KMAN PUBLISHING INSTITUTE

Article history:
Received 06 December 2025
Revised 22 March 2026
Accepted 10 April 2026
Published online 01 July 2026

Journal of Resource Management and Decision Engineering

Volume 5, Issue 4, pp 1-16

Detection of Attacks in Internet of Things Devices Using an Optimized Ensemble Classification Based on Deep Transfer Learning and the Harris Hawks Algorithm

Farqad. Abdullah Mohammed[1], Saba. Joudaki[2*], Mezher. H Mezher[3], Mahdi. Mosleh[1]

[1] Department of Computer Engineering, Isf.C., Islamic Azad University, Isfahan, Iran
[2] Department of Computer Engineering, Khor.C., Islamic Azad University, Khorramabad, Iran
[3] Department of Electronics and Communication, College of Engineering, University of Al-Qadisiyah,Al-Diwaniyah, Iraq

*** Corresponding author email address**: saba.joudaki@iau.ac.ir

A r t i c l e I n f o

Article type:
Original Research

How to cite this article:
Abdullah Mohammed, F., Joudaki, S., H Mezher, M., & Mosleh, M. (2026). Detection of Attacks in Internet of Things Devices Using an Optimized Ensemble Classification Based on Deep Transfer Learning and the Harris Hawks Algorithm. *Journal of Resource Management and Decision Engineering*, *5*(4), 1-16.
https://doi.org/10.61838/kman.jrmde.294

A B S T R A C T

With the rapid expansion of the Internet of Things (IoT) and the increasing number of cyberattacks targeting these devices, the use of efficient methods for attack detection has become increasingly important. In this study, a novel approach based on ensemble deep transfer learning optimized by the Harris Hawks Optimization (HHO) algorithm is proposed for detecting attacks in IoT devices. In this method, multiple deep transfer learning models are employed, which are capable of transferring learned knowledge from data in other domains to IoT-related data. Subsequently, the Harris Hawks algorithm is utilized to optimize the model parameters and integrate them into an ensemble classifier. The Edge-IIoTset dataset is used to evaluate the performance of the proposed method. The obtained results indicate that the detection accuracy reaches 99.8%, while the false alarm rate is significantly reduced. These findings demonstrate the high effectiveness of the proposed method in enhancing the security level of IoT devices.

Keywords: *Internet of Things (IoT), Attack Detection, Deep Transfer Learning, Ensemble Classification, Harris Hawks Optimization Algorithm, Metaheuristic Optimization.*

1. Introduction

The rapid proliferation of the Internet of Things (IoT) has fundamentally transformed contemporary technological ecosystems, enabling seamless interconnectivity among devices, systems, and infrastructures across domains such as smart cities, healthcare, manufacturing, and supply chain management (Jiang, 2025; Jin & Karki, 2025; Marcus et al., 2025). This pervasive integration of IoT technologies has significantly enhanced operational efficiency, real-time decision-making, and data-driven management processes. However, the expansion of IoT networks has also introduced substantial security vulnerabilities due to the heterogeneous, distributed, and resource-constrained nature of connected devices (Sarker et al., 2023; Yang et al., 2017). As IoT systems increasingly underpin critical infrastructures, ensuring robust cybersecurity mechanisms has become a paramount concern for both researchers and practitioners.

One of the most critical challenges in IoT environments is the detection and mitigation of cyberattacks, particularly distributed denial-of-service (DDoS) attacks, which can severely disrupt network availability and system functionality (Hasan, 2023; Radhika & Kulothungan, 2019). These attacks exploit the limited computational and security capabilities of IoT devices, making traditional security approaches insufficient. Moreover, the diversity of attack vectors, including routing attacks, sinkhole attacks, and intrusion attempts, further complicates the development of effective detection mechanisms (Sharma et al., 2017; Tseng et al., 2011). Consequently, advanced intrusion detection systems (IDS) tailored for IoT environments are required to address these evolving threats.

Machine learning (ML) and deep learning (DL) techniques have emerged as powerful tools for enhancing IoT security, particularly in the context of intrusion detection (Ahmad & Alsmadi, 2021; Thakkar & Lohiya, 2021). These approaches leverage data-driven models to identify patterns and anomalies indicative of malicious activities. Recent studies have demonstrated the effectiveness of ML-based methods in detecting DDoS attacks and other forms of intrusions by analyzing network traffic and behavioral features (de Lima Filho et al., 2019; Rani et al., 2023). However, conventional ML techniques often struggle with high-dimensional data, dynamic network conditions, and the need for extensive feature engineering.

Deep learning models, particularly convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have been widely adopted to overcome these limitations by automatically extracting hierarchical features from complex datasets (Van Houdt et al., 2020; Zhao et al., 2024). CNN-based architectures are particularly effective in capturing spatial patterns in data, while models such as long short-term memory (LSTM) networks are capable of modeling temporal dependencies. These capabilities have led to significant improvements in the accuracy of intrusion detection systems in IoT environments (Stefanos et al., 2022; Xiao et al., 2024). Despite these advancements, deep learning models often require large labeled datasets and extensive computational resources, which may not always be feasible in IoT scenarios.

To address these challenges, transfer learning has been introduced as a promising approach that enables models to leverage knowledge learned from related domains and apply it to new tasks with limited data (Chen et al., 2023; Yan, 2024). In the context of IoT security, deep transfer learning has demonstrated its potential to improve detection performance while reducing training time and data requirements (Mehedi et al., 2022; Sahu et al., 2024). By utilizing pre-trained models, transfer learning facilitates the adaptation of existing knowledge to IoT-specific datasets, thereby enhancing model generalization and robustness.

In addition to transfer learning, ensemble learning techniques have been widely explored to further improve the performance of intrusion detection systems. Ensemble methods combine multiple base classifiers to achieve better predictive accuracy and robustness compared to individual models (Bouke et al., 2023; Khanday et al., 2023). By aggregating the outputs of diverse models, ensemble approaches can mitigate the weaknesses of individual classifiers and provide more reliable detection results. Hybrid models that integrate machine learning and deep learning techniques have also been proposed to enhance detection capabilities in IoT environments (Omar et al., 2023; Shahid et al., 2024).

Another critical aspect of improving model performance lies in the optimization of hyperparameters. Traditional manual tuning methods are often inefficient and may not yield optimal results, especially in complex models with numerous parameters. Metaheuristic optimization algorithms have gained significant attention as effective tools for automated hyperparameter tuning (Heidari et al., 2019). Among these, the Harris Hawks Optimization (HHO) algorithm has shown promising results in various optimization tasks due to its ability to balance exploration and exploitation in the search space (Gharehchopogh et al.,

2023). The application of such algorithms in IoT intrusion detection can significantly enhance model accuracy and convergence efficiency.

Recent research has also emphasized the importance of high-quality datasets for training and evaluating intrusion detection systems. The evolution of IoT security datasets highlights the need for realistic, diverse, and comprehensive data to ensure reliable model performance (Kaur et al., 2023). Datasets such as Edge-IIoTset provide a more accurate representation of real-world IoT environments, enabling the development of more effective detection models. Furthermore, techniques such as feature selection and dimensionality reduction have been employed to improve model efficiency and reduce computational complexity (Zong & Huang, 2021).

Despite these advancements, several challenges remain in the development of effective IoT intrusion detection systems. These include handling data imbalance, adapting to dynamic network conditions, ensuring scalability, and maintaining high detection accuracy while minimizing false positives and false negatives (Heidari & Jabraeil Jamali, 2023; Mustapha et al., 2023). Additionally, the integration of multiple techniques, such as deep learning, transfer learning, and metaheuristic optimization, presents new opportunities for improving system performance but also introduces complexity in model design and implementation.

Given these challenges, there is a growing need for intelligent, adaptive, and efficient frameworks that can leverage the strengths of multiple approaches to enhance IoT security. The combination of deep transfer learning, ensemble classification, and advanced optimization techniques represents a promising direction for addressing the limitations of existing methods. Such hybrid frameworks can improve detection accuracy, reduce computational overhead, and enhance the robustness of intrusion detection systems in complex IoT environments.

Therefore, this study aims to develop an optimized ensemble intrusion detection model based on deep transfer learning and the Harris Hawks Optimization algorithm to improve the accuracy and robustness of attack detection in IoT environments.

2. Methods and Materials

In this section, the proposed method is described with the aim of improving accuracy and efficiency in attack detection within Internet of Things (IoT) environments. The overall structure of the proposed method is illustrated in Figure 1 and consists of five main stages. This method is designed based on the integration of deep learning models and the utilization of metaheuristic algorithms for parameter optimization, so that, on the one hand, the learning capability of the model is enhanced, and on the other hand, the accuracy and robustness in detecting unknown attacks are improved. The main stages of the proposed method are as follows.

Data Preprocessing: In the first step, the raw data collected from the network environment are examined. At this stage, data cleaning operations, normalization of numerical values, removal of outliers and incomplete data, and transformation of data into an appropriate format for modeling are performed. Subsequently, relevant features are extracted from the network data, and the dataset is divided into training and testing subsets to enable model training and performance evaluation.

Construction of Base Models Using Deep Transfer Learning: In this stage, several base models are developed using deep transfer learning architectures. These models are capable of transferring knowledge acquired from prior training on large-scale datasets to the current problem. As a result, the training process is accelerated, and the accuracy of the models in detecting complex patterns is improved.

Integration of Base Models via Ensemble Learning: After training the base models, their outputs are combined using an ensemble learning approach. The objective of this stage is to leverage the strengths of different models and reduce the potential errors of individual models. This component plays a critical role in improving the overall system accuracy and enhancing the generalization capability of the model under diverse network conditions.

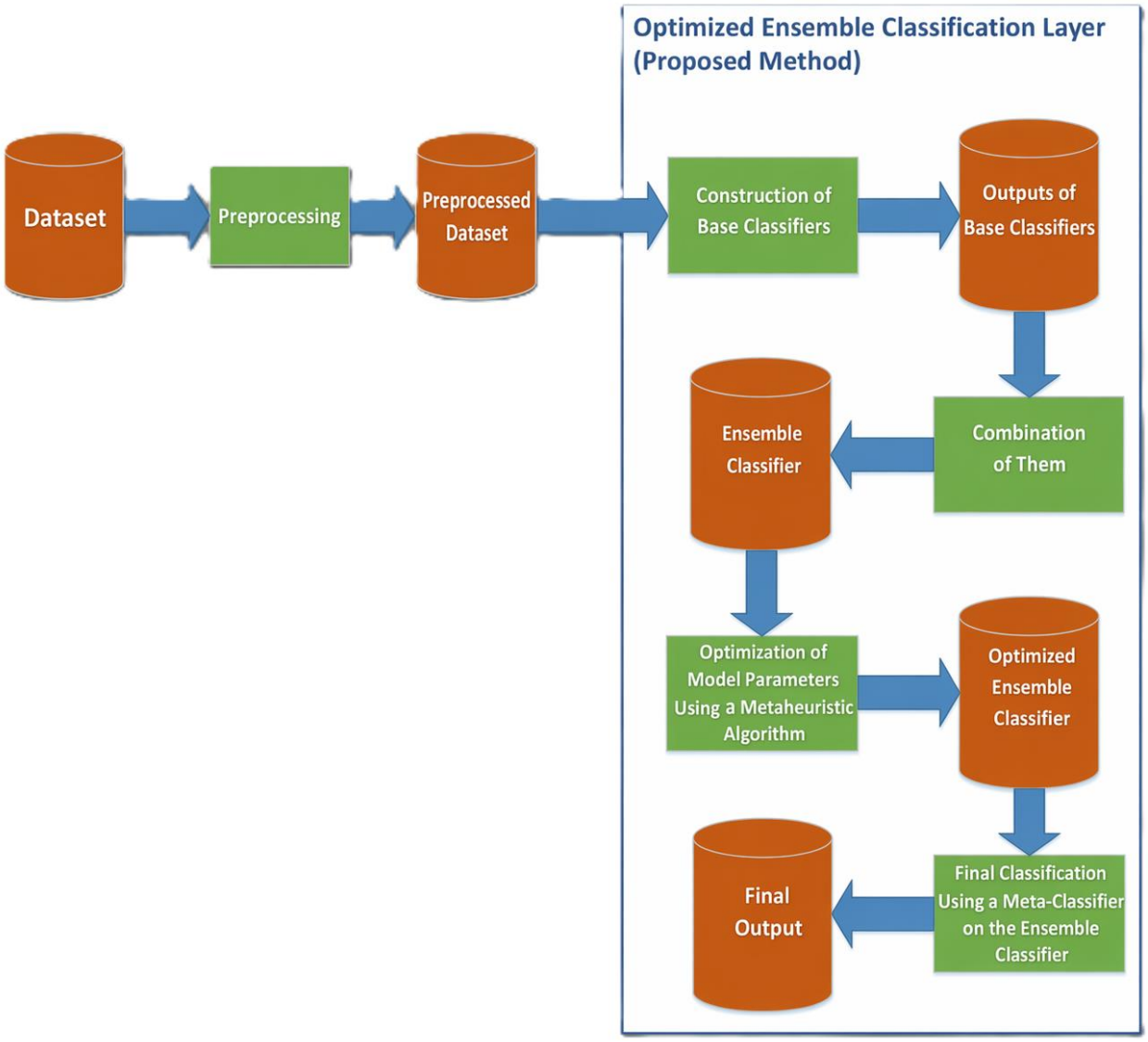
Optimization of Deep Learning Model Parameters: In this stage, to achieve optimal performance, the parameters of the deep learning models are tuned and optimized using metaheuristic algorithms. These algorithms, inspired by natural behaviors (such as evolution, swarm intelligence, and ecological balance), are capable of intelligently exploring the search space and identifying an optimal combination of parameters. The outcome of this stage is improved convergence speed and enhanced accuracy of the final model.

Final Classification Using a Meta-Classifier: In the final step, the outputs of the base models and the features extracted from previous stages are provided as inputs to a higher-level classifier. This meta-classifier analyzes and combines the outputs of the base models to make the final decision and classify the data into normal or malicious categories.

Overall, stages two through five are considered complementary components of the optimized ensemble deep transfer learning framework utilizing metaheuristic algorithms. This framework is designed to achieve an intelligent, accurate, and reliable system for attack detection in dynamic and complex IoT environments.

Figure 1

Block diagram of the proposed method



2.1. Dataset

In this study, the Edge-IIoTset dataset is used to implement and evaluate the proposed method. This dataset is designed to simulate a real-world IoT environment and includes traffic data generated from the activities of more than ten types of smart devices connected to the network. The dataset contains samples of normal behavior as well as fourteen different types of attacks associated with common IoT communication protocols. Notable features of this dataset include high device diversity, coverage of various attack types across different network layers, and precise recording of packet-level attributes. Due to its comprehensiveness, high quality, and strong resemblance to real-world conditions, this dataset is used as the primary reference for training, testing, and evaluating the proposed model in this study.

2.2. Preprocessing

In this section, preprocessing operations are performed on the initial raw data. Preprocessing is considered one of the most critical stages in the data analysis pipeline, as the quality of input data plays a decisive role in the performance and accuracy of machine learning and deep learning models. If the data are not properly prepared, even the most advanced algorithms cannot produce satisfactory results.

The main preprocessing steps in this study include the following three essential stages.

Data Cleaning: In this stage, incomplete, noisy, or erroneous data are identified and either removed or corrected. The presence of missing data and outliers can reduce model accuracy; therefore, data cleaning is essential for improving the quality and consistency of the dataset.

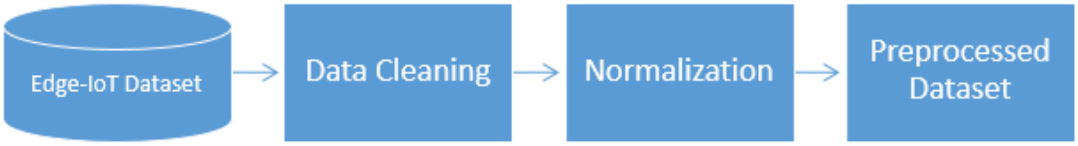
Data Transformation: In this step, the data are converted into a suitable format for processing by the models. This stage may include operations such as encoding categorical features, dimensionality reduction, or transforming data scales into formats compatible with learning algorithms.

Data Normalization: In this stage, feature scales are transformed into a specified range (typically $[0, 1]$or $[-1,1]$). The objective of normalization is to prevent the disproportionate influence of features with different scales. This process improves the convergence speed of learning algorithms and enhances model accuracy.

These three steps are presented as key preprocessing stages in Figure 2 and play an important role in preparing raw data for subsequent analysis and modeling stages.

Figure 2

Preprocessing stages



The features are normalized, and outliers are removed. For normalizing numerical data, the Min–Max normalization method is employed. This method is one of the most widely used normalization techniques, in which feature values are mapped into a specified range, typically $[0, 1]$. As a result, all input values are placed on a uniform scale, preventing the disproportionate influence of features with different ranges.

The general formula for Min–Max normalization is as follows:

$$x_{\text{new}}(i) = \frac{x_{\text{old}}(i) - \min(x)}{\max(x) - \min(x)}$$

where $x_{\text{old}}(i)$denotes the original feature value, $\min(x)$represents the minimum value of the feature, $\max(x)$represents the maximum value of the feature, and $x_{\text{new}}(i)$denotes the normalized value.

This transformation ensures that different features are scaled into a standard range, enabling more accurate comparison and processing by learning algorithms. Additionally, the removal of outliers alongside normalization improves data quality and prevents the negative impact of anomalous data on model performance.

2.3. Proposed Optimized Ensemble Classification Method Based on Deep Transfer Learning

In this section, the optimized ensemble classifier based on deep transfer learning using the Harris Hawks Optimization (HHO) metaheuristic algorithm is described. The overall structure of the proposed method is illustrated in Figure 3.

The main idea of this study is to present a multi-level classifier based on deep transfer learning and feature optimization using the Harris Hawks Optimization algorithm for attack detection in Internet of Things (IoT) devices. The rationale for employing deep transfer learning is that it enables the utilization of knowledge acquired from other domains for detecting attacks in IoT environments. Moreover, this approach reduces the model training time. On the other hand, the use of ensemble classification plays a significant role in improving accuracy.

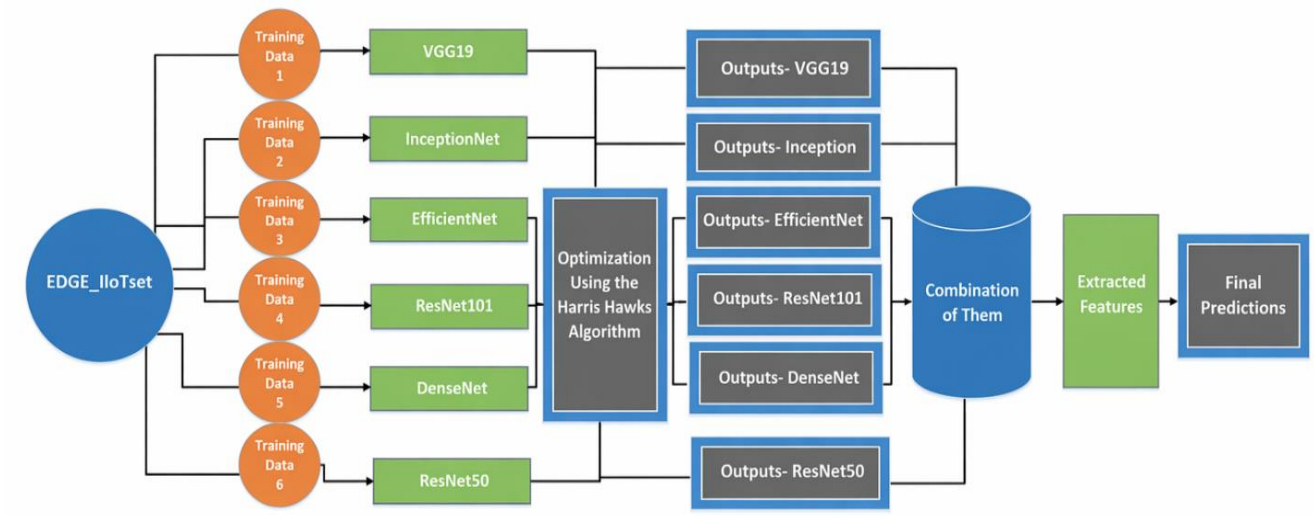
In the proposed method, the Edge-IIoTset dataset is first received as input and fed into base classifiers based on deep transfer learning (pre-trained networks). Then, the outputs of these classifiers are transferred to the second level as features. At this stage, the Harris Hawks Optimization algorithm is applied to obtain the optimal values of the hyperparameters. The output of this step is a probability

vector corresponding to the 14 classes available in the Edge-IIoTset dataset.

A probability vector implies that for each class in the Edge-IIoTset dataset, a probability value is assigned. The higher the probability of a sample belonging to a class, the greater the likelihood that the sample actually belongs to that class. The output of this stage includes optimized parameters obtained using the Harris Hawks Optimization algorithm. Finally, the model output is fed into a high-level machine learning classifier to generate the final output.

Figure 3

Proposed architecture of the optimized ensemble classifier



As shown in Figure 3, the architecture of the proposed ensemble layer is illustrated. In summary, the three main layers of this architecture include the following stages.

In the first stage, the input of this section is the Edge-IIoTset dataset, and based on this input, base deep transfer learning models are constructed.

In the second stage, hyperparameter optimization is performed using the Harris Hawks algorithm, and the optimal parameters are extracted from this stage.

In the third stage, the output of the previous stage is provided to a final classification layer using a high-level machine learning classifier, and the final output is obtained.

2.3.1. Construction of Base Deep Transfer Learning Models

In this section, the base models are constructed using six deep transfer learning architectures. As previously stated, deep transfer learning refers to transferring knowledge (weights obtained from pre-trained neural networks) from one dataset to another. These methods have been widely applied in various classification and image analysis tasks.

In the proposed architecture, six base classifiers based on deep transfer learning and convolutional neural networks (CNNs) are employed. These six architectures include VGG19, EfficientNetV7, ResNet101, ResNet50, DenseNet121, and InceptionV3. All these architectures are designed based on convolutional neural networks.

A CNN is a deep neural network widely used in image classification and consists of three main layers.

The convolution layer is responsible for extracting features from images.

The pooling layer is used for feature compression.

The fully connected layer is responsible for final classification and generating the output.

2.3.2. Hyperparameter Optimization Using the Harris Hawks Algorithm

In this section, the Harris Hawks metaheuristic algorithm is employed to obtain the optimal values of hyperparameters using the base models. Hyperparameter optimization has a significant impact on the final accuracy of the output. In many traditional methods, these parameters are typically tuned manually, which is a difficult and time-consuming task. This issue becomes more pronounced when a large number of layers and base networks are used. Moreover, manual parameter tuning is not universally applicable across all datasets.

In this study, the most important hyperparameters that have the greatest impact on the final accuracy of the model include the following.

The learning rate is one of the most critical hyperparameters in training deep models. It determines how quickly the model weights are updated during the learning process. A very high learning rate may lead to instability and loss of learning, while a very low learning rate reduces the convergence speed.

The dropout rate determines the proportion of neurons that are randomly deactivated in each layer during training. This technique helps prevent overfitting. Selecting an appropriate value improves the generalization capability of the model.

The number of dense layers refers to the fully connected layers used after convolutional layers. The selection of the number of these layers and the number of neurons in each layer plays a crucial role in the final accuracy.

The number of neurons in each dense layer is considered an optimizable parameter in each layer.

The batch size determines how many samples are used to update the weights in each iteration. An appropriate value can influence both the training speed and model accuracy.

The number of epochs represents the number of times the entire dataset is processed by the model. A large number of epochs may lead to overfitting, while a small number may result in insufficient training.

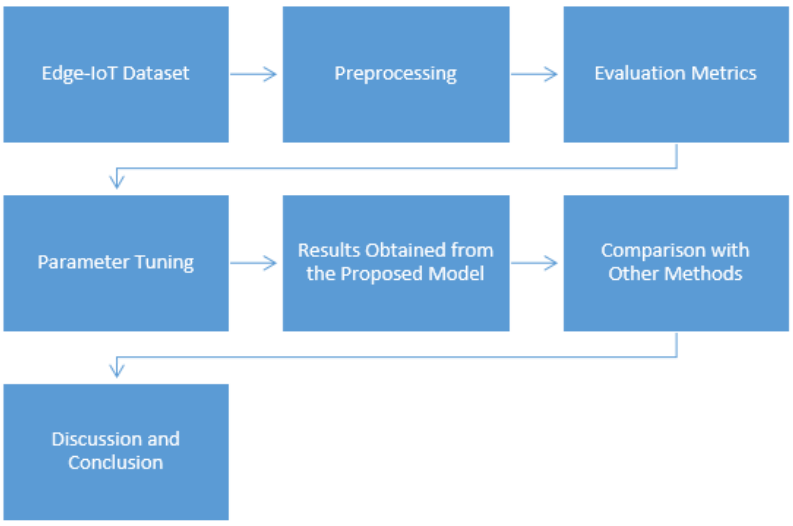
Considering that in the present problem, six or seven deep transfer learning networks are employed in an ensemble manner, each of these networks has a set of hyperparameters (learning rate, number of layers, number of neurons, and others) that affect model performance. The objective of this section is to determine the optimal combination of these hyperparameters for each network using the Harris Hawks Optimization algorithm.

3. Findings and Results

In this section, the simulations and experiments conducted on the proposed method are examined. The dataset is described in Section 4.1. Data preprocessing is explained in Section 4.2. Then, the evaluation metrics are presented in Section 4.3. After that, the parameters of the proposed model are tuned to achieve optimal values (Section 4.4). The results obtained from the proposed model are explained in Section 4.5. In addition, the proposed method is compared with several established and state-of-the-art methods (Section 4.6). The following figure illustrates the evaluation process of the proposed method.

Figure 4

Block diagram of implementation



3.1. Data Collection

Within the proposed framework, the Edge-IIoTset cybersecurity dataset is used for implementing and evaluating the method. This dataset is generated by simulating a real-world Internet of Things environment and includes more than 10 types of IoT-related devices. The dataset contains 14 categories of attacks associated with IoT communication protocols.

3.2. Preprocessing

One of the challenges in this dataset is the imbalance in the number of samples across classes. Some classes contain a very large number of samples, while others contain very few. For example, the DDoS_UDP class contains 121,567 samples, representing approximately 22% of the total samples, whereas classes such as MITM and FingerPrinting contain 358 and 853 samples, respectively, which account for less than 1% of the total samples. This issue reduces the model accuracy.

Initially, the data must be balanced. For resampling, an oversampling technique is applied to generate synthetic data for minority classes. In this study, a generative adversarial network (GAN)-based oversampling technique is employed for data balancing. In addition to increasing the number of samples in minority classes, this method also reduces redundancy and repetition issues in the dataset.

3.3. Evaluation Metrics

In this section, three main evaluation metrics are introduced: precision, recall, and accuracy. These metrics are used for performance evaluation and are defined in Equations (1) to (4).

$$\text{Precision} = \frac{TP}{TP + FN}$$

$$\text{Recall} = \frac{TP}{TN + FP}$$

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

$$F1\text{-Score} = \frac{2 \times (\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}}$$

Here, FP and FN represent incorrect predictions for each class, while TP and TN denote correct classifications. Clearly, the closer the values of TP and TN, the better the model performance. The main diagonal of the confusion matrix consists of TP and TN values.

3.4. Hyperparameter Tuning Using Harris Hawks Optimization

3.4.1. Tuning Transfer Learning Parameters Using HHO

As stated in the proposed method, three hyperparameters—learning rate, dropout rate, and the number of layers—have a significant impact on model accuracy. Therefore, the Harris Hawks Optimization (HHO) algorithm is used for tuning these parameters. These parameters are considered optimization variables, and the best combination is obtained using HHO.

To implement HHO, the PyHHO library must first be installed, and for each network, the optimal values of these parameters are extracted separately. The optimal values obtained for each hyperparameter across different transfer learning networks are presented in Table 1.

Table 1

Optimized Hyperparameters Obtained Using the Proposed HHO Algorithm

Network	Hyperparameters	Optimal Value by HHO
VGG19	Learning Rate	0.0015
	Dropout Rate	0.15
	Number of Dense Layers	2
	Number of Neurons per Layer	256
	Batch Size	128
	Number of Epochs	100
EfficientNetV7	Learning Rate	0.001
	Dropout Rate	0.18
	Number of Dense Layers	3
	Number of Neurons per Layer	256
	Batch Size	128
	Number of Epochs	100
ResNet101	Learning Rate	0.001
	Dropout Rate	0.15
	Number of Dense Layers	2
	Number of Neurons per Layer	128
	Batch Size	64
	Number of Epochs	100
ResNet50	Learning Rate	0.002
	Dropout Rate	0.15
	Number of Dense Layers	2

	Number of Neurons per Layer	256
	Batch Size	128
	Number of Epochs	120
DenseNet121	Learning Rate	0.002
	Dropout Rate	0.14
	Number of Dense Layers	3
	Number of Neurons per Layer	256
	Batch Size	128
	Number of Epochs	100
InceptionV3	Learning Rate	0.001
	Dropout Rate	0.12
	Number of Dense Layers	2
	Number of Neurons per Layer	256
	Batch Size	128
	Number of Epochs	100

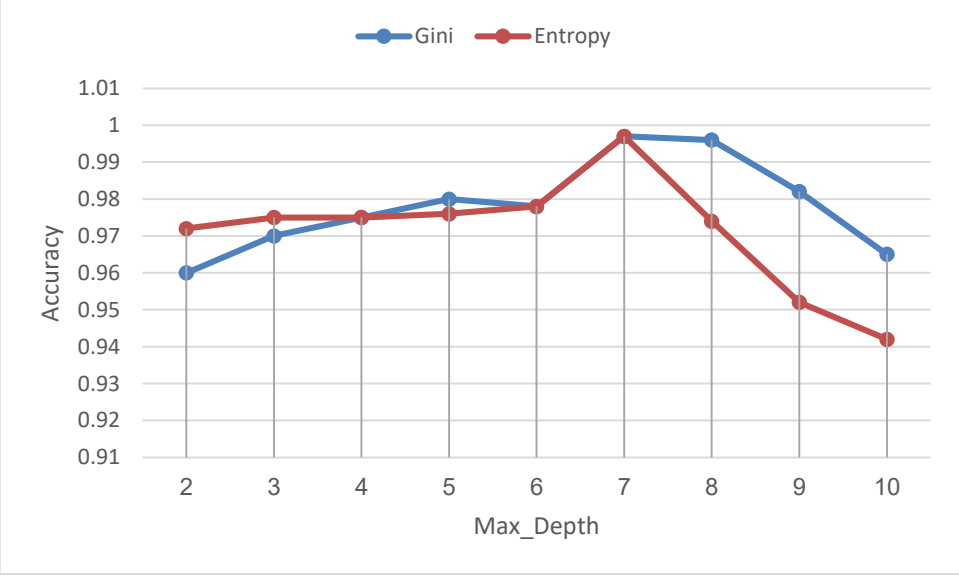
In each iteration, the HHO algorithm generates a new set of parameters, and the deep transfer learning models are trained using these parameters. Then, the validation accuracy of the model is calculated, and the algorithm moves toward the best parameter configuration. As shown in the table above, the learning rate ranges between 0.001and 0.003, the dropout rate ranges from 0.1to 0.5, the number of dense layers varies between 1and 3, the number of neurons per layer ranges from 64to 512, and the batch size ranges from 16to 128.

3.4.2. Tuning Random Forest Parameters

As explained in the previous section, the important parameters of the Random Forest algorithm were examined, and the best results are presented in Table 4. The obtained parameters were evaluated on the test dataset. Various experiments were conducted using different parameter settings to determine the optimal configuration for the Random Forest algorithm. These experiments were performed using both entropy and Gini criteria, as well as several maximum depth values ranging from 2 to 10. The accuracy results obtained for these configurations are illustrated in Figure 5.

Figure 5

Effect of Gini and Entropy criteria with different Max_Depth values on the dataset



As shown in Figure 5, with an increase in the Max_Depth value, the accuracy increases. The highest accuracy is achieved using the Gini criterion with Max_Depth = 7. After reaching the value of 7, the accuracy trend decreases.

Therefore, the optimal value for this parameter is 7. For other parameters, based on the conducted experiments, the values presented in Table 2 were obtained.

Table 2

Optimized Hyperparameters for Random Forest

Hyperparameter	Value
n_estimators	100
max_features	log2
max_depth	7
min_samples_split	2
min_samples_leaf	1
bootstrap	True
criterion	Gini

3.5. Experimental Results

In this section, the results obtained from the experiments are presented. The 5-fold cross-validation method is used for evaluation. Table 3 shows the results obtained on the training and testing datasets. Additionally, the values of precision, recall, and F1-score are illustrated in Figures 6, 7, and 8.

Table 3

Final Accuracy Obtained on Training and Test Datasets

Model	**Training Set (%)**	**Test Set (%)**
Proposed Model	100	99.978

Figure 6

Precision obtained on the dataset for training and test data

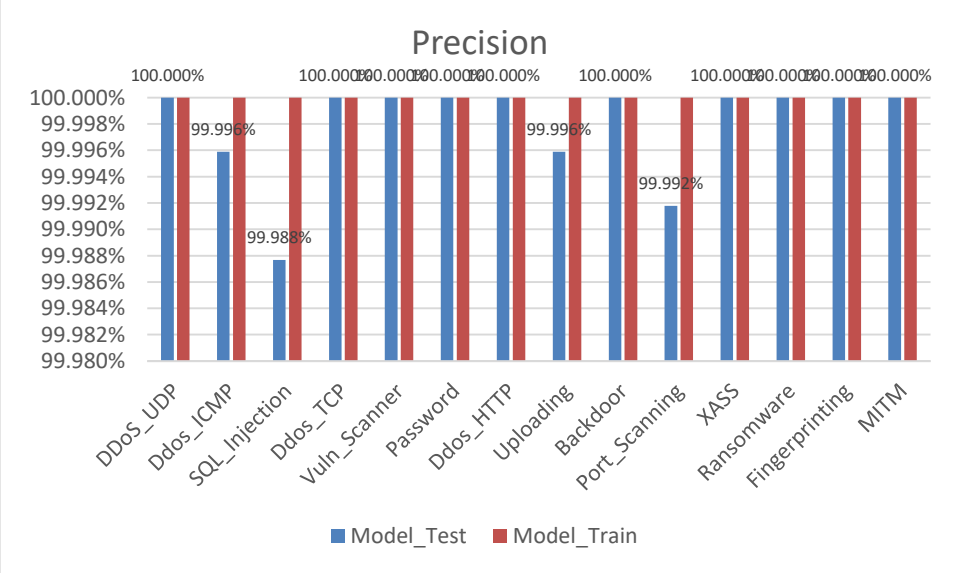
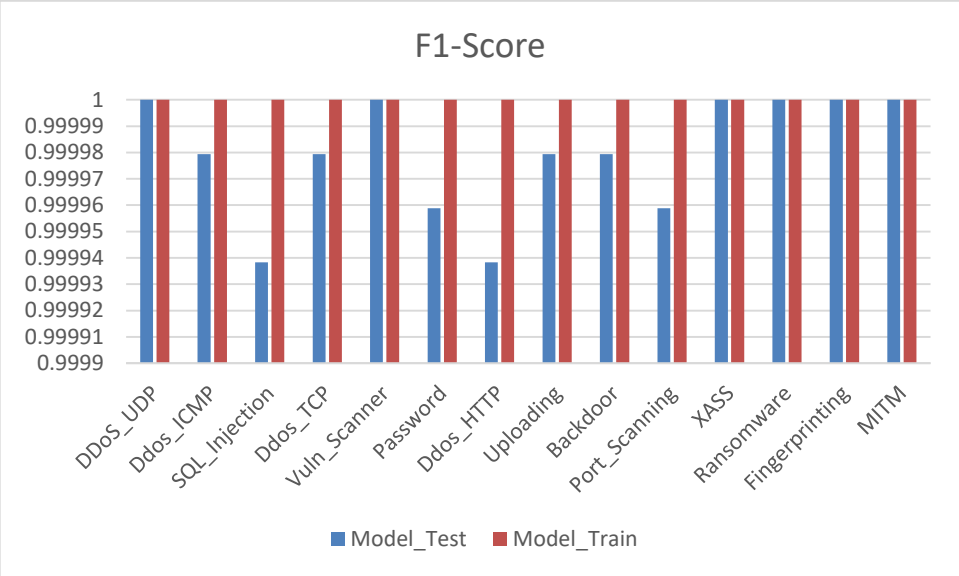


Figure 7

Recall obtained on the dataset for training and test data

Figure 8

Precision obtained on the dataset for training and test data



As shown in Figures 6, 7, and 8, the evaluation metrics including accuracy, recall, and F1-score are reported separately for the training and testing datasets. In the training dataset, all classes achieve 100% performance across all metrics. For the testing dataset, the accuracy is 100% for all classes, except for the classes "DDoS_ICMP," "SQL_Injection," "Uploading," and "Port_Scanning," where it is approximately 99.99%. Similarly, the recall is 100% for all classes, except for "DDoS_TCP," "DDoS_HTTP," "Password," and "Backdoor," where it is approximately 99.99%. Furthermore, the F1-score is 100% for all classes, except for "DDoS_TCP," "DDoS_HTTP," "Password," "Backdoor," "DDoS_ICMP," "SQL_Injection," "Uploading," and "Port_Scanning," where it is approximately 99.99%.

Considering that the proposed method utilizes an optimized ensemble classification approach, the accuracy of the model is significantly improved. This improvement is primarily due to the optimal parameter configuration, which plays a crucial role in enhancing the performance of neural

networks and consequently improving the final accuracy. This leads to a reduction in $FN$and FPvalues, thereby increasing overall accuracy.

3.6. Comparison with Previous Works

In this section, a final comparison between the proposed method and other approaches is presented. In recent years, various methods have been developed for detecting attacks on IoT devices; however, most of these methods suffer from limitations in accuracy or performance on real-world datasets.

The proposed method, by utilizing deep transfer learning, optimized ensemble classification, and the Harris Hawks Optimization algorithm, achieves a very high level of accuracy. The results obtained in this study are compared with several previous methods in Table 4.

Table 4

Comparison of the Proposed Method with Previous Works

Source	Dataset(s)	Method	Accuracy
(Hasan, 2023)	ROUT-4-2023	Hybrid intrusion detection system for RPL IoT networks using ML and DL	95%
(Shahid et al., 2024)	CICIDS2017	Deep learning model for IoT intrusion detection systems	95%
(Omar et al., 2023)	UNSW-NB15, CIC-IDS2018, CIC-IoT2023	Deep learning-based network intrusion detection system in IoT	98.2%
(Xiao et al., 2024)	BoT-IoT, CSE-CIC-IDS2018	End-to-end intrusion detection using deep learning	99.2%
(Yesi Novaria et al., 2024)	KDDCup-99, NSL-KDD, BoT-IoT, CICIDS-2017	IoT intrusion detection using deep learning and advanced optimization	96.7%
(Fatani et al., 2021)	BoT-IoT	IoT intrusion detection using deep learning	95.4%
(Dawoud et al., 2020)	BoT-IoT	Deep learning for IoT intrusion detection	96.7%
Proposed Method	Edge-IIoTset	Optimized ensemble hybrid classifier using HHO	99.8%

These methods utilize machine learning and deep learning algorithms to enhance security and detect intrusions in IoT networks. The proposed method achieves an accuracy of 99.8% using an optimized ensemble hybrid classifier with the Harris Hawks Optimization algorithm and significantly outperforms other approaches. The use of the Harris Hawks Optimization algorithm for precise parameter tuning improves adaptability and accuracy on the Edge-IIoTset dataset. This dataset is relatively recent and demonstrates the capability of the proposed method to address modern IoT security challenges.

For comparison, method (Hasan, 2023) achieves 95% accuracy on the ROUT-4-2023 dataset, which focuses on specific IoT routing vulnerabilities; however, its limited scope restricts its applicability in broader IoT environments. Method (Shahid et al., 2024) achieves 95% accuracy on CICIDS2017 using deep learning for threat detection, but its reliance on a specific dataset raises concerns about generalizability to newer datasets such as Edge-IIoTset. Method (Omar et al., 2023) demonstrates promising results on UNSW-NB15 and CIC-IDS2018; however, the absence of precise accuracy metrics makes direct comparison difficult. Method (Xiao et al., 2024) reports near-perfect accuracy (approximately 99.2%) on BoT-IoT and CSE-CIC-IDS2018, but the lack of detailed methodological explanations raises concerns regarding scalability and dataset adaptability. Older methods such as (Dawoud et al., 2020; Fatani et al., 2021) provide a historical perspective on the use of optimization and deep learning techniques but either do not report precise accuracy levels or fail to perform effectively on modern datasets.

4. Discussion and Conclusion

The findings of this study demonstrate that the proposed optimized ensemble classification framework based on deep transfer learning and Harris Hawks Optimization (HHO) achieves exceptionally high performance in detecting cyberattacks within IoT environments. Specifically, the model attained a near-perfect accuracy of 99.978% on the test dataset, alongside consistently high precision, recall, and F1-score values across almost all classes. These results indicate that the integration of transfer learning, ensemble classification, and metaheuristic optimization significantly enhances the capability of intrusion detection systems to accurately identify both normal and malicious traffic patterns. The negligible reduction in performance for a small subset of classes further highlights the robustness of the proposed framework in handling complex and imbalanced datasets.

The superior performance of the proposed model can be attributed to several interrelated factors. First, the use of deep transfer learning enables the model to leverage pre-

trained knowledge from large-scale datasets, thereby improving feature extraction and pattern recognition capabilities. This is consistent with prior studies that have demonstrated the effectiveness of transfer learning in enhancing model generalization and reducing training time in IoT intrusion detection tasks (Chen et al., 2023; Yan, 2024). Moreover, the ability of transfer learning models to adapt learned representations to new domains contributes to improved detection of previously unseen attack patterns, which is critical in dynamic IoT environments (Mehedi et al., 2022; Sahu et al., 2024).

Second, the ensemble learning strategy employed in this study plays a crucial role in improving detection accuracy. By combining multiple base classifiers, the proposed method effectively mitigates the limitations of individual models and enhances overall system reliability. This finding aligns with previous research indicating that ensemble approaches outperform single-model architectures by reducing variance and improving predictive stability (Bouke et al., 2023; Khanday et al., 2023). The integration of diverse deep learning architectures, including VGG19, ResNet variants, DenseNet, and Inception-based models, allows the system to capture complementary feature representations, thereby increasing the robustness of the detection process.

Another significant contributor to the observed performance improvements is the application of the Harris Hawks Optimization algorithm for hyperparameter tuning. The results indicate that optimizing key parameters such as learning rate, dropout rate, and network architecture leads to enhanced convergence and improved classification accuracy. This observation is supported by previous studies that emphasize the importance of metaheuristic optimization in achieving optimal model configurations (Gharehchopogh et al., 2023; Heidari et al., 2019). The ability of HHO to effectively explore the search space and identify optimal parameter combinations contributes to the reduction of both false positives and false negatives, thereby enhancing overall system performance.

Furthermore, the preprocessing and data balancing techniques employed in this study have a substantial impact on model performance. The use of GAN-based oversampling to address class imbalance ensures that minority classes are adequately represented during training, leading to improved detection accuracy across all classes. This finding is consistent with prior research highlighting the importance of balanced datasets in achieving reliable intrusion detection performance (Kaur et al., 2023). Additionally, normalization and outlier removal contribute to improved data quality, which in turn enhances model training and evaluation.

The results also demonstrate that the proposed model performs exceptionally well across different types of attacks, including DDoS, SQL injection, and port scanning. This indicates that the model is capable of capturing both low-level and high-level features associated with diverse attack patterns. Such capability is critical in IoT environments, where attacks can vary significantly in their characteristics and impact (Hasan, 2023; Rani et al., 2023). The high recall values observed in the results suggest that the model is particularly effective in identifying malicious activities, thereby reducing the risk of undetected attacks.

When compared with existing methods, the proposed approach significantly outperforms several state-of-the-art models reported in the literature. For instance, traditional machine learning-based intrusion detection systems typically achieve lower accuracy due to their reliance on handcrafted features and limited ability to capture complex patterns (Ahmad & Alsmadi, 2021; Thakkar & Lohiya, 2021). Similarly, deep learning-based models without optimization or ensemble mechanisms often suffer from issues such as overfitting and suboptimal parameter selection (Stefanos et al., 2022; Xiao et al., 2024). The integration of multiple advanced techniques in the proposed framework addresses these limitations and results in superior performance.

The findings of this study also contribute to the growing body of literature on hybrid intrusion detection systems that combine machine learning and deep learning approaches. Previous studies have demonstrated the effectiveness of hybrid models in improving detection accuracy and robustness (Omar et al., 2023; Shahid et al., 2024). The results of this study extend these findings by demonstrating that the addition of metaheuristic optimization further enhances model performance. This highlights the importance of integrating multiple complementary techniques in the design of advanced intrusion detection systems.

Another important implication of the results is the scalability and adaptability of the proposed framework. The use of transfer learning and metaheuristic optimization allows the model to be adapted to different IoT environments with minimal modifications. This is particularly important in real-world applications, where IoT networks are highly dynamic and heterogeneous (Heidari & Jabraeil Jamali, 2023; Sarker et al., 2023). The ability to maintain high

performance across diverse conditions underscores the practical applicability of the proposed method.

Despite the promising results, it is important to consider the broader context of IoT security and the challenges associated with deploying such models in real-world environments. While the proposed framework demonstrates high accuracy on the Edge-IIoTset dataset, further evaluation on additional datasets and real-time scenarios is necessary to fully assess its effectiveness. Moreover, the computational complexity associated with ensemble learning and optimization algorithms may pose challenges for deployment in resource-constrained IoT devices.

The overall findings of this study suggest that the integration of deep transfer learning, ensemble classification, and metaheuristic optimization represents a highly effective approach for improving intrusion detection in IoT environments. The results not only confirm the effectiveness of each individual component but also highlight the synergistic benefits of their combination. This study therefore provides valuable insights into the design of next-generation intrusion detection systems capable of addressing the evolving challenges of IoT security.

One limitation of this study is the reliance on a single dataset (Edge-IIoTset) for model training and evaluation, which may limit the generalizability of the results to other IoT environments with different characteristics. Additionally, the computational complexity of the proposed model, due to the use of multiple deep learning architectures and optimization algorithms, may hinder its real-time implementation in resource-constrained IoT devices. Another limitation is the potential sensitivity of the model to hyperparameter settings, despite the use of optimization techniques, which may require further fine-tuning for different applications.

Future research should focus on evaluating the proposed framework across multiple datasets and real-world IoT environments to validate its robustness and generalizability. Additionally, efforts should be made to reduce the computational complexity of the model through techniques such as model compression, pruning, or lightweight architectures. Further exploration of advanced optimization algorithms and hybrid approaches may also contribute to improved performance. Moreover, incorporating explainable artificial intelligence (XAI) techniques could enhance the interpretability of the model and facilitate its adoption in critical applications.

From a practical perspective, the findings of this study highlight the potential of advanced hybrid models in enhancing IoT security. Organizations and practitioners can leverage the proposed framework to develop more effective intrusion detection systems capable of identifying a wide range of cyber threats. Implementing such systems can improve the resilience of IoT networks, reduce the risk of cyberattacks, and support the secure deployment of IoT technologies in various domains.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethics Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were considered.

References

Ahmad, R., & Alsmadi, I. (2021). Machine Learning Approaches to IoT Security: A Systematic Literature Review. *Internet of Things*, *14*, 100365. https://doi.org/10.1016/j.iot.2021.100365

Bouke, M. A., Abdullah, A., Alshatebi, S. H., Abdullah, M. T., & El Atigh, H. (2023). An Intelligent DDoS Attack Detection Tree-Based Model Using Gini Index Feature Selection Method. *Microprocessors and Microsystems*, *98*, 104823. https://doi.org/10.1016/j.micpro.2023.104823

Chen, X., Yang, R., Xue, Y., Huang, M., Ferrero, R., & Wang, Z. (2023). Deep Transfer Learning for Bearing Fault Diagnosis: A Systematic Review Since 2016. *Ieee Transactions on*

Instrumentation and Measurement, *72*, 1-21. https://doi.org/10.1109/TIM.2023.3244237

Dawoud, A., Sianaki, O. A., Shahristani, S., & Raun, C. (2020). *Internet of Things Intrusion Detection: A Deep Learning Approach* 2020 IEEE Symposium Series on Computational Intelligence (SSCI), https://doi.org/10.1109/SSCI47803.2020.9308293

de Lima Filho, F. S., Silveira, F. A., de Medeiros Brito Junior, A., Vargas-Solar, G., & Silveira, L. F. (2019). Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning. *Security and Communication Networks*, *2019*(1), 1574749. https://doi.org/10.1155/2019/1574749

Fatani, A., Abd Elaziz, M., Dahou, A., Al-Qaness, M. A. A., & Lu, S. (2021). IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization. *IEEE Access*, *9*, 123448-123464. https://doi.org/10.1109/ACCESS.2021.3109081

Gharehchopogh, F. S., Abdollahzadeh, B., Barshandeh, S., & Arasteh, B. (2023). A Multi-Objective Mutation-Based Dynamic Harris Hawks Optimization for Botnet Detection in IoT. *Internet of Things*, *24*, 100952. https://doi.org/10.1016/j.iot.2023.100952

Hasan, M. (2023). DDoS: Distributed Denial of Service Attack in Communication Standard Vulnerabilities in Smart Grid Applications and Cyber Security with Recent Developments. *Energy Reports*, *9*, 1318-1326. https://doi.org/10.1016/j.egyr.2023.05.184

Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of Things Intrusion Detection Systems: A Comprehensive Review and Future Directions. *Cluster Computing*, *26*(6), 3753-3780. https://doi.org/10.1007/s10586-022-03776-z

Heidari, A. A., Mirjalili, S., Faris, H., Aljarah, I., Mafarja, M., & Chen, H. (2019). Harris Hawks Optimization: Algorithm and Applications. *Future Generation Computer Systems*, *97*, 849-872. https://doi.org/10.1016/j.future.2019.02.028

Jiang, Z. (2025). AI-Driven Market Demand Forecasting for IoT Hardware in Smart Buildings: Implications for Investment in the Digital Economy. *GBP Proceedings Series*, *14*, 163-169. https://doi.org/10.70088/hsm3ap94

Jin, S., & Karki, B. (2025). Integrating IoT and blockchain for intelligent inventory management in supply chains: A multi-objective optimization approach for the insurance industry. *Journal of Engineering Research*, *13*(2), 527-537. https://doi.org/10.1016/j.jer.2024.04.021

Kaur, B., Dadkhah, S., Shoeleh, F., Neto, E. C. P., Xiong, P. a. I. S., Lamontagne, P., Ray, S., & Ghorbani, A. A. (2023). Internet of Things (IoT) Security Dataset Evolution: Challenges and Future Directions. *Internet of Things*, *22*, 100780. https://doi.org/10.1016/j.iot.2023.100780

Khanday, S. A., Fatima, H., & Rakesh, N. (2023). Implementation of Intrusion Detection Model for DDoS Attacks in Lightweight IoT Networks. *Expert Systems with Applications*, *215*, 119330. https://doi.org/10.1016/j.eswa.2022.119330

Marcus, L., Zhang, Y., & Patel, R. (2025). The impact of intelligent systems, big data, and IoT on management accounting. *Journal of Emerging Technologies in Accounting*, *22*(1), 15-32.

Mehedi, S. T., Anwar, A., Rahman, Z., Ahmed, K., & Islam, R. (2022). Dependable Intrusion Detection System for IoT: A Deep Transfer Learning Based Approach. *IEEE Transactions on Industrial Informatics*, *19*(1), 1006-1017. https://doi.org/10.1109/TII.2022.3164770

Mustapha, A., Chbib, F., Fadlallah, A., Fahs, W., & El Attar, A. (2023). Detecting DDoS Attacks Using Adversarial Neural Network. *Computers & Security*, *127*, 103117. https://doi.org/10.1016/j.cose.2023.103117

Omar, E., Eman, S., Mohamed, M., & Karim, E. (2023). EIDM: Deep Learning Model for IoT Intrusion Detection Systems. *Journal of Supercomputing*, *79*, 13241-13261. https://doi.org/10.1007/s11227-023-05197-0

Radhika, R., & Kulothungan, K. (2019). Mitigation of Distributed Denial of Service Attacks on the Internet of Things. *Applied Mathematics and Information Sciences*, *13*(5), 831-837. https://doi.org/10.18576/amis/130517

Rani, S. J., Ioannou, I., Nagaradjane, P., Christophorou, C., Vassiliou, V., Charan, S., Prakash, S., Parekh, N., & Pitsillides, A. (2023). Detection of DDoS Attacks in D2D Communications Using Machine Learning Approach. *Computer Communications*, *198*, 32-51. https://doi.org/10.1016/j.comcom.2022.11.013

Sahu, M., Dash, R., Mishra, S. K., Humayun, M., Alfayad, M., & Assiri, M. (2024). A Deep Transfer Learning Model for Green Environment Security Analysis in Smart City. *Journal of King Saud University-Computer and Information Sciences*, *36*(1), 101921. https://doi.org/10.1016/j.jksuci.2024.101921

Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2023). Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions. *Mobile Networks and Applications*, *28*(1), 296-312. https://doi.org/10.1007/s11036-022-01937-3

Shahid, U., Hussain, M. Z., Hasan, M. Z., Haider, A., Ali, J., & Altaf, J. (2024). Hybrid Intrusion Detection System for RPL IoT Networks Using Machine Learning and Deep Learning. *IEEE Access*, *12*, 113099-113112. https://doi.org/10.1109/ACCESS.2024.3442529

Sharma, D., Mishra, I., & Jain, S. (2017). A Detailed Classification of Routing Attacks Against RPL in Internet of Things. *International Journal of Advance Research, Ideas and Innovations in Technology*, *3*(1), 692-703.

Stefanos, T., Thomas, L., & Konstantinos, R. (2022). Deep Learning in IoT Intrusion Detection. *Journal of Network and Systems Management*, *30*. https://doi.org/10.1007/s10922-021-09621-9

Thakkar, A., & Lohiya, R. (2021). A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges. *Archives of computational methods in engineering*, *28*(4), 3211-3243. https://doi.org/10.1007/s11831-020-09496-0

Tseng, F. H., Chou, L. D., & Chao, H. C. (2011). A Survey of Black Hole Attacks in Wireless Mobile Ad Hoc Networks. *Human-Centric Computing and Information Sciences*, *1*, 1-16. https://doi.org/10.1186/2192-1962-1-4

Van Houdt, G., Mosquera, C., & Nápoles, G. (2020). A Review on the Long Short-Term Memory Model. *53*(8), 5929-5955. https://doi.org/10.1007/s10462-020-09838-1

Xiao, W., Lie, D., & Guang, Y. (2024). A Network Intrusion Detection System Based on Deep Learning in the IoT. *80*, 24520-24558. https://doi.org/10.1007/s11227-024-06345-w

Yan, T. (2024). A Comprehensive Survey of Deep Transfer Learning for Anomaly Detection in Industrial Time Series: Methods, Applications, and Directions. *IEEE Access*.

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet of Things. *Ieee Internet of Things Journal*, *4*(5), 1250-1258. https://doi.org/10.1109/JIOT.2017.2694844

Yesi Novaria, K., Siti, N., Deris, S., & Bhakti, Y. S. (2024). An End-to-End Intrusion Detection System with IoT Dataset Using Deep Learning with Unsupervised Feature Extraction. *International Journal of Information Security*, 1619-1648. https://doi.org/10.1007/s10207-023-00807-7

Zhao, X., Zhang, Y., Han, X., Deveci, M., & Parmar, M. (2024). A Review of Convolutional Neural Networks in Computer

Vision. *57*(4), 99. https://doi.org/10.1007/s10462-024-10721-6

Zong, Y., & Huang, G. (2021). A Feature Dimension Reduction Technology for Predicting DDoS Intrusion Behavior in Multimedia Internet of Things. *Multimedia Tools and Applications*, *80*(15), 22671-22684. https://doi.org/10.1007/s11042-019-7591-7