IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 7 January 2024, accepted 27 February 2024, date of publication 1 March 2024, date of current version 7 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3372859

RESEARCH ARTICLE

Improved Crow Search-Based Feature Selection and Ensemble Learning for IoT Intrusion Detection

D. JAYALATCHUMY[1], RAJAKUMAR RAMALINGAM[2], ARAVIND BALAKRISHNAN[3], MEJDL SAFRAN[4], AND SULTAN ALFARHOOD[4]

[1]Department of Computer Science and Engineering, Perunthalaivar Kamarajar Institute of Engineering and Technology, Karaikal 609603, India
[2]Centre for Automation, School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu 600127, India
[3]Department of Computer Science and Technology, Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh 517325, India
[4]Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

Corresponding authors: Rajakumar Ramalingam (rajakumar.r@vit.ac.in) and Mejdl Safran (mejdl@ksu.edu.sa)

This work was supported by King Saud University, Riyadh, Saudi Arabia, through the Researchers Supporting Project Number (RSPD2024R1027).

ABSTRACT Network intrusion detection in the Internet of Things (IoT) framework has posed considerable challenges in recent decades. A wide variety of machine-learning approaches are introduced in network intrusion detection. The existing methodologies commonly lack consistency in achieving optimal performance across various multi-class categorization tasks. The present study elucidates implementing a unique intrusion system with the primary objective of enriching the efficacy of network intrusion detection. In the initial phase, it is imperative to employ data-denoising methodologies to effectively tackle the issue of data imbalance. In the next step, the enhanced Crow search algorithm is used to determine the most significant features that aid in better classifying intrusion attacks. In the final phase, the ensemble classifier takes the selected features as input to categorize the standard and invader labels. The present work introduces an ensemble mechanism that comprises four distinct classifiers. The assessment of the proposed approach is validated on two denoised datasets, specifically NSL-KDD and UNSW-NB15. The experimental outcomes demonstrate that the formulated approach achieves exceptional accuracy of 99.4% and 99.2% for the NSL-KDD and UNSW-NB15 datasets, respectively.

INDEX TERMS Network intrusion detection, crow search algorithm, machine learning, ensemble learning, Internet of Things.

I. INTRODUCTION

Internet of Things (IoT) refers to developing the Internet infrastructure to include many networked computing devices embedded into our daily lives. Data transmission and reception allow these gadgets to interact with their surroundings and connect with other systems. The wide use of IoT devices has increased data sharing. However, this increase in data transmission may expose users to cyber threats. The IoT's numerous and heterogeneous components make security more important. Implementing countermeasures to protect IoT data from cyber threats is hence essential [1]. Figure 1 illustrates the architecture of IoT with regard to numerous layer-wise attacks. Cybersecurity is a field dedicated towards safeguarding various components within the cyberspace ecosystem. The Internet infrastructure consists of software, computer equipment, telecommunications networks, computer servers, peripheral gadgets, data, and information, among other essential components. Its primary objective is to mitigate potential risks and threats that may compromise these components' integrity, confidentiality, and availability. Cybersecurity aims to ensure cyberspace's resilience and protection by implementing robust security measures and protocols. The primary motive of this endeavour is to mitigate

The associate editor coordinating the review of this manuscript and approving it for publication was Md. Arafatur Rahman.

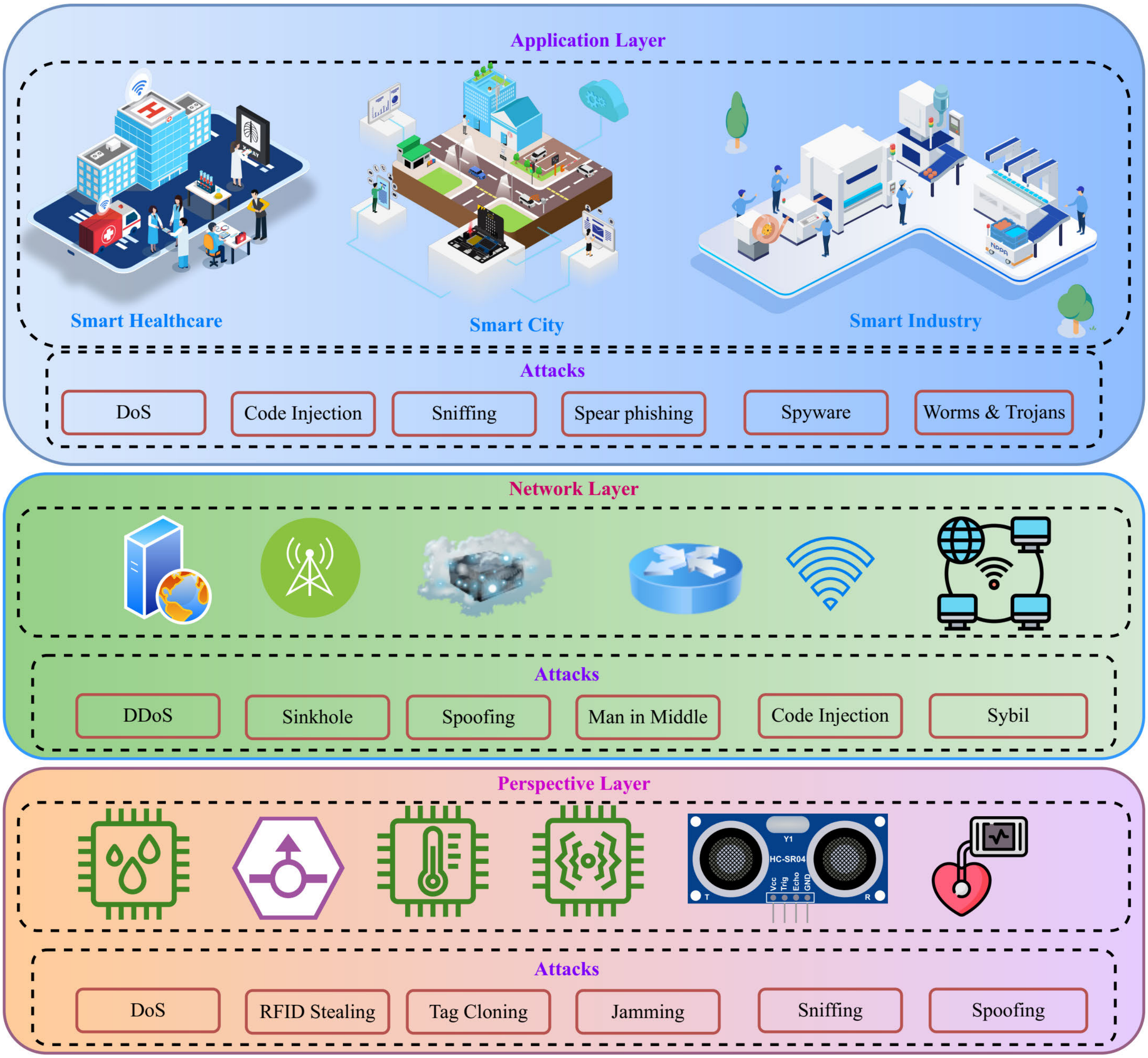


FIGURE 1. IoT Architecture with layer-wise attacks.

and address potential risks and vulnerabilities that could compromise the integrity, confidentiality, and availability of these components [2].

In cybersecurity, Intrusion Detection Systems (IDS) protects Internet-connected systems from internal and external attacks [3]. IDS is needed to address security challenges due to the Internet's pervasiveness and rising cyberattacks. IDS is further classified into two methods, namely anomaly-based IDS (AIDS) and network-based IDS (NIDS). An AIDS method may locate and detect system or dataset abnormalities. This strategy compares data patterns to normal behavior to find deviations. Meanwhile, it alerts users to abnormalities, allowing them to respond quickly and reduce risks. These upgraded security measures enable signal-based algorithms to detect zero-day attacks and known threats [4]. However, creating sophisticated network-based IDS is tough, and analysing massive amounts of data is a challenging issue. The amount of data makes invasion detection harder. Another problem is distinguishing network activity from assaults. Determining the boundaries of these two groups is difficult, deterring intelligent NIDS generation.

In the last decade, machine learning (ML) approaches have been increasingly used in the development of IDS [5]. Nevertheless, due to the accelerated advancement of the Internet, the gathered intrusion information holds a variety of insignificant features that mitigate the efficacy of ML approaches. Hence, it is necessary to streamline the significant feature set related to attack categorization. Hence, Feature Selection (FS) is of utmost importance in ensuring the reliability and intelligence of an IDS. FS aims to find a subset of characteristics that maintain data quality while decreasing redundancy. FS retains the most valuable information and discards extraneous aspects by carefully selecting features. Machine learning and data analysis rely on this approach to increase computing efficiency, model interpretability, and dimensionality. Based on its qualities, FS has been widely used in classification, regression, optimisation, and text classification [6]. Basically, FS is considered as NP-hard issue. The remarkable efficacy of meta-heuristic approaches in addressing NP-hard issues has captured the attention of researchers, prompting them to consider these algorithms for FS.

Meta-heuristic algorithms are efficient in searching for numerous feasible solutions in every iteration without prior knowledge. They hold strong intensification and diversification capabilities when compared with traditional approaches. Recently, researchers from various domains applied meta-heuristic algorithms to FS. Some of the recent works that employed meta-heuristic algorithms for FS in IDS are: Genetic Algorithm (GA) [7], Bat Optimization algorithm (BOA) [10], Particle Swarm Optimization (PSO) [8], Dragonfly Algorithm (DA) [11], Grey Wolf Optimization (GWO) [9], Firefly optimization (FFO) [12], whale optimization algorithm (WOA) [13] and Pigeon Inspired Optimizer (PIO) [14]. Among them, Alazzam et al. [14] proposed a PIO to select the prominent features by eradicating the redundant features. In addition, sigmoid functions are used to convert the velocity to a binary format. Bahram et al. [15] manoeuvred the Artificial Bee Colony (ABC) approach to enhance the efficiency of IDS by mitigating the malicious traffic in the network. They applied ABC to enrich the values of linkage weight and biases. Khare et al. [16] applied the Spider Monkey Optimization (SMO) algorithm to minimise the dimensionality of the problem by selecting the significant features. Subsequently, the chosen characteristics are inputted into a deep neural network (DNN) to improve the classification accuracy. However, the above-specified approaches still have the limitations of poor convergence and exploring the search space, thereby striking into local optima.

Recently, Askarzadeh [17] proposed a novel optimization algorithm, namely the Crow Search Algorithm (CSA), which has garnered significant interest from the research community since its inception. The evaluation results of CSA indicate its high efficiency in addressing optimization problems, particularly those that pose challenges for the fields of science and engineering. In the present context, it is noticable that the algorithm exhibits ease of implementation with a limited number of parameters. However, the CSA algorithm has some limitations, most notably the high chance of being struck in local optima due to the awareness probability parameter [18]. Furthermore, past iterations of the CSA algorithm used a mechanism that depended on randomness to explore both intensification and diversification. To annihilate the above-mentioned issues, various researchers proposed modified versions of CSA. Some of the recent works, such as Sayed et al. [19] introduced chaotic CSA (CCSA) to handle the FS problem for standard UCI benchmark datasets. Ouadfel et al. [20] proposed enhanced CSA (ECSA) to determine the prominent characteristics and enrich the classification accuracy. The authors applied ECSA to 16 UCI repository datasets and achieved better accuracy. However, it still suffers in adaptability and is prone to being struck in local optimal during instantiation. Therefore, it is necessary to propose an improved global search process and a dynamic adaptive parameter (DAP). This study discusses an improved CSA that obliterates the difficulties and trades off the search process by incorporating improved search capability and DAP.

The primary importance of this work is emphasised as below:

- Employ a MinMax Scalar and a Modified Adaptive Synthetic Sampling (MADASYN) approach to handle the pervasive challenges of imbalance and over-fitting issues.
- To propose an Improved Crow Search Algorithm (ICSA) by incorporating an improved search process and dynamic adaptive parameters for optimal feature selection from denoised datasets.
- To design an ensemble classifier to classify multi-class classification within two denoised datasets, specifically the NSL-KDD and UNSW-NB15 datasets. The selected features effectively alleviate the computational burden by eliminating feature vectors characterized by high correlation.
- To assess the efficacy of the ensemble classifier using a range of performance metrics, including accuracy, F1-score, false positive rate, recall, and precision rate.

The organization of this article is structured as follows: Section II comprehensively summarizes the current state-of-the-art studies on this topic. The discussion of the datasets and problem formulation is displayed in Section III. Section IV provides an analysis and examination of the proposed technique. Section V presents the experimental results and subsequent discussion. The paper concludes with key findings in Section VI.

II. RELATED WORK

Dwivedi et al. [21] employs an ensemble model and a meta-heuristic approach to choose features on the IDS dataset and came up with high-rated characteristics. In the study, the researchers employed the SVM classifier to classify incursions and conventional assaults effectively. The EFSAGOA-SVM model, which was employed in the study, yielded a classification report with notable accuracy. However, it is crucial to note that the model's computational cost was high, as the quantitative evaluation showed. To enhance the classification outcomes, a cutting-edge hybrid meta-heuristic optimization method was employed in conjunction with a SVM classifier. In another work, Li et al. [22] proposed utilising a multiple convolutional neural network (MCNN) to enhance the efficiency and effectiveness of IoT-based identification systems. The outcome validates the efficiency of the proposed MCNN technique in achieving superior classification precision while maintaining lower computational complexity. It was explicitly observed in the framework of the NSL-KDD dataset. The MCNN technique, as currently implemented, focuses exclusively on data security, with a specific emphasis on its application within the industrial IoT context.

Tao et al. [23] presents the integration of a genetic algorithm with SVM to enhance the performance of intrusion attack classification. This integration specifically focused on weight, parameter, and feature selection, aiming to optimize the classification process. The comprehensive simulation analysis conducted in the study has revealed that the suggested model effectively reduces the error percentage and improves classification by providing faster convergence. However, it should be noted that the SVM classifier is primarily designed to handle binary classification tasks. As a result, its performance may be suboptimal when applied to datasets with multiple classes, especially larger ones, such as intrusion databases. Kunhare et al. [24] proposed the utilization of Particle Swarm Optimizer (PSO) to pick significant traits from the NSL-KDD. This approach aimed to enhance the precision rate and decrease the false positive rate in IoT-based IDS.

Ramaiah et al. [25] suggested a shallow and optimised neural network architecture that could find and classify malicious attacks in the KDDCup 99 database. The results of the simulation indicate that the IDS system presented in the study exhibited a higher level of performance when assessed using various evaluation measures. In the realm of deep learning, it is widely acknowledged that attaining superior classification outcomes necessitates utilizing high-performance processing systems. However, it is significant to note that such schemes come with a significant computational cost. Chen et al. [26] suggested combining k-means clump with a meta-heuristic algorithm to make IoT-based identification work better. However, it is not suitable for multi-class intrusion classification scenarios.

Alazzam et al. [17] present a novel approach to selecting optimal features in IoT-based IDS. The technique employed in the study utilizes a pigeon-inspired approach to achieve ideal feature selection. This approach has been acknowledged as highly operative and associated with other meta-heuristic methods that are also investigated in the study. The results specify that the pigeon-inspired optimization technique exhibits superior performance compared to other optimization techniques in various evaluation metrics. However, it is worth noting that the current optimization technique exhibits a limitation in dealing with local minima, which should be addressed in future research endeavours. Wang et al. [27] puts forward a new method that combines improved kernel-based extreme learning with a neural network to solve the problems that come up with IoT-based identification. Experiments in the study showed that the IKBELM-DBN model presented had the best classification performance when compared to other intelligent data classification models that were already out there. The DBN's computational complexity arises during training the network, as it involves intricate data models.

The novel ID framework projects by Kan et al. [28] involve the combination of CNNs with the adaptive PSO algorithm. In the present study, the PSO technique was employed to determine the optimal parameters of the CNN model, thereby enhancing its classification performance. However, it is noteworthy that this approach incurred significant computational costs. Alazzam et al. [29] offers a novel and efficient identification framework that leverages the power of a one-class SVM. This context is designed to be lightweight, ensuring minimal computational overhead while achieving robust and accurate identification capabilities. The light-weighted ID framework has demonstrated superior performance compared to other models. Imrana et al. [30] carried out the Bi-directional Long Short-Term Memory (Bi-LSTM) network for efficient IDS. The Bi-LSTM network has demonstrated superior detection rate performance associated to other approaches, as shown by higher scores in f1-score, recall, accuracy, and precision. The Bi-LSTM network that has been presented exhibits certain challenges, namely overfitting and vanishing gradients. Tomer and Sharma [31] employed an ensemble machine-learning approach for identifying and detecting attacks in IoT systems.

Xu et al. [32] presents a new way to fix the problem in the IoT network by creating a five-layer auto-encoder model. The auto-encoder model demonstrates a commendable ability to address the challenges posed by outliers and dimensionality reduction effectively. However, it is significant to note that the prototype does encounter a limitation in the form of overfitting. Azzaoui et al. [33] introduced a deep neural network (DNN) model specifically designed to classify IoT network traffic. Through their experiments, the researchers discovered that the DNN model had exceptional classification performance on the NSL-KDD database. In the realm of DNNs, it is widely acknowledged that achieving higher classification results necessitates a larger amount of training data. However, it is crucial to acknowledge that this increased data necessity comes with higher computing costs.

Dahou et al. [34] successfully combined a CNN with the reptile search technique to address the identification challenges in the framework of IoT. The utilization of the RSA is explored to enhance the concert of the CNN model. Specifically, the RSA is introduced to classify the optimal values for various parameters in the CNN model. As the literature would indicate, the CNN-RSA approach has demonstrated commendable performance on various online intrusion databases. However, it is noteworthy that the model's computational requirements were found to be relatively high. To effectively address the issues, a cutting-edge ensemble model has been created and combined with the Fruitfly Optimisation Algorithm (FOA) to achieve better intrusion detection performance while working with limited computing time.

Additionally, the study by Nour et al. [35] proposed a comprehensive approach that combines unsupervised and statistical techniques to detect abnormal traffic patterns in LTE mobile networks. The modelling of the healthy network was conducted using unsupervised learning techniques. Various factors, including revenue, customer satisfaction, and performance, were taken into consideration during the modelling process. The severity of the situation was effectively managed through the utilization of a statistical approach, which aimed to ensure the optimal functioning of the network. The study by Louk and Tama [36] has successfully created a comprehensive framework that addresses the difficulties brought about by imbalanced data. This framework incorporates standalone and ensemble strategies, providing a robust approach to effectively handling imbalanced datasets. As stated in their report, the researchers observed that Easy Ensemble exhibited superior performance compared to other contemporary standalone and ensemble strategies. The results of this study also exhibit that both undersampling and oversampling methods can be trusted when used with boosting-based ensemble approaches instead of the more common initial-based ensemble approaches.

Aburomman and Reaz [37] introduced an ensemble model in their study, wherein they employed the PSO technique to derive an ideal ensemble model for the purpose of intrusion detection. The Local Unimodal Sampling (LUS) technique was employed to select the optimal parameter for the PSO algorithm. The author's utilization of the Weighted Moving Average (WMA) technique facilitated the construction of an ensemble model. The investigation conducted by the author revealed that novel methodologies exhibit higher concert in terms of accuracy when associated with the WMA approach. Moreover, Sarvari et al. [38] has proposed an innovative method for detecting anomalies. This approach leverages the combination of the Minimum Covariance Determinant (MCF) and evolutionary NN techniques. The researchers then evaluated the performance of their approach using the conventional NSL-KDD dataset, which serves as a benchmark in anomaly detection research. The adoption of the MCF technique in this study aims to select the most promising features from the provided feature space. This strategic decision was taken to mitigate the computational complexity associated with the feature selection process and enhance the overall efficiency of the classifier. Thereafter, the features picked using the MCF method were fed into the evolutionary neural network algorithm to correctly divide system traffic into two groups: regular traffic and irregular traffic. The experimental findings have demonstrated that the suggested methodology has led to notable enhancements in both the concert and efficacy of IDS.

In the study by Ma et al. [39], the researchers suggested using a linear SVM model to detect irregular traffic. The methodology utilized NLP methods for pre-processing and extracting feature vectors. Subsequently, the extracted trait vector was provided to the classifier to facilitate identifying anomalous traffic patterns. Camacho et al. [40] initiates a novel approach to anomaly detection. The researchers suggest an extension to Principal Component Analysis (PCA) by incorporating group-wise PCA and supplementary exploratory features derived from recent applications in the relevant domain. Table 1 summarises similar research using FS techniques for IDS, including their dataset and number of features (NF) used for model training. The symbol × indicates the author did not report the information, and the cons of the existing model are discussed.

A. MOTIVATION

Based on our investigation, it was noticed that most of the previous works have focused on classical ML techniques for improvement in IDS. The main aim of the developed IDSs was to identify network traffic profiling data for unauthorized access or malicious activity. However, these typical methods have performed poorly on huge, complex datasets due to numerous features. Consequently, the researchers were attracted towards meta-heuristic approaches owing to its ease of implementation and efficacy in handling complex problems with strong search capability. Since, the recent studies on meta-heuristic methods are prone to optimal struck and premature convergence due to improper trade-off among the search process. Similarly, few researchers in their previous studies manually curate ensembles of two or more classifiers to enrich the classification process. However, these approaches have various limitations due to their trial-and-error development. In addition, few methods have been established to effectively address class imbalance and feature selection in IDS. However, the current methods for class imbalance datasets produce unsatisfactory results.

Hence, our proposed approach incorporates three phases of work, primarily, an efficient class imbalance approach with MADASYN and Min-Max Scalar function that can mitigate the imbalance issues and convert the features into 0 and 1. Secondly, an improved crow search algorithm with improved search process and DAP to select the significant features. Finally, an ensemble learning model with majority voting scheme improve the IDS classification accuracy.

III. PRELIMINARIES

The subsequent section provides a complete overview of the two datasets utilized in this study to discourse the issue of class imbalance. These datasets, namely NSL-KDD [32] and UNSW-NB15 [49], were selected for their relevance to the research objective. Furthermore, we formulate the analysis of the problem to effectively tackle the presence of malicious actors in commonly encountered situations. In addition,

TABLE 1. Critical analysis of IDS methods in literature.

Ref.	Algorithm	DP	FS	Classifier	Class.	Dataset	NF	Cons
[41]	LS-SVM	×	Improved forward floating selection	SVM	Binary	KDD99	6	Limited dataset size utilized.
[42]	CFS-BA	Data Normalization	Correlation based FS with Bat Algorithm	SVM	Binary	NSL-KDD, AWID, CIC-IDS2017	10, 8, 13	Computational cost is high
[43]	LS-IDS	Dimension Reduction	×	B-Stacking Ensemble	Multi-class	CICIDS2017, NSL-KDD	28	Poor performance on U2R and R2L attack types
[44]	RANet	Min-Max normalization	CNN	CNN based RANet	Multi-class	NSL-KDD, KDD99, CICIDS2017	41 and 122	Poor performance on infrequent attack types
[45]	CP-GWO	Correlation Reduction	closest position based GWO	CNN+LSTM	Binary	NSL-KDD, DARPA1998, DDoS-1.0, KDD99	5	Especially designed for DDoS detection
[46]	GWO-PSO	Data normalization	Hybrid GWO+PSO approach	Ensemble KMeans+SVM	Binary	NSL-KDD	20	Can only distinguish among attack and benign traffic
[47]	GEO-SMPIF	Min-Max normalization	Corporate Hierarchy optimization	Self-constructing Multi-layer Perceptron Interfaced Fuzzy system	Binary	NSL-KDD, UNSW-NB15	11, 13	considered only binary classification
[48]	FOA-IDS	Min-Max normalization	Firefly optimization algorithm	Ensemble SVM+KNN+LSTM+MLP	Multi-class	NSL-KDD, UNSW-NB15	11, 11	Poor performance on infrequent attack types

GWO - Grey Wolf Optimization; FOA - Firefly optimization algorithm; LS - Least Square; MLP - Multi-layer perceptron; AWID - Aegean WI-FI intrusion dataset; KNN - K-Nearest Neighbors; DP – Data Preprocessing; FS - Feature Selection; Class. – Classification; NF – Number of Features selected

this discourse delves into the conventional Crow search algorithm, examining its outcomes in terms of exploitation and exploration.

A. DATASET DESCRIPTION

The primary objective of employing a machine-learning-based approach is to effectively extract meaningful and valuable information from the input data. Consequently, the performance of the ML system is contingent upon the quality of the input data provided. The present study utilizes two distinct datasets, specifically the NSL-KDD and UNSW-NB15 datasets. The NSL-KDD dataset, commonly called the network dataset, was developed to address the limitations noticed in the KDD'99 dataset. The NSL-KDD dataset comprises a total of 148,517 records of network flow information. Among these records, 77,054 are classified as standard records, while the rest, 71,463 are classified as attack records. The dataset under consideration comprises 41 distinct features, encompassing 32 numerical variables and nine categorical attributes [32]. The introduction of the UNSW-NB15 dataset was conducted by the Cyber Range Laboratory for Cyber Security, utilizing the IXIA framework. This dataset encompasses a comprehensive collection of both normal and attack records. The dataset encompasses a mean value of 22,18,761 and a deviation of 3,21,283 attack records. Moreover, it is noteworthy to mention that the dataset under consideration comprises 49 distinct features. Among these features, 42 are characterized by numerical values, while the remaining 6 exhibit categorical values, as reported in [49].

B. PROBLEM FORMULATION

This study considers the feature set α, which encompasses a wide range of features denoted as μ. Additionally, we examine instances represented by (β_i, γ_i), where $\beta_i \rightarrow \sigma$ represents actual network traffic samples and $\gamma_i \rightarrow \tau$ signifies the corresponding labelled classes. Furthermore, we acknowledge the existence of various types of attacks, which are denoted as ϕ. The primary objective of IDS is to achieve a classifier, indicated as $f : \sigma \rightarrow \tau$, that accurately represents the arrival of network traffic. The invader's objective is to produce indistinguishable attack information ω, which can then be incorporated into the existing instances β_i, creating an attacker instance denoted as β^+. Moreover, it is essential to note that the provided instance will be classified as $\beta_i + \omega \neq \gamma_i$. In the present investigation, we have introduced a MADASYN [50] to generate the appropriate β^+coefficient. This coefficient effectively addresses the class imbalance problem by achieving a balanced representation of both the minority and majority classes. Furthermore, the researchers have proposed incorporating a meta-heuristic-based feature selection technique. This technique aims to identify and select the most relevant features that can assist machine learning and deep learning approaches in reducing the dimensionality of the data. Doing so enables the models to classify instances effectively and accurately as either normal or belonging to an attacker.

C. CROW SEARCH ALGORITHM

Crow Search Algorithm [17] is a meta-heuristic algorithm that draws inspiration from the social behavior of crows, specifically their mechanism for hiding food. Crows can conceal food items and retain accurate recollections of their locations for extended periods, often spanning several months. The individuals of this species exhibit a social behavior known as flocking, wherein they congregate and coexist in a group. Within this flock, everyone engages in the fascinating behavior of attempting to locate the concealed food sources belonging to their fellow group members. In addition, it specifies that crows exhibit a remarkable behavior of diligently safeguarding their food resources by regularly altering the location of their caches. A novel model proposes to effectively represent the feature selection problem based on the observed behavior of crows. The mathematical formulation of standard CSA is represented as follows:

Each search agent position i at iteration k in the search boundary determined by a vector γ_i^k and Equation (1) symbolizes a suitable individual for the issue being investigated.

$$\gamma_i^k = [\gamma_1^k, \gamma_2^k, \ldots, \gamma_n^k]; \quad i = 1, \ldots, P_s;\ k = 1, \ldots, M_{iter} \tag{1}$$

where NP determines the population size, and M_iter denotes the overall iterations. Crows save their food hiding position in memory m_i^k, which is also their best posture. Crows move through the search region and aim to take hidden food each iteration. Crow updates its position using Eq. (2).

$$\gamma_i^k = \begin{cases} \gamma_i^k + r_i \times FL_i^k(m_i^k - \gamma_i^k), & \text{if } rand > AP_i^k. \\ arbitrary\ \ location, & \text{or else.} \end{cases} \tag{2}$$

where r_i and rand denote the arbitrary values with rigid distribution within the range of [0, 1], and AP_i^k symbolizes the awareness likelihood of crow i at k, FL_i^k indicates the flight length of crow i at k. Lower values of FL enrich the intensification, and higher values lead to diversification. Algorithm 1 showcases the pseudocode for the standard CSA.

IV. PROPOSED METHODOLOGY

A. DATA PRE-PROCESSING

The pre-processing of a dataset encompasses various essential phases, such as data regularization, reduction, cleaning, and transformation. These phases are crucial in preparing the dataset for further analysis and modeling. The significance of these steps cannot be understated, as they have the potential to greatly impact the concert of the classifier. Primarily, it is imperative to eliminate null values and duplicate records to mitigate any potential bias that may arise from these frequently occurring records. In contrast, it specifies that both datasets on the training sets do not contain any duplicate records. The subsequent step involves the implementation of data denoising, which is achieved by scaling the data values to a proportional and specific range for each feature. The MADASYN sampling technique is a method that aims to improve the learning proportion by strategically adjusting the classification verdicts to challenging instances [50]. Additionally, it works to mitigate the bias that arises from class imbalance.

In contrast, the MinMax scaler approach transforms the acquired data into a normalized range from 0 to 1. This procedure is used to mitigate the impact of negative vectors of attributes and abnormalities on the dataset. The mathematical expression of the scalar $\overrightarrow{\Psi}_{i,\nu}$ is presented as follows in Equation (3).

$$\overrightarrow{\Psi}_{i,\nu} = \frac{\Psi_{i,\nu} - \Psi_{i,\nu}^{min}}{\Psi_{i,\nu}^{max} - \Psi_{i,\nu}^{min}}(\nu^{max} - \nu^{min}) + \nu^{min} \tag{3}$$

where $\Psi_{i,\nu}^{min}$ and $\Psi_{i,\nu}^{max}$ specify the lower and upper bounds of i^th attribute concerning the input instances ν. ν^{max} and ν^{min} denote the maximum and minimum values that re-scale the attained intrusion from the original collected data $\Psi_{i,\nu}$ [51]. The subsequent stage involves the transformation of the symbolic data into numerical representations. In each dataset analysed, the attack types have been transformed, resulting in a binary label assignment. Specifically, the attack instances have been allotted a label value of 1, whereas the typical instances are allotted a label value of 0. In the context of training datasets, it is essential to note that exclusively standard data samples are extracted from them. During this period, the system has been designed to exclusively learn and process normal traffic, thereby necessitating the exclusion of any other data types. The data that has been appropriately sampled and re-scaled is then provided to the CSA for further analysis and optimization.

B. PROPOSED FEATURE SELECTION USING ICSA

In the proposed model, it is essential to note that every position occupied by a crow corresponds to a specific subset of features within the overall global feature set. The variable γ_j^k represents the positional value of crow j at iteration k. Crows can remember the location where they have concealed objects. The variable ϕ_i^k represents the memory of the crow j during the iteration k. The crows can retain and recall information regarding the optimal location or perch they have encountered thus far. During each k, crow j endeavours to keep track of crow i. There are five potential search states:

State 1: Improved Local Search using the chaos technique

The crow i lacks awareness that the j is actively engaged in the pursuit of locating its concealed location. The crow j updates its position using Eq. (4).

$$\gamma_j^{k+1} = \gamma_j^k + \psi_j \times \chi_j^k(\phi_i^k - \gamma_j^k) \tag{4}$$

where C_j denotes the chaos function that takes the place of the standard CSA random function and $chijk$ represents the distance the crow j traveled during its flight. The chaos function improves the convergence rate by incorporating a chaotic sine map. The mathematical expression of C_j is

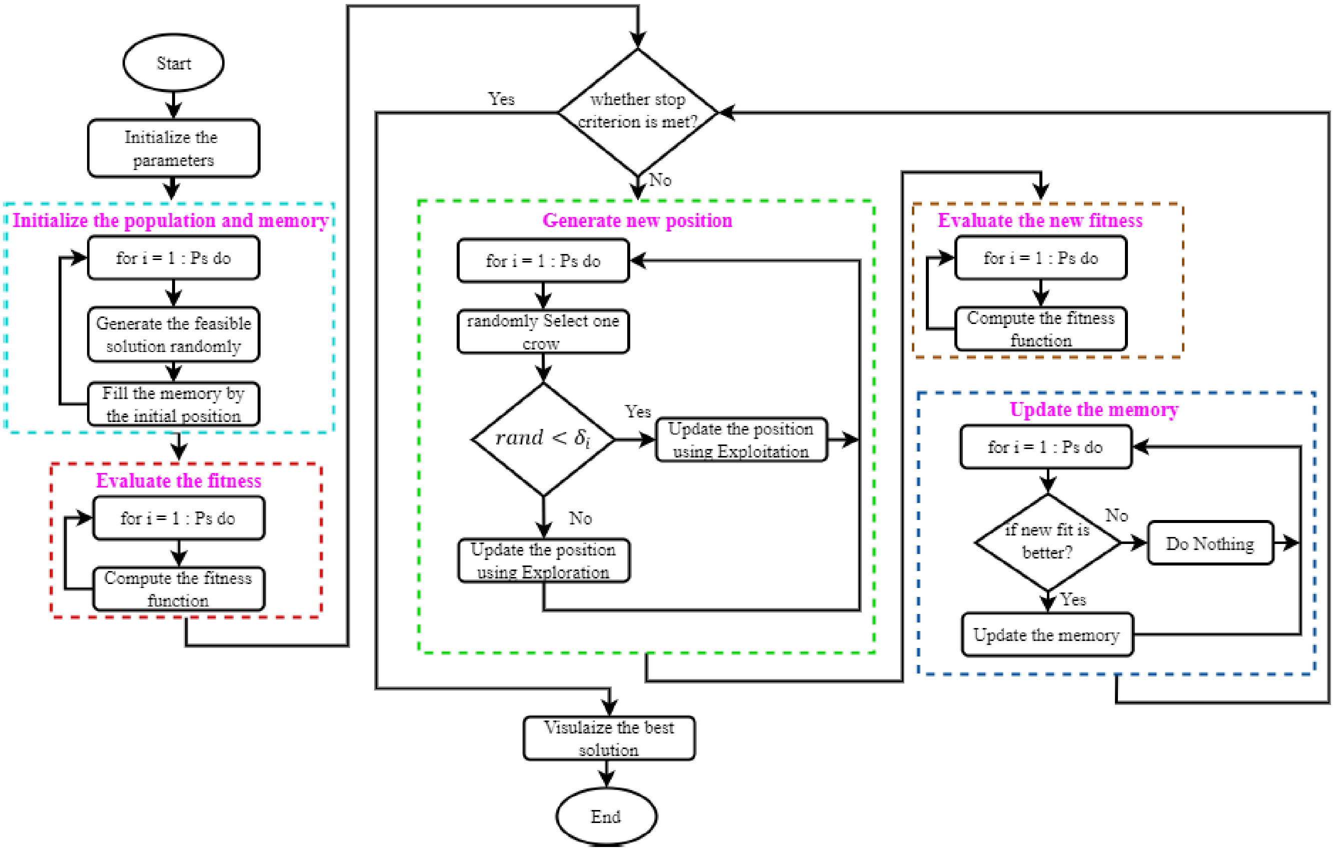

Start
Initialize the parameters
Initialize the population and memory
for i = 1 : Ps do
Generate the feasible solution randomly
Fill the memory by the initial position
Evaluate the fitness
for i = 1 : Ps do
Compute the fitness function
whether stop criterion is met?
Yes
No
Generate new position
for i = 1 : Ps do
randomly Select one crow
rand < δi
Yes
Update the position using Exploitation
No
Update the position using Exploration
Evaluate the new fitness
for i = 1 : Ps do
Compute the fitness function
Update the memory
for i = 1 : Ps do
if new fit is better?
No
Do Nothing
Yes
Update the memory
Visulaize the best solution
End

FIGURE 2. Flowchart of Improved Crow Search Algorithm.

expressed in Eq. (5).

$$\psi_j^{k+1} = \begin{cases} sin(\pi\psi_j^k) & k > 1 \\ 0.7 & k = 1 \end{cases} \quad (5)$$

The chaotic method's coefficient has been explicitly defined so that its return values are limited to the range of 0 to 1. According to Mirjalili and Lewis's [52] proposal, there were a total of eight transfer functions used in the literature. The functions under investigation have been classified into two primary categories: S-shape and V-shape. Based on the investigation, we notice that the V2 transfer function outperforms other functions by yielding superior results. Our work used the V2 transfer function for the local search process.

State 2: Global Search Process

Crow *i* possesses knowledge regarding pursuing crow *j* towards the concealed location. Therefore, it can be inferred that the crow *i* exhibits a behavioral adaptation by altering its hiding place to safeguard itself from potential threats posed by the crow *j*. In the present scenario, the crow *i* exhibits a behavior wherein it selects a position randomly.

The overall crow position in two states is mathematically formulated in Eq. (6).

$$\gamma_j^{k+1} = \begin{cases} \gamma_j^k + \psi_j \times \chi_j^k(\phi_i^k - \gamma_j^k) & rand < \delta_i \\ select \;\; random \;\; position & otherwise \end{cases} \quad (6)$$

State 3: Dynamic Awareness Probability (DAP)

This paper presents the dynamic awareness parameter (DAP) method, in which fit crows use a local search strategy while less fit crows use a global search strategy to become apt. It is crucial to observe that the adaptive parameter (AP) in the standard CSA has the same value throughout the algorithm's execution. The AP value is typically set to 0.1, which is considered standard CSA. The DAP method is implemented in the ICSA scheme, and the AP property of each crow varies according to its rank. The mathematical formulation of the DAP method δ_i is expressed in Eq. (7).

$$\delta_i = \vartheta^{min} + (\vartheta^{max} - \vartheta^{min} \times \frac{R_i}{N} \quad (7)$$

where R_i denotes the rank of the crow i within the N population of crows, the ϑ^{max} and ϑ^{min} represent the minimum and maximum values of the AP, respectively. Based on the experimentation, we set up the ϑ^{max} and ϑ^{min} values as 0.1 and 0.8, respectively. Under our findings, we observe an inverse relationship between the hierarchical rank of crows and their corresponding levels of AP. Specifically, crows that occupy higher ranks within the social hierarchy tend to exhibit lower AP values, while those that occupy lower ranks tend to display higher AP values. The DAP level is set up at the beginning of the program, which is a significant step. The practical definition of the DAP value is the percentage

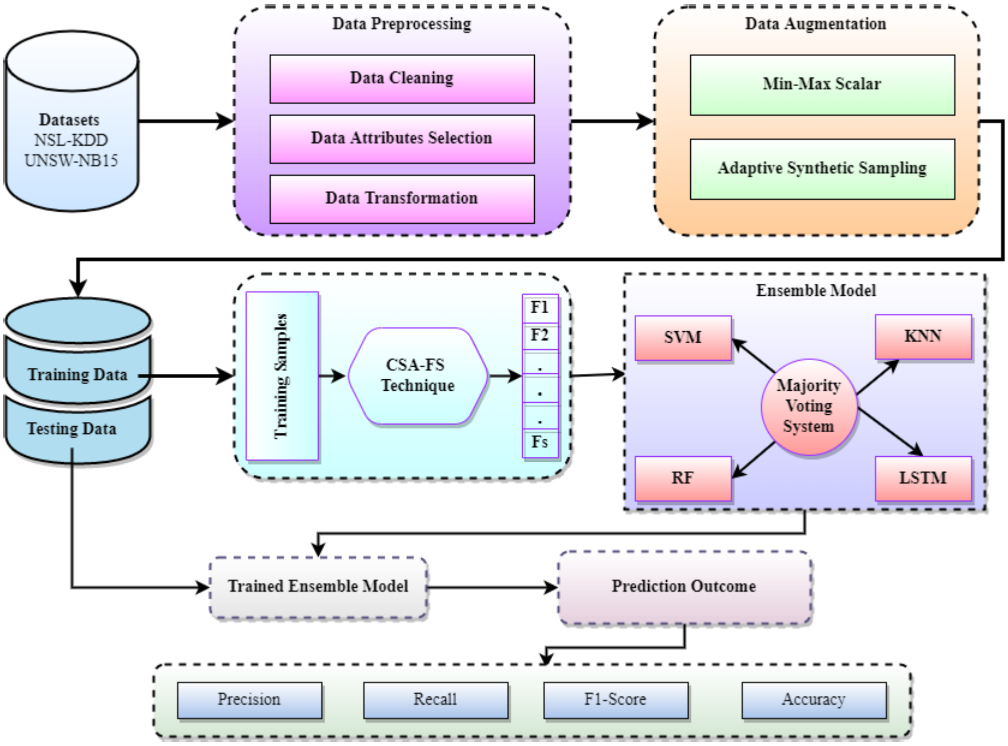


FIGURE 3. The architecture of proposed ICSA-FS based Ensemble Model for NIDS.

TABLE 2. Values of the hyper-parameters for the various classifiers.

Approach	Hyper-Parameters	Values
RF	max_depth	50
	n_estimators	50
KNN	No. of neighbors	22
	Distance weight	Equal
	Distance metric	Spearman
SVM	Complexity constant	102
	Convergence epsilon	11
LSTM	No. of Dense layer	10
	Activation Function	RELU
	Learning rate	0.1
	Momentum	0.8
	Batch_size	64
	Decay rate	0.97

of crows that look in their area; on average, seven out of ten crows use local search methods [53].

State 4: Replace the memory of the crow

The CSA uses a fitness function to assess the viability of individual location. After updating positions, the fitness function assesses the new location. If the new location is improved than the previous one, the crow updates its memory accordingly.

$$\phi_j^{k+1} = \begin{cases} \gamma_j^k + 1 & fit(\gamma_j^k + 1) < fit(\gamma_j^k) \\ \phi_j^k & otherwise \end{cases} \tag{8}$$

State 5: Fitness Function

The proposed approach utilizes a fitness function to determine the efficacy of the crows' position. The mathematical representation of the fitness function is commonly expressed in Eq. (9).

$$\delta_i = \vartheta^{min} + (\vartheta^{max} - \vartheta^{min} \times \frac{R_i}{N} \tag{9}$$

where Acc denotes the accuracy resulting from the ensemble learning model, and F_s and F_N indicate the number of chosen characteristics and the total number of characteristics, respectively. ω specifies the weight argument that establishes a proportional relationship between the two primary performance criteria of the algorithms, namely correctness and the number of chosen characteristics. The findings indicate a negative correlation between the value of *omega* and the number of characteristics the algorithm selects. As ω increases, the algorithm tends to choose a minimal subset of characteristics. This reduction in feature selection harms the overall correctness of the algorithm's performance. Based on the principles outlined in the fitness equation, we can infer that when the numerical value of fitness is elevated, a particular position among the crow's options is deemed superior to the remaining alternatives. In the present study, we empirically determine the value of ω to be 0.2. Algorithm 1 presents the proposed algorithm of ICSA for the feature selection process. The flowchart of the proposed ICSA approach is projected in Figure 2.

C. ENSEMBLE LEARNING CLASSIFIER

The ensemble IDS is employed in this phase after feature selection. The ensemble IDS receives the results of

TABLE 3. Parameters settings of proposed approach and existing approaches.

Ref.	Approach	Parameters	Values
[55]	modified Local Outlier Factor (LOF)	Threshold	1.3
		C	300
		K	65
[56]	Salp Swarm Algorithm based grey wolf optimization for feature selection (SSA-FGWO)	Coefficient (c1)	[2/e, 2]
		Convergence constant	[0,2]
[57]	Salp Swarm Algorithm-based feature selection (SSA-XGBoost)	Coefficient (c1)	[2/e, 2]
		Upper, lower bound	[5, -5]
[58]	Binary Salp swarm algorithm (BSSA)	Control Parameter (c1)	[0,1]
		Control Parameter (c2)	[0,1]
[59]	Improved Harris Hawks Optimization (IHHO)	Energy factor (E)	0.5
		Control Parameter	[0,1]
Proposed	Improved Crow Search Algorithm based Feature Selection (ICSA-FS)	Dynamic Awareness Parameter (DAP)	0.1
		Chaos Function coefficient	[0,1]
		Weight factor (ω)	0.2

TABLE 4. Selected features set by proposed ICSA-FS from NSL-KDD and UNSW-NB15.

Datasets	# features	Selected Feature set
NSL-KDD	11	[2, 4, 6, 10, 12, 17, 23, 28, 36, 37, 41]
UNSW-NB15	7	[3, 8, 12, 23, 29, 38, 43]

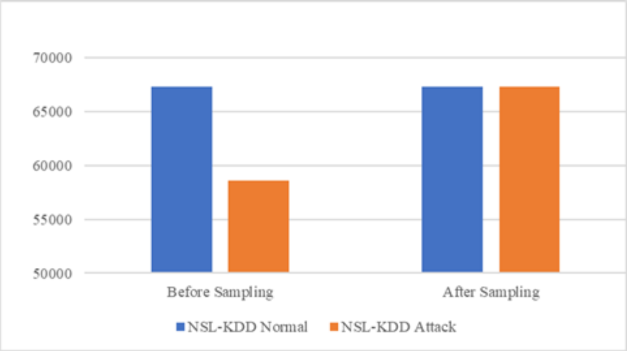


FIGURE 4. Confusion Matrix achieved by proposed ICSA-FS technique on NSL-KDD.

each ICSA-FS feature selection procedure. SVMs were employed to classify linear and non-linear data in which Small to medium-sized datasets gets benefited. When data distribution implies comparable data points have similar labels, KNN may be a viable choice. RF produces good concert in many problems without over-fitting, giving it a trustworthy solution. LSTMs work well for NLP, speech recognition, and time series data. CNN is not chosen since they are not ideal for all data types. LSTM or classic machine learning models may be better for non-spatial or grid-less data like text. The best classifier outcome is selected for further investigation using majority voting.

In this work, the ensemble approach is utilized to train the model using important features during the training step. The RF method, an integral component of the ensemble IDS, is subsequently provided with the selected traits as input. The ensemble IDS combines four different classifiers

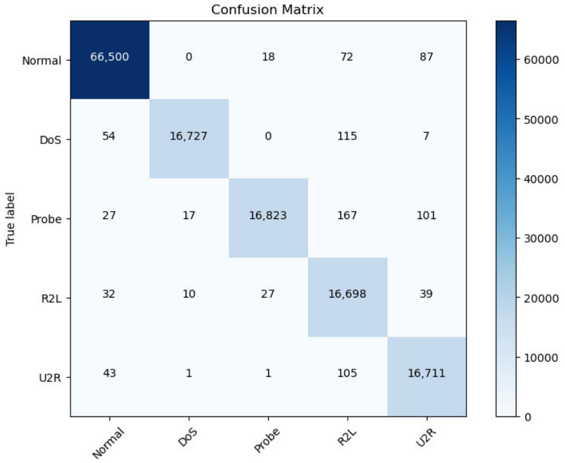


FIGURE 5. Flowchart of Improved Crow Search Algorithm.

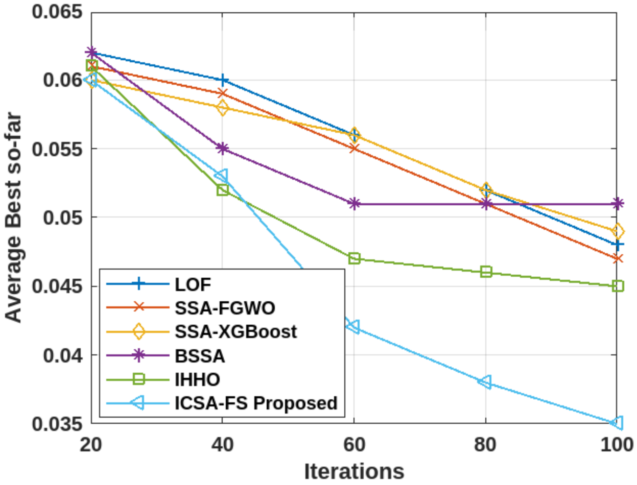
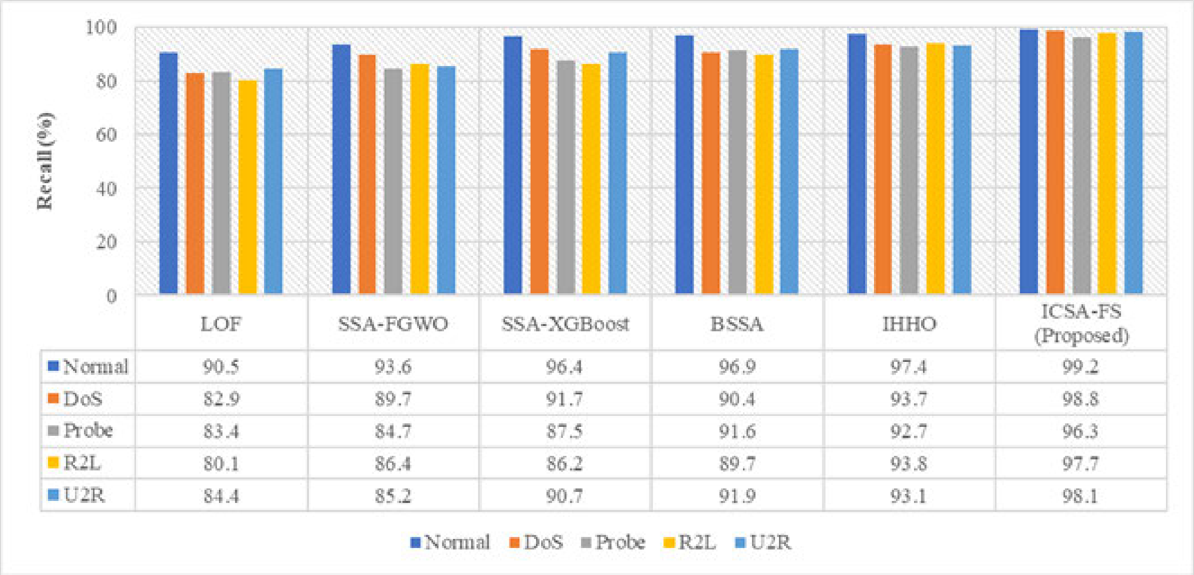
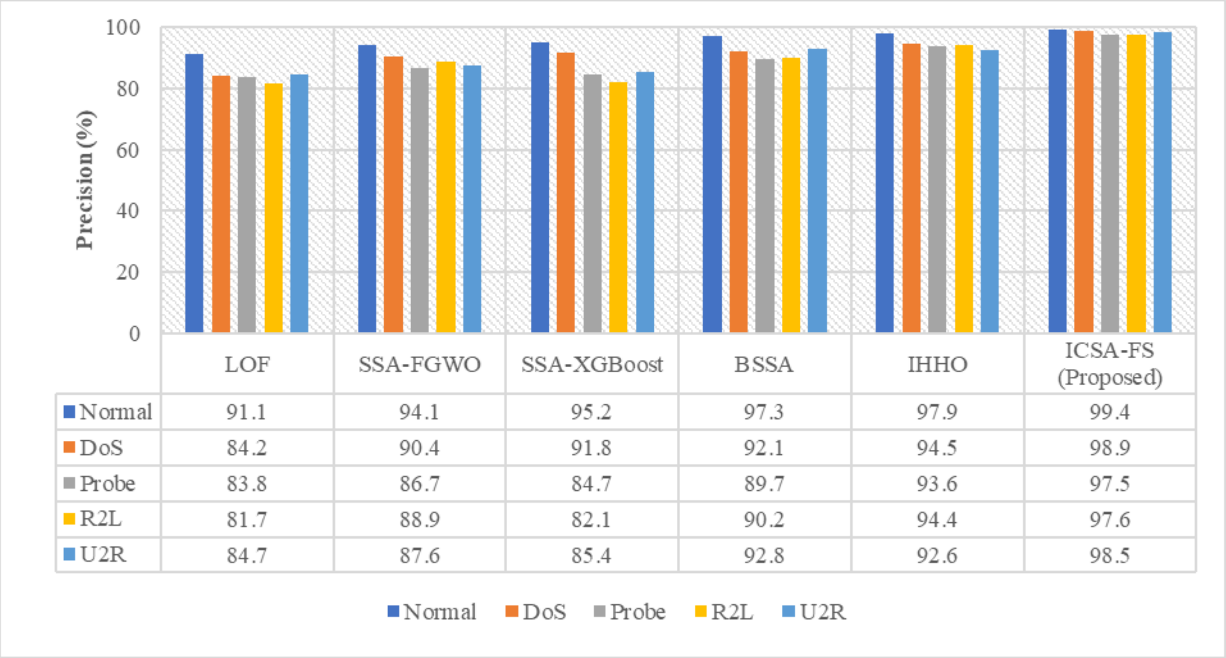


FIGURE 6. Convergence curve of proposed ICSA-FS with other compared models on NSL-KDD.



	LOF	SSA-FGWO	SSA-XGBoost	BSSA	IHHO	ICSA-FS (Proposed)
■Normal	90.5	93.6	96.4	96.9	97.4	99.2
■DoS	82.9	89.7	91.7	90.4	93.7	98.8
■Probe	83.4	84.7	87.5	91.6	92.7	96.3
■R2L	80.1	86.4	86.2	89.7	93.8	97.7
■U2R	84.4	85.2	90.7	91.9	93.1	98.1

FIGURE 7. Recall outcomes of ICSA-FS with other comparative models on NSL-KDD.



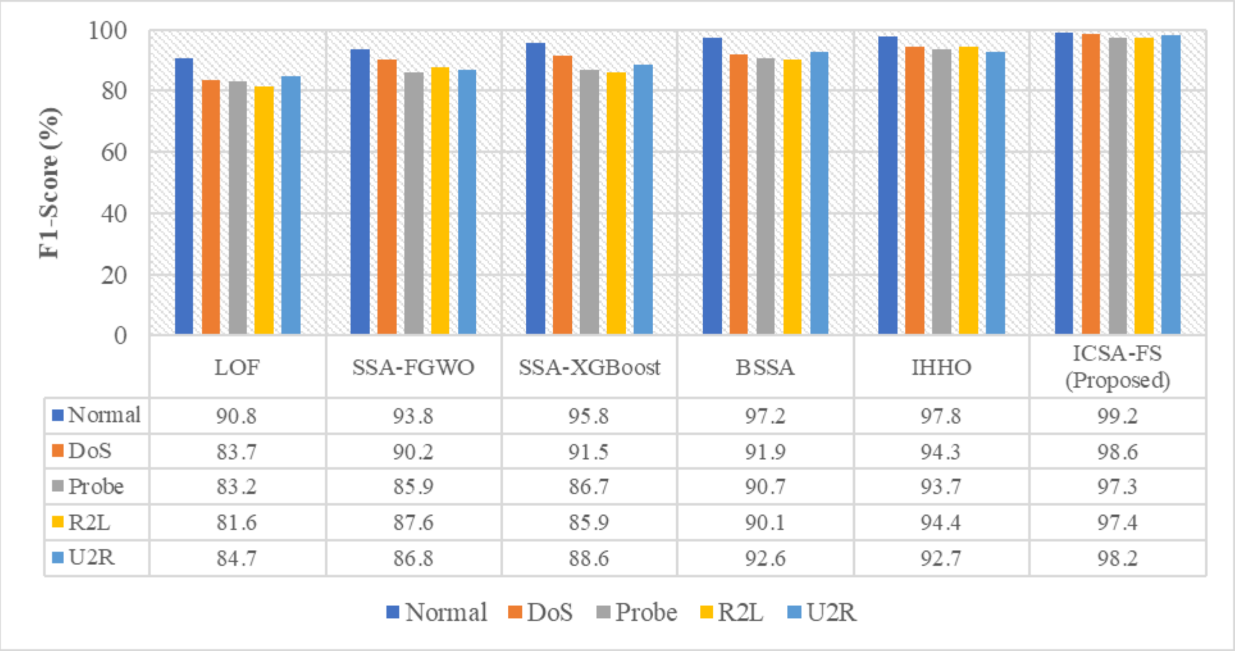
	LOF	SSA-FGWO	SSA-XGBoost	BSSA	IHHO	ICSA-FS (Proposed)
■Normal	91.1	94.1	95.2	97.3	97.9	99.4
■DoS	84.2	90.4	91.8	92.1	94.5	98.9
■Probe	83.8	86.7	84.7	89.7	93.6	97.5
■R2L	81.7	88.9	82.1	90.2	94.4	97.6
■U2R	84.7	87.6	85.4	92.8	92.6	98.5

FIGURE 8. Precision outcomes of ICSA-FS with other comparative models on NSL-KDD.

into a single method. These classifiers are the SVM, KNN, RF and LSTM. Integrating weighted votes from the output of three different classifiers has an impact on the final decision regarding the classification outcome for the testing samples. The working process of the Majority voting scheme [54] is accessible in Algorithm 2. The overall architecture of the projected algorithm is illustrated in Figure 3.

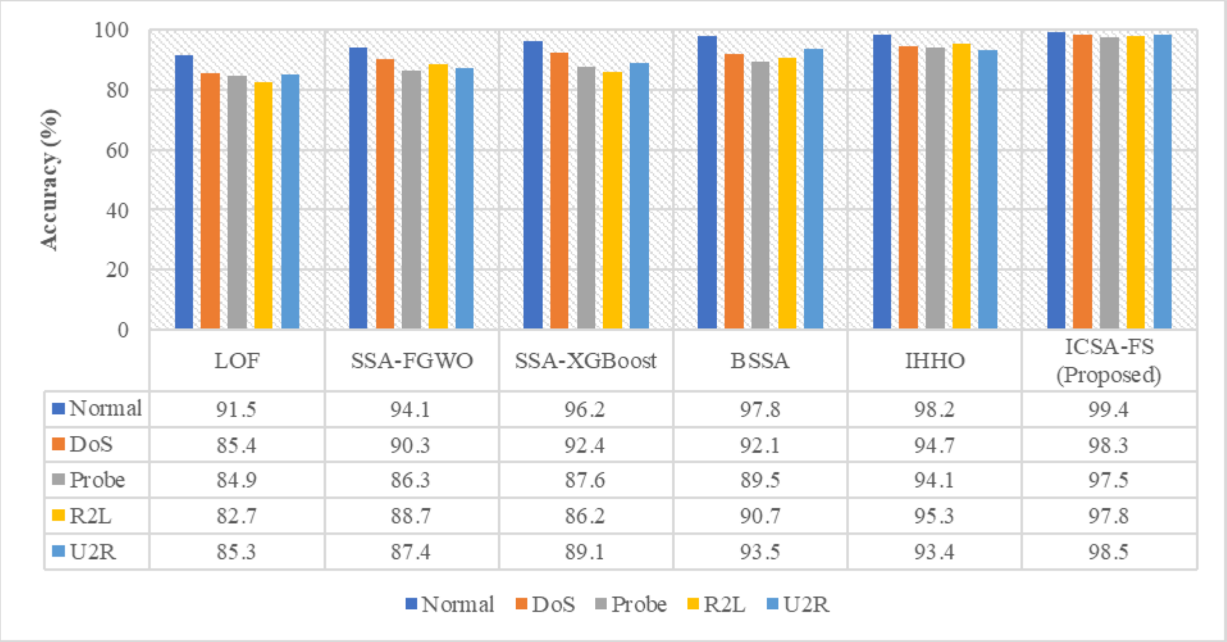
D. COMPUTATIONAL COMPLEXITY

One of the most crucial factors in determining the efficacy of an algorithm is its computational complexity. Several parameters, NP, M_iter, problem dimensions, and an updating mechanism, can be used to estimate the computational cost of the proposed strategy. ICSA is a meta-heuristic approach that holds an enriched search process with dynamic awareness parameters to trade-off search capability. Consequently, the



	LOF	SSA-FGWO	SSA-XGBoost	BSSA	IHHO	ICSA-FS (Proposed)
Normal	90.8	93.8	95.8	97.2	97.8	99.2
DoS	83.7	90.2	91.5	91.9	94.3	98.6
Probe	83.2	85.9	86.7	90.7	93.7	97.3
R2L	81.6	87.6	85.9	90.1	94.4	97.4
U2R	84.7	86.8	88.6	92.6	92.7	98.2

FIGURE 9. F1-Score outcomes of ICSA-FS with other comparative models on NSL-KDD.



	LOF	SSA-FGWO	SSA-XGBoost	BSSA	IHHO	ICSA-FS (Proposed)
Normal	91.5	94.1	96.2	97.8	98.2	99.4
DoS	85.4	90.3	92.4	92.1	94.7	98.3
Probe	84.9	86.3	87.6	89.5	94.1	97.5
R2L	82.7	88.7	86.2	90.7	95.3	97.8
U2R	85.3	87.4	89.1	93.5	93.4	98.5

FIGURE 10. Accuracy outcomes of ICSA-FS with other comparative models on NSL-KDD.

computational complexity of ICSA is provided as follows:

$$O(ICSA) = O(I) + M_{iter} \times O(E) + O(U) \tag{10}$$

where the initialization complexity of $O(I)$ is measured as $O(P_s \times D)$, the evaluation complexity of $O(E)$ is determined based on the evaluation of a search agent $O(P_s)$ and the updating complexity of $O(U)$ is computed based on $O(M_{iter} \times P_s \times D)$.

V. EXPERIMENTATION AND RESULT ANALYSIS

A. EXPERIMENTAL ENVIRONMENT

The present study implements the ensemble model based on the proposed ICSA technique using the Python 3.8 software tool. The computational resources employed include a CPU with a clock speed of 3.4 GHz and 8 cores, along with 16GB of RAM. The processor utilized is an Intel Core i7. Furthermore, the implementation incorporates a range of

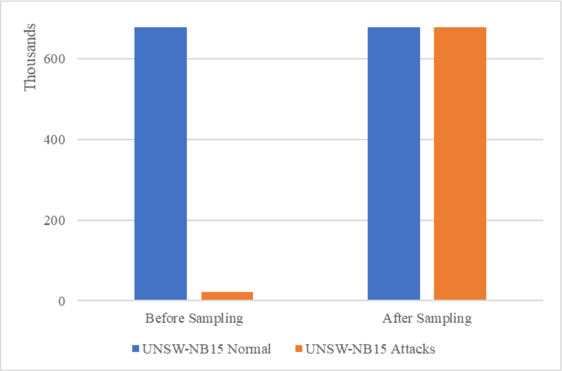


FIGURE 11. UNSW-NB15 Dataset before and after sampling.

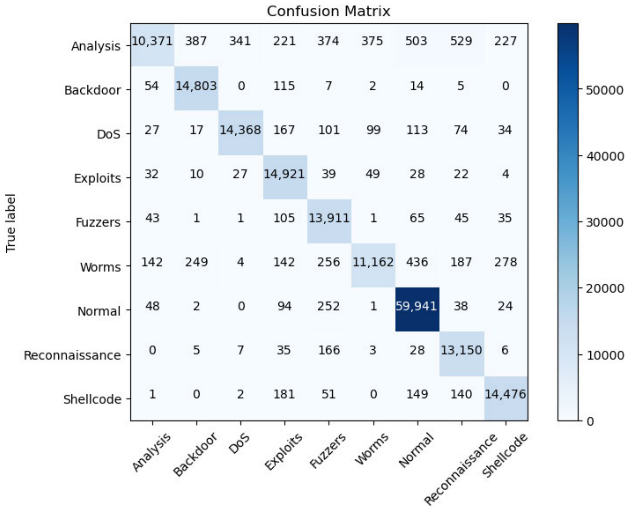


FIGURE 12. Convergence curve of proposed ICSA-FS with other compared models on UNSW-NB15.

libraries, including Numpy, Pandas, Keras, TensorFlow, and Scikit-Learn. On the contrary, MS Excel is employed to store both the original and derived datasets. The hyper-parameter values of the various classifiers used in the experimentation are presented in Table 2. On the other hand, the experimental settings of the proposed algorithm and various existing approaches are described in Table 3. The selected feature set by the proposed ICSA-FS model from the NSL-KDD and UNSW-NB15 datasets is presented in Table 4.

The proposed ICSA-FS approach is evaluated by assessing its performance using various system of measurement, including Precision (P), Recall (R), F1-Score, False Positive Rate (FPR), and Accuracy (ACC). Confusion matrices serve as valuable tools for facilitating direct comparisons between the outcome values of Tr_{+ve}, Fl_{+ve}, Tr_{-ve}, and Fl_{-ve}. The performance metrics can be mathematically formulated based on the confusion matrices.

Precision (P) – It is defined by dividing actual positive instances Tr_{+ve} with the sum of true positive instances Tr_{+ve} and false positive instances Fl_{+ve}. The mathematical expression of precision is given in Eq. (11).

$$P = \frac{Tr_{+ve}}{Tr_{+ve} + Fl_{+ve}} \tag{11}$$

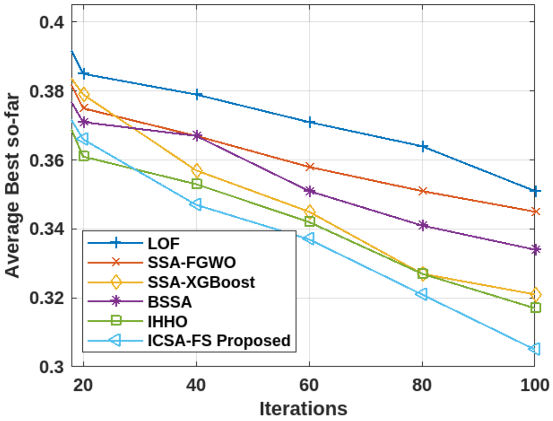


FIGURE 13. Confusion Matrix achieved by proposed ICSA-FS technique.

Recall (R) – It is defined as the ratio of true positive instances Tr_{+ve} and the sum of true positive instances Tr_{+ve} and false negative instances Fl_{-ve}. The mathematical formulation of recall is presented in Eq. (12).

$$R = \frac{Tr_{+ve}}{Tr_{+ve} + Fl_{-ve}} \tag{12}$$

Accuracy (ACC) is a significant metric widely used in classification tasks to measure the concert of a classifier. It is computed by dividing the number of accurate estimates by the overall number of estimates by the classifier. The mathematical expression of ACC is provided in Eq. (13).

$$ACC = \frac{Tr_{+ve} + Tr_{-ve}}{Tr_{+ve} + Tr_{-ve} + Fl_{+ve} + Fl_{-ve}} \tag{13}$$

F1-Score is determined as the average harmonic of P and R. The mathematical formulation of F1-Score is formulated in Eq. (14).

$$F1 - Score = \frac{P * R}{P + R} \tag{14}$$

B. RESULT ANALYSIS ON NSL-KDD

The data augmentation is performed on the NSL-KDD dataset to handle the class imbalance issue. The outcome of data augmentation is presented in Figure 4. The confusion matrix achieved by the proposed approach is presented in Figure 5. Later, the balanced dataset is provided as an input for the proposed model. Figure 6 illustrates the convergence curve of the proposed ICSA-FS with other compared models on NSL-KDD. In addition, Figures 7-10 detail the NSL-KDD database's multi-class classification outcomes on various existing models. Figures 7 and 8 illustrate the outcome of precision and recall rate of the proposed ICSA-FS model in comparison to the LOF, SSA-FGWO, SSA-XGBoost, BSSA, and IHHO. The ICSA-FS-based ensemble model that was developed has produced the highest classification result. The proposed classifier has achieved a better classification rank by effectively lowering the discrepancy and bias of the ML models in comparison to the individual classifiers. Using

TABLE 5. Recall and Precision outcome of ICSA-FS with other comparative models on UNSW-NB15.

Performance Metrics	Attack Type	LOF	SSA- FGWO	SSA- XGBoost	BSSA	IHHO	ICSA-FS (Proposed)
Recall (%)	Normal	91.5	89.7	91.2	93.4	95.6	99.1
	DoS	81.1	84.6	87.2	88.5	91.8	96
	Backdoor	59.8	62.1	65.6	68.8	72.2	82.4
	Exploits	73.1	74.9	77.9	78.6	83	85.6
	Reconnaissance	81.4	79.9	84.8	87.9	89	92
	Analysis	24.3	22.9	31.1	37.2	41.4	52.6
	Fuzzers	67.6	66.7	72	75.4	79.8	85.4
	Shellcode	51.2	50.1	55.5	58.9	74.1	84.7
	Worms	46.3	47.1	52.9	57	66.6	71.8
Precision (%)	Normal	94.1	93.4	95.3	96.1	96.8	99.3
	DoS	85.3	86.4	89.9	91.9	93.1	95.2
	Backdoor	63.4	64.2	68.5	72	74.2	82.1
	Exploits	75.2	76.9	80.4	84.1	86.6	87.3
	Reconnaissance	80.8	82.3	86.8	89.4	91.3	92.3
	Analysis	26.6	26	33.1	39.6	43.4	52.7
	Fuzzers	70.4	69.1	74.5	79.9	83.1	87.6
	Shellcode	53.8	53.3	60.4	57.8	75.9	83.5
	Worms	48.5	49.7	56.2	62.5	65.8	72.1

TABLE 6. F1-Score and Accuracy outcome of ICSA-FS with other comparative models on UNSW-NB15.

Performance Metrics	Attack Type	LOF	SSA- FGWO	SSA- XGBoost	BSSA	IHHO	ICSA-FS (Proposed)
F1-Score (%)	Normal	93.6	92.3	94	95.6	97	98.9
	DoS	83.9	86.3	89.4	91	92.8	95.1
	Backdoor	62.2	63.8	67.7	71.1	73.9	76.7
	Exploits	74.8	76.6	79.9	82.1	85.5	86.9
	Reconnaissance	81.9	81.9	86.6	89.5	90.9	92.1
	Analysis	25.9	24.9	32.6	45.9	52.9	54.4
	Fuzzers	69.7	68.6	73.9	78.4	82.2	87
	Shellcode	53.1	52.3	58.5	59	76.6	72.5
	Worms	48	49	55.1	60.3	66.8	71.3
Accuracy (%)	Normal	93.8	92.6	95	95.6	97.3	99.2
	DoS	84.8	86.6	89.6	91.8	93	97.4
	Backdoor	62.9	64.7	68.2	72.1	79.4	85
	Exploits	75	76.9	80	82.1	85.6	88.5
	Reconnaissance	82.1	82.4	86.8	89.5	91.7	94.9
	Analysis	26.5	25.4	33.2	39.9	53.8	54.7
	Fuzzers	69.8	69.2	74.1	78.4	82.7	91
	Shellcode	53.6	53.3	59.2	59.4	75.2	73.7
	Worms	48.9	49.9	55.4	60.6	67.1	72.2

distinct performance criteria, the developed ICSA-FS-based ensemble model's multi-class classification outcome on the NSL-KDD.

The proposed model attained the outcome of normal class 99.2%, DoS of 98.8%, Probe of 96.3%, R2L of 97.7% and U2R of 98.1% of recall values deliberates the proposed approach capacity to classify all positive occasions in all classes. In addition, the proposed model achieves 99.4%, 98.9%, 97.5%, 97.6%, and 98.5% of precision values indicating a high degree of accuracy in correctly identifying positive instances in the classes normal, DoS, probe, R2L, and U2R, as shown in Figure 7 and 8. Figure 7 and 8 also specifies the graphical representation of the multi-class classification result of the ICSA-FS based ensemble prototype that was constructed using recall and precision. The ICSA-FS based ensemble model in the multi-class classification required a restricted computing time of 39.7 sec, which is much less than compared models.

Based on Figures 9 and 10, it is clear that the ensemble model, which was created using the ICSA-FS, has done better at the multi-class classification task than other models that had been used before. The F1-measure, a metric that combines precision and recall, also reached an impressive value for the normal class of 99.2%, DoS of 98.6%, Probe of 97.3%, R2L of 97.4% and U2R of 98.2%. The accuracy of the model, which measures the overall correctness of predictions, was recorded for normal at 99.4%, DoS at 98.3%, Probe at 97.5%, R2L at 97.8% and U2R at 98.5%.

These outcomes collectively validate the high concert quality and effectiveness of the developed ICSA-FS-based ensemble approach on the NSL-KDD. The multi-class classification outcomes of F1-score and accuracy of the ICSA-FS-based ensemble approach are visually represented in Figures 9 and 10. These figures showcase the results obtained by employing various evaluation measures to assess the performance of the proposed approach. Furthermore, it is worth noting that the computational time required for the developed ICSA-FS-based ensemble model in the context of multi-class classification is notable less when compared to alternative models.

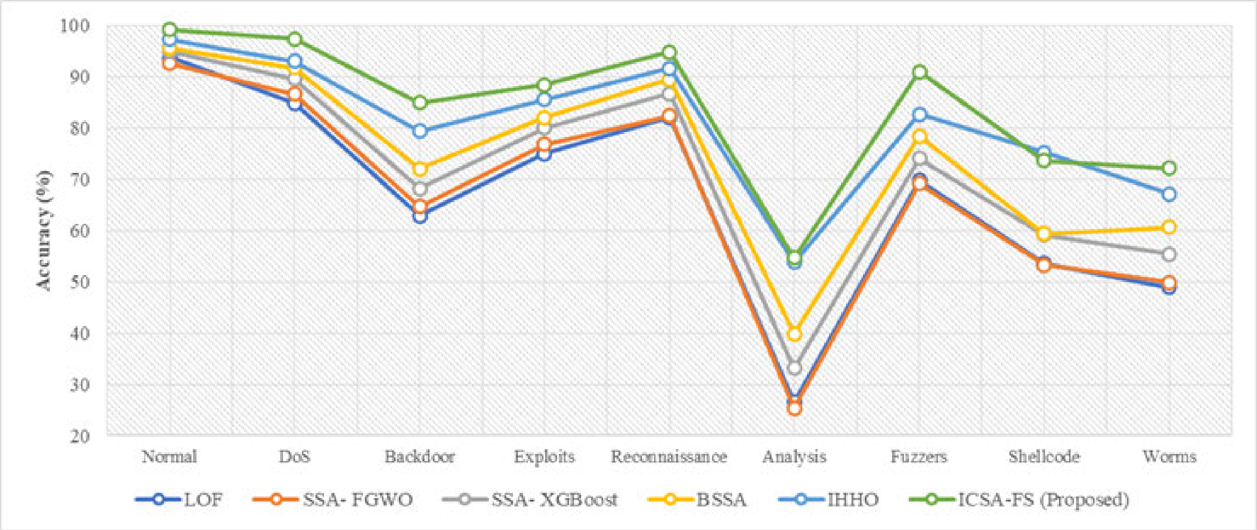
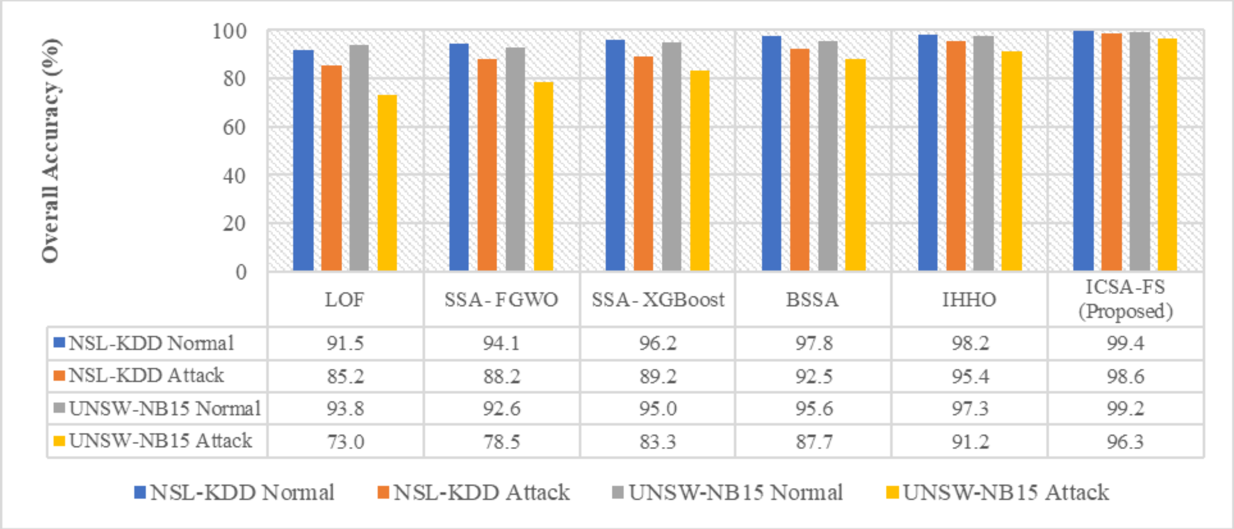


FIGURE 14. Accuracy of the proposed ICSA-FS model with other models on the UNSW-NB15.



	LOF	SSA- FGWO	SSA- XGBoost	BSSA	IHHO	ICSA-FS (Proposed)
■NSL-KDD Normal	91.5	94.1	96.2	97.8	98.2	99.4
■NSL-KDD Attack	85.2	88.2	89.2	92.5	95.4	98.6
■UNSW-NB15 Normal	93.8	92.6	95.0	95.6	97.3	99.2
■UNSW-NB15 Attack	73.0	78.5	83.3	87.7	91.2	96.3

FIGURE 15. Overall Accuracy of the proposed ICSA-FS model with other models on the NSL-KDD and UNSW-NB15 datasets.

C. RESULT ANALYSIS ON UNSW-NB15

The data augmentation is performed on the UNSW-NB15 dataset to handle the class imbalance issue. The outcome of data augmentation is presented in Figure 11. Figure 12 illustrates the convergence curve of proposed ICSA-FS with other compared models on UNSW-NB15. Figure 13 presents the confusion matrix that the suggested approach produced. Tables 5 and 6 display the multi-class classification outcomes of the ICSA-FS-based ensemble approach that was experimented on the UNSW-NB15. From Table 5, the ensemble model based on ICSA-FS has achieved a recall rate for normal of 99.1%, DoS of 96.0%, Backdoor of 75.4%, exploits of 85.6%, reconnaissance of 92%, analysis of 49.6%, fuzzers of 85.4%, shellcode of 70.7% and worms of 68.8%; these results are noticeably better than those of the compared models. In addition, Table 5 provides the precision score of multi-class classification by the proposed model and other compared models. It is noticed that the ensemble model based on ICSA-FS has achieved a precision score for normal of 99.3%, DoS of 95.2%, backdoor of 77.1%, exploits of 87.3%, reconnaissance of 92.3%, analysis of 48.7%, fuzzers of 87.6%, shellcode of 73.5%, and worms of 73.1%.

From Table 6, it has been observed that the ensemble model, which was developed using the ICSA-FS, has demonstrated superior performance in the multi-class classification task compared to previously established models. The F1-measure, a metric that combines precision and recall, also reached an impressive value for normal class of 98.9%, DoS of 95.1%, Backdoor of 76.7%, exploits of 86.9%, reconnaissance of 92.1%, analysis of 49.4%, fuzzers of 87%, shellcode of 72.5% and worms of 71.3%. The accuracy of the model, which measures the overall correctness of predictions, was recorded for normal class of 99.2%, DoS of 97.4%, Backdoor of 80%, exploits of 88.5%, reconnaissance of 94.9%, analysis of 54.7%, fuzzers of 91%, shellcode of 76.7% and worms of 75.2%. Figure 14 provides the graphical representation of accuracy achieved by proposed model and other compared models.

The ICSA-FS in this study uses arbitrary numbers determined by the swarming crows' global communication. The ideal qualities for IDs are selected more effectively by the meta-heuristic optimizers, such as ICSA when it comes to multi-objective optimization. The ensemble classifier's computational cost and time are greatly decreased by choosing the best attributes.

D. DISCUSSION

The comparative outcomes of the proposed approach associated with the preceding approaches are illustrated in Figure 15. The experimental investigation that was conducted provides evidence to support the efficacy of the newly developed ICSA-FS ensemble model in addressing the challenges associated with dimensionality reduction and outlier detection. The detection accuracy of the approach on the NSL-KDD database has been observed to be 99.4% for normal and 98.6% for attack classes. The work by Boukela et al. [55] presented a novel approach that involved a modified local outlier factor. The LOF model achieved an accuracy of normal 91.5% and an attack of 85.2% for NSL-KDD. Similarly, for UNSW-NB15, the LOF model achieved an accuracy of normal of 93.8% and an attack of 73%, respectively. The SSA-FGWO proposed by Qaraad et al. [56] achieved an accuracy for NSL-KDD of 94.1% for normal and 88.2% for attack class. In addition, SSA-FGWO achieved an accuracy for UNSW-NB15 of 92.6% for normal and 78.5% for attack class.

Shekhawat et al. [58] introduced the BSSA model, which demonstrated high accuracy in classifying normal and attack classes. Specifically, the model reached an accuracy of 97.8% for normal class and 92.5% for attack class. Additionally, on UNSW-NB15, the BSSA model produced accuracy's of 95.6% for normal class and 87.7% for attack class. In their study, Hussien et al. [59] introduced the IHHO model, which demonstrated an accuracy rate of 98.2% for normal class and 95.4% for attack class. Similarly, on UNSW-NB15, the IHHO model attained an accuracy of 97.3% for normal class and 91.2% for attack class.

VI. CONCLUSION AND FUTURE WORK

This research presents a novel ensemble approach called ICSA-FS for IDS in the IoT context. The deployment and implementation of the ICSA-FS based ensemble model involve using benchmark databases, specifically NSL-KDD and UNSW-NB15. The challenges posed by data unbalancing and computational complexity have been effectively addressed by utilizing MADASYN sampling approach and incorporating a MinMax scalar. Moreover, the model introduced in this study effectively utilizes the advantages of the ICSA algorithm to reduce the feature dimensions. This reduction in feature dimensions is crucial in reducing the computational and training time required for the model. The achievement of multi-class classifications is facilitated by using an ensemble classifier. The present study involves conducting an experimental investigation of the ICSA-based ensemble model. This investigation entails the utilization of various evaluation metrics to ensure the accuracy of the proposed model. As outlined in the outcome discussion section, the ensemble model based on ICSA-FS demonstrated detection accuracy's of 99.4% for the NSL-KDD and 99.2% for the UNSW-NB15 datasets. These results surpass existing models such as LOF, SSA-FGWO, SSA-XGBoost, BSSA, and IH-HO. Furthermore, it is worth noting that the developed ICSA-FS based ensemble model provides less computation time than the comparative approaches. One limitation of the ICSA-FS based ensemble model is its exclusive deployment in online databases. Hence-forth, to expand upon the present study, it is recommended that the CSA-FS based ensemble model can be applied to various real-time intrusion databases to conduct a more comprehensive assessment of its performance.

ACKNOWLEDGMENT

The authors extend their appreciation to King Saud University for funding this research through Researchers Supporting Project Number (RSPD2024R1027), King Saud University, Riyadh, Saudi Arabia.

REFERENCES

[1] V. Kumar, A. K. Das, and D. Sinha, "UIDS: A unified intrusion detection system for IoT environment," *Evol. Intell.*, vol. 14, no. 1, pp. 47–59, Sep. 2019, doi: 10.1007/s12065-019-00291-w.

[2] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M. A. Latif, F. Al-Turjman, and L. Mostarda, "Cyber security threats detection in Internet of Things using deep learning approach," *IEEE Access*, vol. 7, pp. 124379–124389, 2019, doi: 10.1109/ACCESS.2019.2937347.

[3] I. Lee, "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management," *Future Internet*, vol. 12, no. 9, p. 157, Sep. 2020, doi: 10.3390/fi12090157.

[4] A. Tabassum, A. Erbad, and M. Guizani, "A survey on recent approaches in intrusion detection system in IoTs," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf.*, Jun. 2019, pp. 1190–1197, doi: 10.1109/iwcmc.2019.8766455.

[5] Y. K. Saheed, A. I. Abiodun, S. Misra, M. K. Holone, and R. Colomo-Palacios, "A machine learning-based intrusion detection for detecting Internet of Things network attacks," *Alexandria Eng. J.*, vol. 61, no. 12, pp. 9395–9409, Dec. 2022, doi: 10.1016/j.aej.2022.02.063.

[6] R. Rajakumar, K. Dinesh, A. Dumka, and L. Jayakumar, "RFA reinforced firefly algorithm to identify optimal feature subsets for network IDS," *Int. J. Grid High Perform. Comput.*, vol. 12, no. 3, pp. 68–87, Jul. 2020, doi: 10.4018/ijghpc.2020070105.

[7] M. T. Nguyen and K. Kim, "Genetic convolutional neural network for intrusion detection systems," *Future Gener. Comput. Syst.*, vol. 113, pp. 418–427, Dec. 2020, doi: 10.1016/j.future.2020.07.042.

[8] H. Jiang, Z. He, G. Ye, and H. Zhang, "Network intrusion detection based on PSO-XGBoost model," *IEEE Access*, vol. 8, pp. 58392–58401, 2020, doi: 10.1109/ACCESS.2020.2982418.

[9] S. K. Prashanth, H. Iqbal, and B. Illuri, "An enhanced grey wolf optimisation-deterministic convolutional neural network (GWO–DCNN) model-based IDS in MANET," *J. Inf. Knowl. Manag.*, vol. 22, no. 4, Mar. 2023, doi: 10.1142/s0219649223500107.

[10] S. Narayanasami, S. Sengan, S. Khurram, F. Arslan, S. K. Murugaiyan, R. Rajan, V. Peroumal, A. K. Dubey, S. Srinivasan, and D. K. Sharma, "Biological feature selection and classification techniques for intrusion detection on BAT," *Wireless Pers. Commun.*, vol. 127, no. 2, pp. 1763–1785, Jul. 2021, doi: 10.1007/s11277-021-08721-8.

[11] N. Devarakonda, S. Anandarao, and R. Kamarajugadda, ''Detection of intruder using the improved dragonfly optimization algorithm,'' *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 1074, no. 1, Feb. 2021, Art. no. 012011, doi: 10.1088/1757-899x/1074/1/012011.

[12] S. K. Shandilya, B. J. Choi, A. Kumar, and S. Upadhyay, ''Modified firefly optimization algorithm-based IDS for nature-inspired cybersecurity,'' *Processes*, vol. 11, no. 3, p. 715, Feb. 2023, doi: 10.3390/pr11030715.

[13] L. Haghnegahdar and Y. Wang, ''A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection,'' *Neural Comput. Appl.*, vol. 32, no. 13, pp. 9427–9441, Aug. 2019, doi: 10.1007/s00521-019-04453-w.

[14] H. Alazzam, A. Sharieh, and K. E. Sabri, ''A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer,'' *Exp. Syst. Appl.*, vol. 148, Jun. 2020, Art. no. 113249, doi: 10.1016/j.eswa.2020.113249.

[15] B. Hajimirzaei and N. J. Navimipour, ''Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm,'' *ICT Exp.*, vol. 5, no. 1, pp. 56–59, Mar. 2019.

[16] N. Khare, P. Devan, C. Chowdhary, S. Bhattacharya, G. Singh, S. Singh, and B. Yoon, ''SMO-DNN: Spider monkey optimization and deep neural network hybrid classifier model for intrusion detection,'' *Electronics*, vol. 9, no. 4, p. 692, Apr. 2020, doi: 10.3390/electronics9040692.

[17] A. Askarzadeh, ''A novel metaheuristic method for solving constrained engineering optimization problems: Crow search algorithm,'' *Comput. Struct.*, vol. 169, pp. 1–12, Jun. 2016, doi: 10.1016/j.compstruc.2016.03.001.

[18] Z. Shi, Q. Li, S. Zhang, and X. Huang, ''Improved crow search algorithm with inertia weight factor and roulette wheel selection scheme,'' in *Proc. 10th Int. Symp. Comput. Intell. Design (ISCID)*, Dec. 2017, pp. 205–209, doi: 10.1109/iscid.2017.140.

[19] G. I. Sayed, A. E. Hassanien, and A. T. Azar, ''Feature selection via a novel chaotic crow search algorithm,'' *Neural Comput. Appl.*, vol. 31, no. 1, pp. 171–188, Apr. 2017, doi: 10.1007/s00521-017-2988-6.

[20] S. Ouadfel and M. Abd Elaziz, ''Enhanced crow search algorithm for feature selection,'' *Exp. Syst. Appl.*, vol. 159, Nov. 2020, Art. no. 113572, doi: 10.1016/j.eswa.2020.113572.

[21] S. Dwivedi, M. Vardhan, S. Tripathi, and A. K. Shukla, ''Implementation of adaptive scheme in evolutionary technique for anomaly-based intrusion detection,'' *Evol. Intell.*, vol. 13, no. 1, pp. 103–117, Sep. 2019, doi: 10.1007/s12065-019-00293-8.

[22] Y. Li, Y. Xu, Z. Liu, H. Hou, Y. Zheng, Y. Xin, Y. Zhao, and L. Cui, ''Robust detection for network intrusion of industrial IoT based on multi-CNN fusion,'' *Measurement*, vol. 154, Mar. 2020, Art. no. 107450, doi: 10.1016/j.measurement.2019.107450.

[23] P. Tao, Z. Sun, and Z. Sun, ''An improved intrusion detection algorithm based on GA and SVM,'' *IEEE Access*, vol. 6, pp. 13624–13631, 2018, doi: 10.1109/ACCESS.2018.2810198.

[24] N. Kunhare, R. Tiwari, and J. Dhar, ''Particle swarm optimization and feature selection for intrusion detection system,'' *Sādhanā*, vol. 45, no. 1, pp. 1–14, May 2020, doi: 10.1007/s12046-020-1308-5.

[25] M. Ramaiah, V. Chandrasekaran, V. Ravi, and N. Kumar, ''An intrusion detection system using optimized deep neural network architecture,'' *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 4, p. e4221, Feb. 2021, doi: 10.1002/ett.4221.

[26] J. Chen, X. Qi, L. Chen, F. Chen, and G. Cheng, ''Quantum-inspired ant lion optimized hybrid k-means for cluster analysis and intrusion detection,'' *Knowl.-Based Syst.*, vol. 203, Sep. 2020, Art. no. 106167, doi: 10.1016/j.knosys.2020.106167.

[27] Z. Wang, Y. Zeng, Y. Liu, and D. Li, ''Deep belief network integrating improved kernel-based extreme learning machine for network intrusion detection,'' *IEEE Access*, vol. 9, pp. 16062–16091, 2021, doi: 10.1109/ACCESS.2021.3051074.

[28] X. Kan, Y. Fan, Z. Fang, L. Cao, N. N. Xiong, D. Yang, and X. Li, ''A novel IoT network intrusion detection approach based on adaptive particle swarm optimization convolutional neural network,'' *Inf. Sci.*, vol. 568, pp. 147–162, Aug. 2021, doi: 10.1016/j.ins.2021.03.060.

[29] H. Alazzam, A. Sharieh, and K. E. Sabri, ''A lightweight intelligent network intrusion detection system using OCSVM and pigeon inspired optimizer,'' *Int. J. Speech Technol.*, vol. 52, no. 4, pp. 3527–3544, Jul. 2021, doi: 10.1007/s10489-021-02621-x.

[30] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, ''A bidirectional LSTM deep learning approach for intrusion detection,'' *Exp. Syst. Appl.*, vol. 185, Dec. 2021, Art. no. 115524, doi: 10.1016/j.eswa.2021.115524.

[31] V. Tomer and S. Sharma, ''Detecting IoT attacks using an ensemble machine learning model,'' *Future Internet*, vol. 14, no. 4, p. 102, Mar. 2022, doi: 10.3390/fi14040102.

[32] W. Xu, J. Jang-Jaccard, A. Singh, Y. Wei, and F. Sabrina, ''Improving performance of autoencoder-based network anomaly detection on NSL-KDD dataset,'' *IEEE Access*, vol. 9, pp. 140136–140146, 2021, doi: 10.1109/ACCESS.2021.3116612.

[33] H. Azzaoui, A. Z. E. Boukhamla, D. Arroyo, and A. Bensayah, ''Developing new deep-learning model to enhance network intrusion classification,'' *Evolving Syst.*, vol. 13, no. 1, pp. 17–25, Jan. 2021, doi: 10.1007/s12530-020-09364-z.

[34] A. Dahou, M. Abd Elaziz, S. A. Chelloug, M. A. Awadallah, M. A. Al-Betar, M. A. A. Al-Qaness, and A. Forestiero, ''Intrusion detection system for IoT based on deep learning and modified reptile search algorithm,'' *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–15, Jun. 2022, doi: 10.1155/2022/6473507.

[35] M. Nour, M. Awad, M. Kamel, M. Essa, and N. Abdelbaki, ''Anomaly detection using unsupervised learning in LTE mobile network,'' in *Proc. 10th Int. Conf. Intell. Comput. Inf. Syst. (ICICIS)*, Dec. 2021, pp. 195–199, doi: 10.1109/icicis52592.2021.9694214.

[36] M. H. L. Louk and B. A. Tama, ''Exploring ensemble-based class imbalance learners for intrusion detection in industrial control networks,'' *Big Data Cognit. Comput.*, vol. 5, no. 4, p. 72, Dec. 2021, doi: 10.3390/bdcc5040072.

[37] A. A. Aburomman and M. B. Ibne Reaz, ''A novel SVM-kNN-PSO ensemble method for intrusion detection system,'' *Appl. Soft Comput.*, vol. 38, pp. 360–372, Jan. 2016, doi: 10.1016/j.asoc.2015.10.011.

[38] S. Sarvari, N. F. Mohd Sani, Z. M, Hanapi, and M. T. Abdullah, ''An efficient anomaly intrusion detection method with feature selection and evolutionary neural network,'' *IEEE Access*, vol. 8, pp. 70651–70663, 2020, doi: 10.1109/ACCESS.2020.2986217.

[39] Q. Ma, C. Sun, B. Cui, and X. Jin, ''A novel model for anomaly detection in network traffic based on kernel support vector machine,'' *Comput. Secur.*, vol. 104, May 2021, Art. no. 102215, doi: 10.1016/j.cose.2021.102215.

[40] J. Camacho, R. Therón, J. M. García-Giménez, G. Maciá-Fernández, and P. García-Teodoro, ''Group-wise principal component analysis for exploratory intrusion detection,'' *IEEE Access*, vol. 7, pp. 113081–113093, 2019, doi: 10.1109/ACCESS.2019.2935154.

[41] M. A. Ambusaidi, X. He, Z. Tan, P. Nanda, L. Lu, and U. T. Nagar, ''A novel feature selection approach for intrusion detection data classification,'' in *Proc. IEEE 13th Int. Conf. Trust, Security Privacy Comput. Commun.*, Sep. 2014, pp. 82–89, doi: 10.1109/trustcom.2014.15.

[42] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, ''Building an efficient intrusion detection system based on feature selection and ensemble classifier,'' *Comput. Netw.*, vol. 174, Jun. 2020, Art. no. 107247, doi: 10.1016/j.comnet.2020.107247.

[43] S. Roy, J. Li, B.-J. Choi, and Y. Bai, ''A lightweight supervised intrusion detection mechanism for IoT networks,'' *Future Gener. Comput. Syst.*, vol. 127, pp. 276–285, Feb. 2022, doi: 10.1016/j.future.2021.09.027.

[44] X. Zhang, F. Yang, Y. Hu, Z. Tian, W. Liu, Y. Li, and W. She, ''RANet: Network intrusion detection with group-gating convolutional neural network,'' *J. Netw. Comput. Appl.*, vol. 198, Feb. 2022, Art. no. 103266, doi: 10.1016/j.jnca.2021.103266.

[45] V. R. S. Dora and V. N. Lakshmi, ''Optimal feature selection with CNN-feature learning for DDoS attack detection using meta-heuristic-based LSTM,'' *Int. J. Intell. Robot. Appl.*, vol. 6, no. 2, pp. 323–349, Jan. 2022, doi: 10.1007/s41315-022-00224-4.

[46] M. Otair, O. T. Ibrahim, L. Abualigah, M. Altalhi, and P. Sumari, ''An enhanced grey wolf optimizer based particle swarm optimizer for intrusion detection system in wireless sensor networks,'' *Wireless Netw.*, vol. 28, no. 2, pp. 721–744, Jan. 2022, doi: 10.1007/s11276-021-02866-x.

[47] S. S. Shankar, B. T. Hung, P. Chakrabarti, T. Chakrabarti, and G. Parasa, ''A novel optimization based deep learning with artificial intelligence approach to detect intrusion attack in network system,'' *Educ. Inf. Technol.*, vol. 29, no. 3, pp. 1–25, Jun. 2023, doi: 10.1007/s10639-023-11885-4.

[48] R. Gangula, M. M. Vutukuru, and M. Ranjeeth Kumar, ''Intrusion attack detection using firefly optimization algorithm and ensemble classification model,'' *Wireless Pers. Commun.*, vol. 132, no. 3, pp. 1899–1916, Oct. 2023.

[49] S. Meftah, T. Rachidi, and N. Assem, ''Network based intrusion detection using the UNSW-NB15 dataset,'' *Int. J. Comput. Digit. Syst.*, vol. 8, no. 5, pp. 477–487, Jan. 2019.

[50] C.-J. Lin and F. Leony, "Evidence-based adaptive oversampling algorithm for imbalanced classification," *Knowl. Inf. Syst.*, vol. 66, no. 3, pp. 2209–2233, Mar. 2024.

[51] L. Munkhdalai, T. Munkhdalai, K. H. Park, H. G. Lee, M. Li, and K. H. Ryu, "Mixture of activation functions with extended min–max normalization for forex market prediction," *IEEE Access*, vol. 7, pp. 183680–183691, 2019, doi: 10.1109/ACCESS.2019.2959789.

[52] S. Mirjalili and A. Lewis, "S-shaped versus V-shaped transfer functions for binary particle swarm optimization," *Swarm Evol. Comput.*, vol. 9, pp. 1–14, Apr. 2013.

[53] B. Samieiyan, P. MohammadiNasab, M. A. Mollaei, F. Hajizadeh, and M. Kangavari, "Novel optimized crow search algorithm for feature selection," *Exp. Syst. Appl.*, vol. 204, Oct. 2022, Art. no. 117486.

[54] A. Sampathkumar, R. Maheswar, P. Harshavardhanan, S. Murugan, P. Jayarajan, and V. Sivasankaran, "Majority voting based hybrid ensemble classification approach for predicting parking availability in smart city based on IoT," in *Proc. 11th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2020, pp. 1–8.

[55] L. Boukela, G. Zhang, M. Yacoub, S. Bouzefrane, S. B. B. Ahmadi, and H. Jelodar, "A modified LOF-based approach for outlier characterization in IoT," *Ann. Telecommun.*, vol. 76, nos. 3–4, pp. 145–153, Apr. 2021.

[56] M. Qaraad, S. Amjad, N. K. Hussein, and M. A. Elhosseini, "Large scale salp-based grey wolf optimization for feature selection and global optimization," *Neural Comput. Appl.*, vol. 34, no. 11, pp. 8989–9014, Jun. 2022.

[57] A. Alsaleh and W. Binsaeedan, "The influence of salp swarm algorithm-based feature selection on network anomaly intrusion detection," *IEEE Access*, vol. 9, pp. 112466–112477, 2021.

[58] S. S. Shekhawat, H. Sharma, S. Kumar, A. Nayyar, and B. Qureshi, "BSSA: Binary salp swarm algorithm with hybrid data transformation for feature selection," *IEEE Access*, vol. 9, pp. 14867–14882, 2021.

[59] A. G. Hussien and M. Amin, "A self-adaptive Harris hawks optimization algorithm with opposition-based learning and chaotic local search strategy for global optimization and feature selection," *Int. J. Mach. Learn. Cybern.*, vol. 13, no. 2, pp. 309–336, Feb. 2022.

D. JAYALATCHUMY received the B.Tech., M.Tech., and Ph.D. degrees in computer science and engineering from PEC, Pondicherry University, Pondicherry, India, in 2004, 2008, and 2018, respectively. She joined the Perunthalaivar Kamarajar Institute of Engineering and Technology, (PKIET), a Government Institute at Karaikal, India, in 2009, where she is currently an Assistant Professor in computer science and engineering. She has more than 14 years of experience teaching undergraduate students. Her research interests include data mining, big data, and data structures. She has published many research papers in international conferences and journals. She has also published many chapters in Springer books series. She is a Life Member of Indian Society for Technical Education and International Association of Engineers.

RAJAKUMAR RAMALINGAM received the Bachelor of Technology, Master of Technology, and Ph.D. degrees in computer science and engineering from Pondicherry Central University, Pondicherry, in 2012, 2014, and 2019, respectively. He is currently an Associate Professor with the Centre for Automation, SCOPE, Vellore Institute of Technology, Chennai, Tamil Nadu, India. He has published 37 research papers in reputed SCI and Scopus indexed journals and conferences. He is a guest editor/reviewer for various international journals. His current research interests include optimization algorithms, wireless senor networks, artificial intelligence, and network security.

ARAVIND BALAKRISHNAN received the Bachelor of Engineering and Master of Engineering degrees in computer science and engineering from Anna University, Chennai, in 2010 and 2013, respectively, and the Ph.D. degree in computer science and engineering from Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India, in 2022. He is currently an Assistant Professor with the Department of Computer Science and Technology, Madanapalle, Andhra Pradesh, India. He has published more than ten papers in reputed SCI, Scopus, UGC care journals, and conferences. His research interests include network security and artificial intelligence.

MEJDL SAFRAN received the bachelor's degree in computer science from King Saud University (KSU), in 2007, and the master's and Ph.D. degrees in computer science from Southern Illinois University, Carbondale, in 2013 and 2018, respectively. His doctoral dissertation was on developing efficient learning-based recommendation algorithms for top-N tasks and top-N workers in large-scale crowdsourcing systems. He is currently an Assistant Professor in computer science with KSU, where he has been a Faculty Member, since 2008. He is also a passionate Researcher and an Educator in the field of artificial intelligence, with a focus on deep learning and its applications in various domains. He has published more than 20 papers in peer-reviewed journals and conference proceedings, such as *ACM Transactions on Information Systems*, *Applied Computing and Informatics*, *Mathematics*, *Sustainability*, *International Journal of Digital Earth*, IEEE Access, *Biomedicine, Sensors*, IEEE International Conference on Cluster, IEEE International Conference on Computer and Information Science, International Conference on Database Systems for Advanced Applications, and International Conference on Computational Science and Computational Intelligence. He has been leading grant projects in the fields of AI in medical imaging and AI in smart farming. His current research interests include developing novel deep learning methods for image processing, pattern recognition, natural language processing, and predictive analytics, and modeling and analyzing user behavior and interest in online platforms. He has been working as an AI Consultant for several national and international agencies, since 2018.

SULTAN ALFARHOOD received the Ph.D. degree in computer science from the University of Arkansas. He is currently an Assistant Professor with the Department of Computer Science, King Saud University (KSU). Since joining KSU, in 2007, he has made several contributions to the field of computer science through his research and publications. His research interests include a variety of domains, including machine learning, recommender systems, linked open data, text mining, and ML-based IoT systems. His work includes proposing innovative approaches and techniques to enhance the accuracy and effectiveness of these systems. His recent publications have focused on using deep learning and machine learning techniques to address challenges in these domains. His research continues to make significant contributions to the field of computer science and machine learning. His work has been published in several high-impact journals and conferences.