Parameter Optimization in a Convolutional Neural Network for Cyberattacks Detection

Maymouna M. Shbail[1†] , Khaled Batiha [1†] and Wafa Alshatafat [2†]

[1†] Department of Computer Science, Al al-Bayt University, Mafraq, Jordan
[2†]Department of Information Systems, Al al-Bayt University, Mafraq, Jordan

Abstract
The rapid evolution of cyber threats poses significant challenges to traditional detection methods, which often lag in identifying advanced attacks and suffer from high false-positive rates. This paper integrated advanced optimization techniques and machine learning to enhance the accuracy and efficiency of intrusion detection systems (IDS). Specifically, it leverages the Jaya optimization algorithm to tune the hyperparameters of convolutional neural networks (CNNs) and support vector machines (SVMs) to detect cyber-attacks, particularly in innovative grid environments. Using the dataset UNSW-NB 15, the accuracy ratio was 99.7%. This paper addressed issues such as feature filtration and model interpretability. The proposed framework, JAYA-CNN-SVM, significantly improved classification accuracy and achieved robust detection across various attack types. The results confirm the effectiveness of the Jaya optimization in overcoming the limitations of traditional tuning methods, representing a step forward in reliable and real-time cybersecurity defenses.

Keywords:
Convolutional Neural Networks, Feature Filtration, JAYA algorithm, Support Vector Machines.

1. Introduction

Cybersecurity events, from man-made to natural catastrophes, are becoming increasingly hazardous to businesses, organizations, and governments. In these situations, intruders use tools to carry out operations, leading to unlawful outcomes that fulfill attackers' goals [1]. Enterprise networks and the Internet are essential for business and economic advancement, and cyberattacks are becoming increasingly frequent. Security experts and technicians have focused on spotting threats. Both public and commercial institutions require robust solutions to safeguard information assets and prevent incursions. Systems that detect intrusions focus on network traffic [1]. Computer networks are vital in the digital age for enterprises to convey sensitive data; therefore, protecting them against intrusion and attack is critical. Because machine-learning techniques can quickly assess data and react to changing threats, they are more advanced in identifying and preventing breaches. Network security relies heavily on intrusion detection systems (IDS), which monitor networks and analyze data to identify anomalous or hostile activities [2]. They have historically relied on anomaly- or signature-based detection, but they have difficulty identifying novel and sophisticated attacks that might not match known signatures or may be overly complicated [2].

Scientists have examined many applications and used machine-learning techniques to identify malicious programs and applications [3]. However, because each program's encryption is constantly different, it can be challenging to identify cyber-attacks. Because similar dangerous files are easily changed and pose a risk, machine learning is the most effective way to identify them [3].
Increased risk: Cyberattacks can spread quickly through flash devices and hard disks, causing significant damage. Cyber-attacks are found using various methods that allow dynamic and static scanning of file representations and content requirements. Establishing detection technologies is essential to achieving high accuracy in identifying hazardous applications, regardless of the difficulties [4].
Dr. Ravi developed innovative Jaya Technology in 2016, identifying minors' gadgets [4]. The Jaya method, which is based on evolutionary optimization, determines the optimal financial and loss solutions without requiring additional parameters, thus enhancing the existing solutions. For optimal results, this approach integrates random selection and iterations [5].

Vladimir Vapnik and Alex Chervonenkis developed a well-known machine learning method called the Support Vector Machine (SVM) in the early 1990s [6]. It is primarily used for regression and classification tasks; it can manage high-dimensional data and perform effectively, even with overlapping classes. SVM seeks to find a linear or non-linear separator that divides data classes by the most significant margin. For linearly separable data, the method can be divided into a linear separator (hyperplane) and a nonlinear separator (Kernel Trick) for non-linear data [6].
Text search, financial forecasting, pattern recognition, and image classification extensively utilize CNNs. The CNN

Manuscript received May 5, 2026
Manuscript revised May 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.5.1

process involves several steps: data preparation, kernel selection, training, evaluation, and parameter fine-tuning. CNNs offer significant advantages, including their effectiveness in handling dimensionality, accuracy, computational efficiency, and generalization capabilities [7].

However, it may be less successful if the categories are significantly imbalanced and computationally intensive, involving large datasets. The model needs to be fine-tuned to ensure optimal performance, and appropriate parameters must be selected for training and testing. In conclusion, the CNN is a versatile deep-learning tool primarily used for classification [8]. However, to achieve optimal performance, one must select appropriate parameters and optimize the model [7].

Jaya developed a CNN-based technology that enhanced the effectiveness and precision of network intrusion detection by utilizing both optimization and classification knowledge. This reduces the likelihood of cyber-attacks and fortifies network security.

This paper presents an innovative method for detecting intrusions in a network environment and utilizes an established dataset, namely UNSW-NB15, to perform a comprehensive evaluation. The many significant contributions of the proposed model are as follows:

- The Jaya optimization algorithm optimizes parameters for CNN.
- A feature filtration procedure is implemented to identify the most relevant features while tackling issues associated with dimensionality reduction. This technique ultimately boosts computing efficiency and enhances model performance.
- The proposed approach utilizes an artificial algorithm, namely the JAYA algorithm, a CNN, and an SVM to enhance attack classification.
- A comprehensive performance evaluation was conducted using UNSW-NB15 dataset. Various evaluation metrics, such as accuracy, precision, recall, and F1-score, were used to assess the proposed model's effectiveness in detecting network attacks. In addition, comparisons with recent papers published on the same datasets are presented.

2. Related Work

Cyberattack detection issues using hyperparameter optimization of support vector machines (SVM) include the computational cost and adaptability to evolving threats. Large datasets require the evaluation of multiple hyperparameter settings, and flexible models are necessary because of the dynamic nature of cyberattacks [8]. Future work will concentrate on designing efficient optimization techniques to optimize the trade-off between detection accuracy and computational expense, and linking hyperparameter selection with machine learning methods such as ensemble learning and deep learning [7]. It is crucial to state that these aspects should evolve in terms of cyber threat models and strategies for improving the detection model used by a system. This optimizes the hyperparameters, which are crucial in most machine-learning algorithms for better outcomes in complex tasks, including cyberattack detection [9]. Considerable research has been conducted on the use of support vector machines (SVMs), convolutional neural networks (CNNs), and the Jaya method in binary classification problems [10]. To achieve high accuracy and good generalization, hyperparameter training should encompass regularization parameters, the type of kernel used, and the parameters involved.

These hyperparameters are tuned using several methods, including grid search, random search, and Bayesian optimization. Therefore, improvements in support vector machines that distinguish malicious communication from benign communication have resulted in significantly better detection of cyberattacks [11]. In machine learning, the Jaya algorithm is a metaheuristic optimization technique that converts the least effective solutions into the most effective solutions. This is because of the lack of speed, simplicity, and hyperparameters for the algorithms used to identify cyberattacks. Using Jaya, researchers can modify the hyperparameter set of a dynamic neural network (CNN) and support a vector machine (SVM), thereby reducing false positives and improving detection rates. For CNN, the hyperparameter adjustment process requires the following parameters: architecture, batch size, learning rate, and other parameters. Fine-tuned CNNs can extend conventional approaches because they can recognize complex patterns related to the realization of cybercrime [12].

Security methods that involve multiple layers of protection are called Security in Depth (DiD) and include firewalls, IDS, antivirus, IPS, and encryption. In addition, patch management, continuous monitoring, access control, training, and security awareness are available [13]. This strategy reduces the likelihood that cyberattacks will succeed. It helps identify, prevent, or mitigate cyber threats and reduces the impact of breaches on organizations. Regular security assessments and additional enhancements ensure that the system remains in line with emerging threats [13].

A conceptual outline and detailed description of each component are included in a diagram illustrating how to enhance the hyperparameters for cyberattack detection using traditional machine learning and deep learning techniques [14].

In [15], JAYA was used as an electricity theft detection system utilizing a Jaya-optimal XGBoost

classifier. The Robust-SMOTE technique is adopted to address the dataset imbalance and oversampling, followed by XGBoost for categorizing customers into ‘Honest’ and 'Fraudster.' The model achieves the most remarkable effectiveness, efficiency, and reliability compared to the other investigated approaches while being repurposed under the minimal computational load to retrain. The findings of the present work show that the proposed approach for theft detection performs the best among all the techniques discussed, as it has the highest accuracy (93.38%), precision (95%), and recall (93.18%). Demonstrating its relevance to the research area.

The widespread use of Internet services and applications has led to increased cyberattacks and the spread of illegal applications [16]. Despite implementing dimensionality reduction and biologically inspired algorithms to improve efficiency, IDS is still used to detect anomalous traffic behavior. The enhanced capability of the IDS to distinguish between normal and abnormal traffic is facilitated by the updated Grey Wolf Optimization (GWO) algorithm. Applying this method while using the UNSWNB-15 dataset, it performed better than the other meta-algorithms; it had an accuracy of 81%, an F1 score of 78%, and a G-mean of 84%.

A novel ID technique was proposed [17] using multi-class classification with a support vector machine (SVM), modified JAYA algorithm (MJAYA), and altered learning-based optimization (MTLBO). The MTLBO algorithm learns subsets of features without compromising prediction quality in supervised learning. The modified JAYA approach improves the parameters C and Gamma of the SVM classifier in the MOBA. The formulated algorithm yielded better results than the conventional TLBO and JAYA algorithms.

A network involved in data sharing is prone to network intrusion that may result in cyberattacks, system destruction, and information loss, as noted in [18]. This paper aims to develop a new network IDS using deep learning and chaotic optimization. Its decision is supported by an understanding of the type of attack made possible by the Chaotic Honey Badger optimization method, M-squared normalization, Extended Synthetic Sampling, kernel-assisted principal component analysis, and Gated Attention Dual Long Short-Term Memory (Dugat-LSTM). The model's efficacy is stated through its comparison with other current models in terms of specific parameters, including accuracy, precision, recall, and F1 score.

In [9], the researchers focused on identifying the classification of cybersecurity attacks using CNN and datasets. The hyperparameters of the CNN configurations were further improved through hyperparameter optimization techniques, such as Grid Search, Random Search, and Bayesian Optimization. The optimized model improved the baseline models, which corroborates the importance of the HPO in developing robust CNN models for cybersecurity.

Kilichev et al. [19] examined hyperparameter optimization for one-dimensional convolutional neural networks (CNNs). Owing to the growing frequency and sophistication of intrusion detection systems (IDSs), effective intrusion detection systems are required. This paper considers nine hyperparameters in a CNN model using particle swarm optimization (PSO) and genetic algorithms (GA). According to the results, all datasets' accuracy, loss, precision, recall, and F1-score have significantly improved. This paper advances network security and the development of sophisticated, reliable, and flexible IDSs.

Deep learning has been combined with hyperparameter optimization, data balance, and high-dimensional reduction. The model (VGG19) exhibits robust performance and generalization on large datasets, outperforming previous models in terms of accuracy [20]. Similarly, FDL-CADIS was proposed [8] to combine deep and machine learning models to help intelligent systems identify and classify cyber-attacks. It converts binary malware files into two-dimensional images, takes features from them, and adjusts the hyperparameters using the MobileNetv2 model. The method performs better in an experimental analysis using voting-based classifiers than existing methods using a benchmark dataset.

In addition, deep learning has been used to identify False Data Injection Attacks (FDIAs) in cyber-physical power systems using a one-dimensional Convolutional Neural Network (CNN) [21]. Adjusting the hyperparameters with different optimizers improved the model's prediction accuracy. In hyperparameter optimization challenges, the CNN-BO approach demonstrated its usefulness by outperforming other optimization algorithms and obtaining a remarkable locational detection accuracy of 96.67% for the IEEE 14-bus system.

Traditional IDSs are no longer effective owing to the introduction of cyber hazards and complicated platforms introduced by the Industrial Internet of Things (IIoT). An improved research optimization was deployed with an ensemble deep learning-based cybersecurity (IRSO-EDLCS) technique for IIoT environments [22]. The IRSO-EDLCS method combines three deep learning models—the autoencoder, bidirectional gated recurrent unit, and deep belief network—with the IRSO algorithm-based feature selection. A modified grey wolf optimizer handles the hyperparameter-tuning process.

The researchers in [23] proposed a deep CNN (DCNN) architecture for IDSs that mines network traffic data for relevant properties through deep learning. The model effectively differentiates between typical and atypical behaviors as it was trained on large datasets. The performance was assessed using four publicly accessible

IDS datasets; the findings indicated a detection accuracy of 99.79%–100%.

Cybersecurity is essential in the current world, but because networks have limited resources, cybercriminals can attack them. An innovative Artificial Intelligence method is intended to detect intrusions efficiently [24]. The Golden Eagle Optimization-based Self-constructing Multi-layer Perceptron Interfaced Fuzzy System (GEO-SMPIF) solution enhances privacy and security in a professional network infrastructure. The technique performs better than current methods regarding accuracy, false alarm rates, and detection rates. The NSL-KDD and UNSW-NB15 datasets were used in an experimental setting to demonstrate their effectiveness.

Data privacy is vital in the banking industry, mainly when dealing with DDoS attacks. Machine learning (ML) is an effective technique for identifying and averting cyberattacks [25]. This paper proposes a hyperparameter optimization method based on hierarchical machine learning for network intrusion classification. Utilizing the CICIDS 2017 standard dataset, the LGBM algorithm successfully improved cybersecurity by categorizing DDoS results with 99.77% accuracy.

The development of interconnected healthcare devices has increased the danger of security compromises associated with the Internet of Medical Things (IoMT). A multilayer perceptron and recursive feature removal model for cyberattacks and anomaly detection was created [26]. The model effectively mitigated cyber assaults in healthcare applications by achieving elevated accuracy rates across several IoMT cybersecurity datasets.

The control and data planes are separated by software-defined networks (SDNs), susceptible to cyberattacks [27]. Owing to its centralization, the control plane is vulnerable to attacks. An IDS is created to safeguard the data. A hybrid metaheuristic with deep learning led to a cyberattack prevention (HMDL-CAP) model in SDN, which is presented in this article. The model employs the SDOFS method, data preprocessing, the HCRNN model, and the Pelican optimization technique for hyperparameter tuning. The tests indicate that the performance is better than that of a set of recent models.

Server cyberattacks are becoming more frequent because of the development of information technology. Conventional IDS finds it challenging to handle numerous, varied forms of attacks. It has been suggested that detection technologies can be improved using machine learning and deep learning. In [9], researchers proposed a hybrid approach based on multi-objective optimization that uses CNN models for MobileNetV2, Shuffle Net, and QR code pictures. The Harris Hawk Optimization algorithm is utilized to choose the most valuable features for classification, leading to a 95.69% accuracy rate and better performance than CNN models.

Some sectors, such as energy, healthcare, and smart homes, can use the Internet of Things (IoT). Thus, the number of connected devices and ad hoc networks also poses additional concerns. Deep learning techniques have shown promise in evaluating IoT devices, and this work introduces an integrated deep learning method known as DCCNN-SMO [28]. The proposed solution performs better than current methods in classifying cybersecurity threats in IoT networks. This is done using the Stolen reference code to detect software piracy.

The need for sophisticated IDS arose from the growing cyberattack susceptibility of Industrial Internet of Things (IIoT) networks. An enhanced Deep Transfer Learning (DTL) IDS designed specifically for heterogeneous IIoT networks was presented in [29]. The system integrates bootstrap aggregation ensemble techniques, genetic algorithms, and CNNs in a tri-layer manner. The 100% attack detection accuracy rate achieved in combating 14 cyber threats proved the performance.

In [30], researchers proposed a hyperparameter-selected fusion neural network and a joint symmetric uncertainty intrusion detection method. It employs PSO, CNN-LSTM, and a feature selection algorithm to reduce data dimensionality and improve classifier performance. This is also evidenced by experiments in which the performance and superiority of the proposed algorithm were evaluated in terms of various assessment criteria, which increased the adaptability and applicability of the approach considered in this study to different datasets for intrusion detection. In addition, deep learning (DL) has exhibited the ability to detect malware and botnet cyberattacks by analyzing large amounts of network traffic data. The proposed DL models can identify anomalies and possible wayward traffic patterns in the ever-complicated relationships among the traffic attributes of a network. In [31], a new method was proposed to determine malware and botnet attacks in IoT networks using LSTM and GAN. This approach enhances security systems by establishing a communication message that is friendly or malicious with very high accuracy. It is possible to adapt to new attack letters using DL models. However, the quality and quantity of the data used can affect it.

3. Methodology

This section outlines the proposed method for optimizing the detection of cyberattacks by integrating these three state-of-the-art technologies. CNNs are then discussed to explain how they can be used to extract features from the data. CNNs are a data-documented computing model that can recognize many significant patterns and features in complicated input through' deep learning. A CNN was employed as the main instrument for data analysis and information extraction concerning cyber-

attacks. Here, CNNs, inputs, outputs, and the arrival of the chosen model training and selection are discussed. The Jaya algorithm is employed to fine-tune the settings and parameters of the neural network and enhance the detection accuracy of attacks. In contrast to genetic algorithms that involve intricate operations, including but not limited to combination and mutation, Jaya's algorithm executes straightforwardly and does not require such steps. This makes it easier for the model to detect cyber-attacks, as the algorithm reduces the error and directs the network to the right solution. By employing Jaya, the time required to analyze the data and perform the function of threat identification in the system is less than that of the other methods. This section provides details concerning the structure of the Jaya algorithm, the parameters used, and its implementation.

A. Methodology

This section outlines the proposed plan for constructing an efficient and accurate means for identifying cyberattacks. First, data on cyberattacks were gathered and cleaned for further use in the model. The following process entails data preprocessing: the data are cleaned, and any improper item is removed while the features are normalized to enhance the model's training. The recovered CNNs were subsequently used to learn and instantiate the feature vectors of the input using the Jaya algorithm. These features feed the cyberattack detection process into the SVM algorithm. Ultimately, the performance of the proposed system is assessed with the help of some criteria, such as accuracy and correctness, for testing the developed approach. A flowchart of the proposed method is shown in Figure 1.

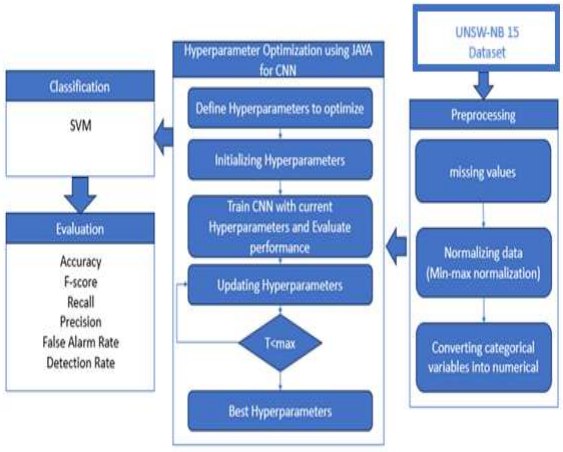

Figure 1. The systematic method is depicted in the flow chart.

1) DATA COLLECTION AND PREPROCESSING

In this step, the input data were preprocessed to remove unwanted noise and missing data after they were collected. The preprocessing technique includes cleaning the data, normalizing it, and transforming categorical variables into numerical ones. The integration and preparation of cybersecurity data from the UNSW-NB15 dataset, which includes significant pre-processing such as managing missing values, normalizing data, and transforming categorical variables into appropriate numerical formats, such as machine learning, which provides for various types of cyberattacks, is the first step in the proposed approach. The data are divided into training and testing to facilitate model creation, construction, and evaluation.

2) DATA CLEANING

Data cleaning purges corrupted, invalid, redundant, insufficient, and inaccurate data from the dataset. Therefore, the overarching purpose of cleaning is to prepare a dataset for analysis and quickly locate the correct data to be queried. Data cleaning involves identifying and addressing consistently unacceptable data formats that contain incorrect data in the dataset. This eliminates irrelevant and redundant data from the dataset, ensuring that duplicate data observations are addressed throughout the dataset. Irrelevant data observations occur when the model is unsuitable for specific attacks. Data cleaning removes the structural errors that occur during data transmission. In addition, it handles missing data by removing observations containing missing values or imputing them based on other observations.

3) NORMALIZATION

Normalization is a preprocessing step in which a new range is derived from an existing range. Because there are uncertain and incomplete data in the dataset, missing data must be corrected by removing irrelevant data to enhance the quality. Therefore, min-max normalization plays an effective role in unifying and normalizing the dataset. A normalization approach is required to maintain a more significant variance in predictions and predictors within a new range. Normalization refers to scaling datasets such that the values of the normalized data fall between zero and one. This normalization technique helps to compare normalized values from two or more different datasets to a certain extent, eliminating the effects of variations in scale. Compared with datasets with smaller values, larger datasets were utilized. Normalization is achieved by subtracting a smaller value from the variable to be normalized. A smaller value was deducted from the maximum value. Normalization is computed using Equation (1)[32].

$$x_{normalized} = \frac{x - x_{normalized}}{x_{maximum} - x_{minimum}} \quad (1)$$

B. CNN for Feature Extraction

Using Jaya-based machine learning, a Convolutional Neural Network (CNN) was built and implemented in the second stage. The CNN was trained to extract significant features from the preprocessed cybersecurity data. We will investigate various CNN architectures to identify the best model for feature extraction. In the next step, the SVM classifier uses the features of the CNN output as the input. This is an essential step because the effectiveness of SVM in identifying cyberattacks is directly affected by the quality of the information that CNN extracts.

C. Hyperparameter Optimization using Jaya

This paper presents the methodology of using a 1D CNN to analyze data and applies the Jaya algorithm to optimize the parameters. This system aims to build a robust classification model using a CNN and improve its performance by selecting the optimal parameters.

1) INPUTS

The system begins with data preprocessing to create training and testing datasets. In this regard, the data are divided into training and test data using data-partitioning techniques. The input data were then redesigned to meet the standard set by the Conv1D lateral layer.

2) INITIALIZE THE CNN

The next step requires running a network initialization function that includes a set of custom parameters and input data. The following parameters were used to build the model.

-Number of filters
-Window size
-Buckling size
-Dense layer units
-Number of layers

The input shape was prepared based on the dimensions of the training data, and a CNN model was built using the specified parameters. The model was then pooled and trained using categorical cross-entropy loss and the Adam optimizer.

3) JAYA PARAMETERS

In the Jaya algorithm, a set of basic parameters is used to ensure the effectiveness of the parameter optimization process. These parameters include the following. Population size refers to the number of individuals (probabilities) in each generation. The population size can significantly affect the quality of the final solutions, as a more significant number increases the chances of exploring the solution space. Each individual represents a solution to the problem that contains the network parameters and kernel type of the SVM.

Max Iterations: represents the maximum number of generations that the algorithm generates. Adjusting this parameter allows the algorithm to perform sufficient optimization before making a final decision. Hyperparameter Space: defines the minimum and maximum values of the parameters to be optimized. This space includes CNN-related parameters, such as the number of filters, kernel size, and stacking layers, as well as SVM algorithm parameters, such as kernel type and C. Update Steps: The formula is used to update individuals, where each individual is modified based on the difference between the optimal and worst-case solutions in the current iteration. These steps help to direct the search for the most promising regions in the solution space.

4) TRAINING THE SVM MODEL

Subsequently, the SVM model was trained using the features extracted from the CNN training data, and the model was evaluated using the test dataset. The model's accuracy was calculated using Equation 2, and the results were stored [33].

$$fitness = \frac{number\_of\_instances\_correctly\_classified}{Total\_number\_of\_instances} \quad (2)$$

5) OPTIMIZING PARAMETERS USING THE JAYA ALGORITHM

The Jaya algorithm begins by generating a random set of solutions (parameters) within the specified range for each parameter. Each solution was evaluated based on the accuracy of the CNN model, and the solutions were updated based on the current best solution. The process continues through a fixed number of iterations, in which the solutions are updated according to the evaluations. Set update: In each iteration, the set of solutions was updated based on the best and worst solutions using Equation 6, as defined in the Jaya algorithm. Performance tracking: Model accuracy is tracked over iterations to identify improvements [34].

$$NewSolution_i = CurrentSolution_i + r_1(BestSolution - |CurrentSolution_i| - r_2(WortSolution - |SurrentSolution_i|) \quad (3)$$

D. SVM for Cyber Attack Detection

The fourth stage is detecting the cyberattack using a support vector machine (SVM) that discovers the features extracted by CNN with Jaya. It is an essential stage through which it is possible to differentiate between normal attacks and cyberattacks.

4. Experimental Results and Evaluation

We mentioned the proposed method that improves the convolutional neural network algorithm by using the Jaya algorithm to select the best parameters. The system must be able to detect an intrusion. Evaluations and tests should be performed using this system to prove this. All the experiments were conducted using the UNSW-NB15 dataset. A performance analysis was performed according to the evaluation of the test set. We used various evaluation measures, including classification accuracy, precision, Recall, and F1 score.

A. UNSW-NB15 Dataset

The dataset was created using the IXIA Perfect Storm tool at the Cyber Range Laboratory at the UNSW. 1 Canberra. It aims to simulate a combination of modern normal activities and artificial attack behaviors, making it suitable for evaluating IDSs [35]. Data combination: The dataset contained records divided into training and testing sets. The training set contained 164,673 records, whereas the test set contained 93000 records. Table 5 lists the number of samples in the training and test data, the number of samples representing attacks, and the number of samples representing normal cases.

B. Model Evaluation and Comparison

To evaluate the proposed model, we considered key performance measures obtained from the confusion matrix [36, 37]. A confusion matrix is a table containing the binary classification results of a binary classifier on the test data. It has four components: the binary classification results.

- TP: True Positive Prediction.
- FP: false-positive prediction.
- TN: True negative prediction.
- FN: false-negative prediction.

Table 1. Provides an overview of the confusion matrix for the binary classification problem of an IDS (attack or no attack). Results are different combinations of expected and actual values.

Table 1: The confusion matrix

	Predicted condition		
	Total population =P+N	Positive (PP)	Negative (PN)
Actual condition	Positive (P)	True positive (TP)	False negative (FN)
	Negative (N)	False positive (FP)	True negative (TN)

[1] https://www.kaggle.com/datasets/dhoogla/unswnb15

1- Accuracy

Classification accuracy is an essential criterion for evaluating classifier performance. This scale shows how the data were classified using a specific classification model, as in equation (4). The best classification accuracy was one, while the worst was zero.

$$\text{Accuracy} = (TP+TN)/ TP+TN+FP+FN) \quad (4)$$

2- Precision

That is, how many of the positive classes we correctly predicted are positive, as shown in equation (5).

$$\text{Precision} = TP/(TP+FP) \quad (5)$$

3- Recall

This implies that we made some correct predictions for all the positive classes. As shown in equation (6), it should be as high as possible.

$$\text{Recall} = TP/(TP+FN) \quad (6)$$

4- F1-Score

If we want the precision and recall criteria involved in the model evaluation, we use this criterion, as shown in equation (7).

$$\text{F1-score} = 2 \times ((\text{recall} \times \text{precision})/ (\text{Recall} * \text{Precision})) \quad (7)$$

5- False Alarm Rate

The false alarm rate (FAR) is a detection system metric that measures the percentage of normal events mistakenly identified as a threat in equation (8).

$$\text{FAR} = FP/(TN+FP) \quad (8)$$

C. Jaya and CNN parameters and simulation environment

The results are presented after introducing the comparison method, dataset, and evaluation criteria.

At this stage, as stated in the proposed method, we used the convolutional neural network to extract the features and the support vector machine to classify the data into two intrusive or non-intrusive categories using the Jaya algorithm to obtain the optimal value of the parameters of this network. Table 2 presents the parameters the Jaya algorithm uses to optimize the neural network in the UNSW-NB15 datasets for binary classification.

Table 2: CNN parameters using JAYA

	UNSW-
Filter 1	28
Kernel Size1	8
Pool Size1	4
Filters2	30
Kernel Size2	3
Pool Size2	2

Dense Units	12
Number of	2
Epochs	96
Batch Sizes	128
SVM Kernel	1
SVM C	0.8
Population	10
Max Iterations	10

D. Test results

The results obtained using binary classification is the proposed method and compares the results with machine learning classification on the UNSW-NB15 dataset.

Table 3 compares the performances of several classification models using the metrics of precision, recall, predictive accuracy, and F1 score. The proposed model outperforms the others, achieving a high precision of 0.997, a recall of 0.999, a predictive accuracy of 0.994, and an F1 score of 0.996. As for the other models, XGBoost performed well with a precision of 0.937 and an F1 score of 0.950, while the decision tree (DT) model achieved a precision of 0.927 and an F1 score of 0.943. The CNN-SVM model achieved a precision of 0.922 and an F1 score of 0.939.

Other models, such as SVM, Logistic, and KNN, perform well but are less than the proposed model, with F1 scores ranging from 0.898 to 0.924.

Table 3: Results for the binary classifier on the dataset UNSW-NB15

method	Accurac	Reca	Precisio	f1scor	FAR
SVM	0.897	0.98	0.868	0.924	0.264
Logistic	0.861	0.96	0.842	0.898	0.315
XGBoo	0.937	0.95	0.951	0.950	0.085
DT	0.927	0.94	0.942	0.943	0.102
KNN	0.901	0.92	0.920	0.923	0.142
CNN-	0.922	0.94	0.938	0.939	0.109
our	0.997	0.99	0.994	0.996	0.004

6) COMPARISON OF STUDIES

To complete the analysis of this research in an integrated, scientific, and systematic manner, the model proposed for this research was compared with the tests of other methods and techniques presented by several researchers in recent scientific articles. Table 4. A comparison of the proposed methods and strategies for identifying a group of students from these studies and recent publications, in contrast with the technology proposed in this research, shows that the efficiency of the technology proposed in this paper is the highest.

Table 4: Comparison table between previous studies

Research Name,	Algorithm	data set	Accuracy
GWO [16]	GWO	UNSWNB-15	81%
Proposed method	JAYA-CNN-SVM	UNSWNB-15	99.7%

4. Conclusion

The increasing sophistication of cyber threats demands advanced intrusion detection systems (IDS) capable of accurately identifying and mitigating attacks. This paper proposed a novel hybrid approach combining Convolutional Neural Networks (CNN), Support Vector Machines (SVM), and the Jaya optimization algorithm to enhance cyberattack detection. By leveraging Jaya for hyperparameter optimization, the model achieved superior feature extraction and classification performance, significantly improving detection accuracy while reducing false alarms.

Experimental evaluations on the NSW-NB15 datasets demonstrated the effectiveness of the proposed method. It achieved high accuracy with 99.7%, precision, recall, and F1-score, outperforming traditional machine learning and deep learning models. The Jaya-optimized CNN-SVM framework proved particularly effective in binary and multi-class classification, showcasing its adaptability to different attack scenarios.

Future work could explore Real-time implementation in large-scale network environments and integration with other metaheuristic algorithms (e.g., Genetic Algorithms, Particle Swarm Optimization) for further refinement. In addition, expansion to newer datasets (e.g., CIC-IDS2017, CSE-CIC-IDS2018) is needed to validate generalizability. Edge computing deployment for low-latency intrusion detection in IoT networks. This study contributes to cybersecurity research by presenting an efficient, optimized deep learning model for intrusion detection. It offers a robust solution to evolving cyber threats. The results highlight the potential of hybrid AI-driven approaches in securing modern network infrastructures.

References

[1] Kunang, Y. N., Nurmaini, S., Stiawan, D., & Suprapto, B. Y. (2021). Attack classification of an intrusion detection system using deep learning and hyperparameter optimization. Journal of Information Security and Applications, 58, 102804.

[2] Masum, M., Shahriar, H., Haddad, H., Faruk, M. J. H., Valero, M., Khan, M. A., ... & Wu, F. (2021, December). Bayesian hyperparameter optimization for deep neural network-based network intrusion detection. In 2021 IEEE International Conference on Big Data (Big Data) (pp. 5413-5419). IEEE.

[3] Inuwa, M. M., & Das, R. (2024). A comparative analysis of various machine learning methods for anomaly detection in cyberattacks on IoT networks. Internet of Things, 26, 101162.

[4] Vincent Banda, T., Blaauw, D., & Watson, B. W. (2023, October). Towards a Supervised Machine Learning Algorithm for Cyberattacks Detection and Prevention in a Smart Grid Cybersecurity System. In Pan African Conference on Artificial Intelligence (pp. 107-128). Cham: Springer Nature Switzerland.

[5] Bitirgen, K., & Filik, Ü. B. (2023). A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in the smart grid. International Journal of Critical Infrastructure Protection, 40, 100582.

[6] Alabsi, B. A., Anbar, M., & Rihan, S. D. A. (2023). CNN-CNN: dual convolutional neural network approach for feature selection and attack detection on Internet of things networks. Sensors, 23(14), 6507.

[7] Roshanzadeh, B., Choi, J., Bidram, A., & Martínez-Ramón, M. (2024). Multivariate time-series cyberattack detection in the distributed secondary control of AC microgrids with convolutional neural network autoencoder ensemble. Sustainable Energy, Grids and Networks, 38, 101374.

[8] Alaca, Y., & Çelik, Y. (2023). Cyber attack detection with QR code images using lightweight deep learning models. Computers & Security, 126, 103065.

[9] Adnyana, I. G., Sugiartawan, P., & Hartawan, I. N. B. Hyperparameter Optimization Techniques for CNN-Based Cyber Security Attack Classification. IJCCS (Indonesian Journal of Computing and Cybernetics Systems), 18(3).

[10] Alzubi, O. A., Qiqieh, I., & Alzubi, J. A. (2023). Fusion of deep learning-based cyberattack detection and classification model for intelligent systems. Cluster Computing, 26(2), 1363-1374.

[11] Kabakus, A. T. (2023). A novel robust convolutional neural network for uniform resource locator classification from the view of cyber security. Concurrency and Computation: Practice and Experience, 35(3), e7517.

[12] Mhmood, A. A., Ergül, Ö., & Rahebi, J. (2024). Detection of cyber-attacks on smart grids using improved VGG19 deep neural network architecture and Aquila optimizer algorithm. Signal, Image and Video Processing, 18(2), 1477-1491.

[13] Saheed, Y. K., Abdulganiyu, O. H., Majikumna, K. U., Mustapha, M., & Workneh, A. D. (2024). ResNet50-1D-CNN: A new lightweight resNet50-One-dimensional convolution neural network transfer learning-based approach for improved intrusion detection in cyber-physical systems. International Journal of Critical Infrastructure Protection, 45, 100674.

[14] Rubai, S. M. (2023). Development of hyper-parameter-tuned-recurrent neural network for detection and mitigation of fraudulent resource consumption attacks in the cloud. Transactions on Emerging Telecommunications Technologies, 34(3), e4723.

[15] Hussain, S., Mustafa, M. W., Ateyeh Al-Shqeerat, K. H., Saleh Al-rimy, B. A., & Saeed, F. (2022). Electric theft detection in advanced metering infrastructure using Jaya optimized combined Kernel-Tree boosting classifier—A novel sequentially executed supervised machine learning approach. IET Generation, Transmission & Distribution, 16(6), 1257-1275.

[16] Alzaqebah, A., Aljarah, I., Al-Kadi, O., & Damaševičius, R. (2022). A modified grey wolf optimization algorithm for an intrusion detection system. Mathematics, 10(6), 999.

[17] Larijani, A., & Dehghani, F. (2023). An efficient optimization approach for designing machine models based on combined algorithms. FinTech, 3(1), 40-54.

[18] 18 Devendiran, R., & Turukmane, A. V. (2024). Dugat-LSTM: Deep learning-based network intrusion detection system using chaotic optimization strategy. Expert Systems with Applications, 245, 123027.

[19] 19 Kilichev, D., & Kim, W. (2023). Hyperparameter optimization for 1D-CNN-based network intrusion detection using GA and PSO. Mathematics, 11(17), 3724.

[20] Adel Binbusayyis, " Hybrid VGG19 and 2D-CNN for intrusion detection in the FOG-cloud environment", Expert Systems with Applications, Volume 238, Part A, 15 March 2024, 121758.

[21] Ibraheem, R., Eddin, M. E., Massaoudi, M., & Abu-Rub, H. (2024, January). Enhancing Locational FDIA Detection in Smart Grids: A Hyperparameter Optimization Analysis. In 2024 4th International Conference on Smart Grid and Renewable Energy (SGRE) (pp. 1-6). IEEE.

[22] Vaiyapuri, T., Shankar, K., Rajendran, S., Kumar, S., Gaur, V., Gupta, D., & Alharbi, M. (2024). Automated cyberattack detection using optimal ensemble deep learning model. Transactions on Emerging Telecommunications Technologies, 35(4), e4899.

[23] Hnamte, V., & Hussain, J. (2023). Dependable intrusion detection system using deep convolutional neural network: A novel framework and performance evaluation approach. Telematics and Informatics Reports, 11, 100077.

[24] Siva Shankar, S., Hung, B. T., Chakrabarti, P., Chakrabarti, T., & Parasa, G. (2024). A novel optimization-based deep learning with artificial intelligence approach to detect intrusion attacks in network systems. Education and Information Technologies, 29(4), 3859-3883.

[25] Dasari, S., & Kaluri, R. (2024). A practical classification of DDoS attacks in a distributed network by adopting hierarchical machine learning and hyperparameters optimization techniques. IEEE Access.

[26] Kilincer, I. F., Ertam, F., Sengur, A., Tan, R. S., & Acharya, U. R. (2023). Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization. Biocybernetics and Biomedical Engineering, 43(1), 30-41.

[27] Arun Prasad, P. B., Mohan, V., & Vinoth Kumar, K. (2024). Hybrid metaheuristics with deep learning enabled cyberattack prevention in software-defined networks. Tehnički vjesnik, 31(1), 208-214.

[28] Vijayalakshmi, P., & Karthika, D. (2023). A hybrid dual-channel convolution neural network (DCCNN) with spider monkey optimization (SMO) is used for cyber security threat detection on the Internet of Things. Measurement: Sensors, 27, 100783.

[29] Latif, S., Boulila, W., Koubaa, A., Zou, Z., & Ahmad, J. (2024). Dtl-ids: An optimized intrusion detection framework using deep transfer learning and genetic algorithm. Journal of Network and Computer Applications, 221, 103784.
[30] Wang, Q., Jiang, H., Ren, J., Liu, H., Wang, X., & Zhang, B. (2024). An intrusion detection algorithm based on joint symmetric uncertainty and hyperparameter optimized fusion neural network. Expert Systems with Applications, 244, 123014.
[31] Kaushik, P. (2023). Unleashing the power of multi-agent deep learning: Cyber-attack detection in IoT. International Journal for Global Academic & Scientific Research, 2(2), 15-29.
[32] Hsu, C.-W., Chang, C.-C., & Lin, C.-J. (2003). A Practical Guide to Support Vector Classification.
[33] [R] 33 Friedrichs, F., & Igel, C. (2005). Evolutionary tuning of multiple SVM parameters. Neurocomputing, 64, 107–117.
[34] Rao, R. V. (2016). "Jaya: A simple and new optimization algorithm for solving constrained and unconstrained optimization problems". International Journal of Industrial Engineering Computations, 7(1), 19-34.
[35] Moustafa, N., & Slay, J. (2015). "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set)."
[36] Chicco D, Jurman G (January 2020). "The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation". BMC Genomics. 21 (1): 6-1–6-13. doi:10.1186/s12864-019-6413-7. PMC 6941312. PMID 31898477.
[37] Alzboon, K.; Al-Nihoud, J.; Alsharafat, W. Novel Network Intrusion Detection Based on Feature Filtering Using FLAME and New Cuckoo Selection in a Genetic Algorithm. Appl. Sci. 2023, 13, 12755. https://doi.org/10.3390/app132312755.

KHALED BATIHA is a professor at AL al-Bayt University, Mafraq, Jordan. His research interests include wireless sensor networks, network security, and data mining.

Wafa Alsharafat received a B.S. degree in computer science from Hashemite University, Zarqa, Jordan, in 2001 and the M.S. and Ph.D. degrees in computer information systems from Arab Academy, Amman, Jordan, in 2004 and 2009, respectively. She is an Associate Professor at AL al-Bayt University, Mafraq, Jordan. Her research interests include wireless sensor networks, artificial intelligence, genetic algorithms, optimization algorithms, and network security.

Maymouna Shbail received a B.S. degree in computer science from AL al-Bayt University, Mafraq, Jordan, in 2012. She is currently a postgraduate student (with a master's degree) working with the Ministry of Education. Her research interests include Cyber Security, Network Security, and Artificial Intelligence.