenment: Future Free Space Optics Architecture & Dynamic Modeling," in Proc. 2nd Int. Conf. Intell. Data Commun. Technol. Internet Things (IDCIoT), pp. 785-791, 2024, doi: 10.1109/IDCIoT59759.2024.10467547.

[20] P. Kavitha et al., "Detection for Melanoma Skin Cancer through ACCF, BPPF, and CLF Techniques with Machine Learning Approach," BMC Bioinformatics, vol. 24, no. 1, 2023, doi: 10.1186/s12859-023-05584-7.

[21] H. Anandaram et al., "Applications of Quantum Cascade Lasers in Spectroscopy and Trace Gas Analysis," in Proc. 4th Int. Conf. Adv. Electr., Comput., Commun., Sustain. Technol. (ICAECT), 2024, doi: 10.1109/ICAECT60202.2024.10469348.

[22] J. Sumithra et al., "A Smart and Systematic Vehicle Headlight Operations Controlling System Based on Light Dependent Resistor," in Proc. 2nd Int. Conf. Intell. Innovative Technol. Comput., Electr., Electron. (ICIITCEE), 2024, doi: 10.1109/IITCEE59897.2024.10467948.

[23] A. Tam et al., "Identification of Brain Tumor on MRI Images with and Without Segmentation Using DL Techniques," E3S Web Conf., vol. 399, 2023, doi: 10.1051/e3sconf/202339904049.

[24] M. Gandhi et al., "An Innovative Method for Paddy Yield Prediction Based on DCNN-ELM Approach," in Proc. 2nd Int. Conf. Intell. Data Commun. Technol. Internet Things (IDCIoT), pp. 762-767, 2024, doi: 10.1109/IDCIoT59759.2024.10467772.

[25] T. Sathya et al., "Bitcoin Heist Ransomware Attack Prediction Using Data Science Process," E3S Web Conf., vol. 399, 2023, doi: 10.1051/e3sconf/202339904056.

[26] R. Sasirekha et al., "Smart Poultry House Monitoring System Using IoT," E3S Web Conf., vol. 399, 2023, doi: 10.1051/e3sconf/202339904055.

DOI: https://doi.org/10.54216/FPA.190204
Received: December 02, 2024 Revised: February 02, 2025 Accepted: March 01, 2025