ISSN: 2834-4928

Research Article

Journal of Electrical Electronics Engineering

Towards a New Approach-Driven Intrusion Detection in IoT Network

Noura Ben Henda[1], Imen Hagui[1]* and Abdelhamid Helali[2]

[1]*LMON, Faculty of Science, Monastir University, Monastir, Tunisia*

[2]*ISIMM, Monastir University, Monastir, Tunisia*

***Corresponding Author**
Imen Hagui, LMON, Faculty of Science, Monastir University, Monastir, Tunisia.

Submitted: 2026, Feb 04; **Accepted**: 2026, Mar 23; **Published**: 2026, Mar 30

Citation: Henda, N. B., Hagui, I., Helali, A. (2026). Towards a New Approach-Driven Intrusion Detection in IoT Network. *J Electrical Electron Eng, 5*(2), 01-12.

Abstract

The integration of Internet of Things (IoT) with artificial intelligence and smart devices (SD) in agriculture has revolutionized traditional farms and significantly improve the productivity and food production. Although the advantage offered by this combination, it still faces security challenges. To fix this problem and ensuring the resilience and reliability of smart agriculture (SA) systems, we propose an advanced network intrusion detection system (NIDS) to detect and address new threats in IoT networks. In this work, we design and evaluate a deep learning-based network intrusion detection system (DL-NIDS) that can successfully identify and detect intrusions in smart agriculture network. The experiment accomplished on three well known datasets namely, NSL-KDD, CIC-IDS-2017, and EdgeIIoTset, demonstrated the effectiveness of our system against the state-of-the-art approaches.

Keywords: Cybersecurity, IoT, Network Intrusion Detection System, Deep Learning, CNN, SVM, Smart Agriculture, Agriculture 4.0

1. Introduction

The widespread integration of Internet of Things (IoT) has fundamentally transformed multiple facets of contemporary existence, including sectors such as smart homes, urban infrastructures, healthcare, and agriculture. Despite the benefits they supply, the growth of IoT devices has posed numerous security vulnerabilities. This is mostly due to the fact that numerous interconnected devices with inadequate built-in security measures, rendering them susceptible to a broad spectrum of cyberattacks. Moreover, the deep interconnectivity of IoT networks amplifies the complexity of their vulnerability to attacks, requiring the implementation of advanced security measures. Effective defense against potential intrusion and malicious actions necessitates the implementation of proactive protection measures, as well as ongoing awareness to neutralize growing threats posed by cyber attackers.

Even though the increased awareness of IoT security issues, existing security measures are sometimes insufficient to defend against the widening range of threat. Conventional intrusion detection system (IDS) are intended primarily for traditional networks and may inadequately identify and mitigate threats targeting IoT devices and networks. Therefore, the necessity for specialized security solutions adapted to inherent features of IoT environments. These solutions must integrate advanced anomaly detection algorithms, real-time threat intelligence feeds, and behavior-based analytics to detect and address new threats in IoT networks. Furthermore, robust encryption protocols, secure authentication methods, and firmware-level security measures are essential for protecting IoT devices from potential vulnerabilities and illegal access. Moreover, ongoing surveillance and automated incident response mechanisms are crucial for maintaining a proactive security stance and mitigating the effects of security breaches on IoT deployments.

In order to protect smart agriculture (SA) environment, proactive security measures are needed, as demonstrated by recent events like Denial of Service attack which overwhelm the network to render devices unreachable [1]. Current research in the field of IoT security have predominantly concentrated on encryption protocols, access control mechanisms, and anomaly detection techniques. The dynamic and varied characteristics of IoT networks pose distinct challenges for intrusion detection, requiring the development of specific solutions designed for IoT environments.

Intrusion detection system play a critical role in securing IoT networks, especially when powered by powerful machine learning and deep learning algorithms. These systems offer several key benefits. First of all, machine learning and deep learning-based IDS can autonomously learn and adapt to new threats enabling real-time detection and response capabilities that traditional rule-based system struggle to achieves. This flexibility enables them to detect previously new threats, decreasing false positives. Second, ML/DL-based IDS models can analyze enormous amounts of IoT data, recognizing complicated patterns with high accuracy. This functionality improves the overall security posture of IoT networks by quickly detecting and mitigation threats. In addition, these IDSs can seamlessly interface with other security measures and IoT devices, offering a holistic security framework that can proactively defending against sophisticated cyber-attacks. In general, the incorporation of ML/DL algorithm into IDS boosts the security resilience of IoT networks, making them more robust and capable of fighting against a wide range of cyber-attacks.

As shown in figure 1, the intrusion detection system (IDS) comprises several sequential steps to monitor and protect network environment from unauthorized access and malicious activities. These steps include the collection of data from monitored IoT network. The collected data is then forwarded to be processed and analyzed using sophisticated algorithms and rules to identify potential security incidents. The step of intrusion identification relies on the intrusion database (Intrusion DB) which contain known attack signatures and anomaly detection techniques to distinguish between normal and suspicious activities. Once an anomaly or potential threat is detected, the IDS generates alerts, such as blocking suspicious traffic or notifying security administrator. Additionally, IDS systems often include a reporting and logging component that records detected events, provides insights into security incidents, and facilitates forensic analysis. Overall, these components constitute a robust security mechanism that enables enterprises and organizations proactively identify and address cyber-threats in real.

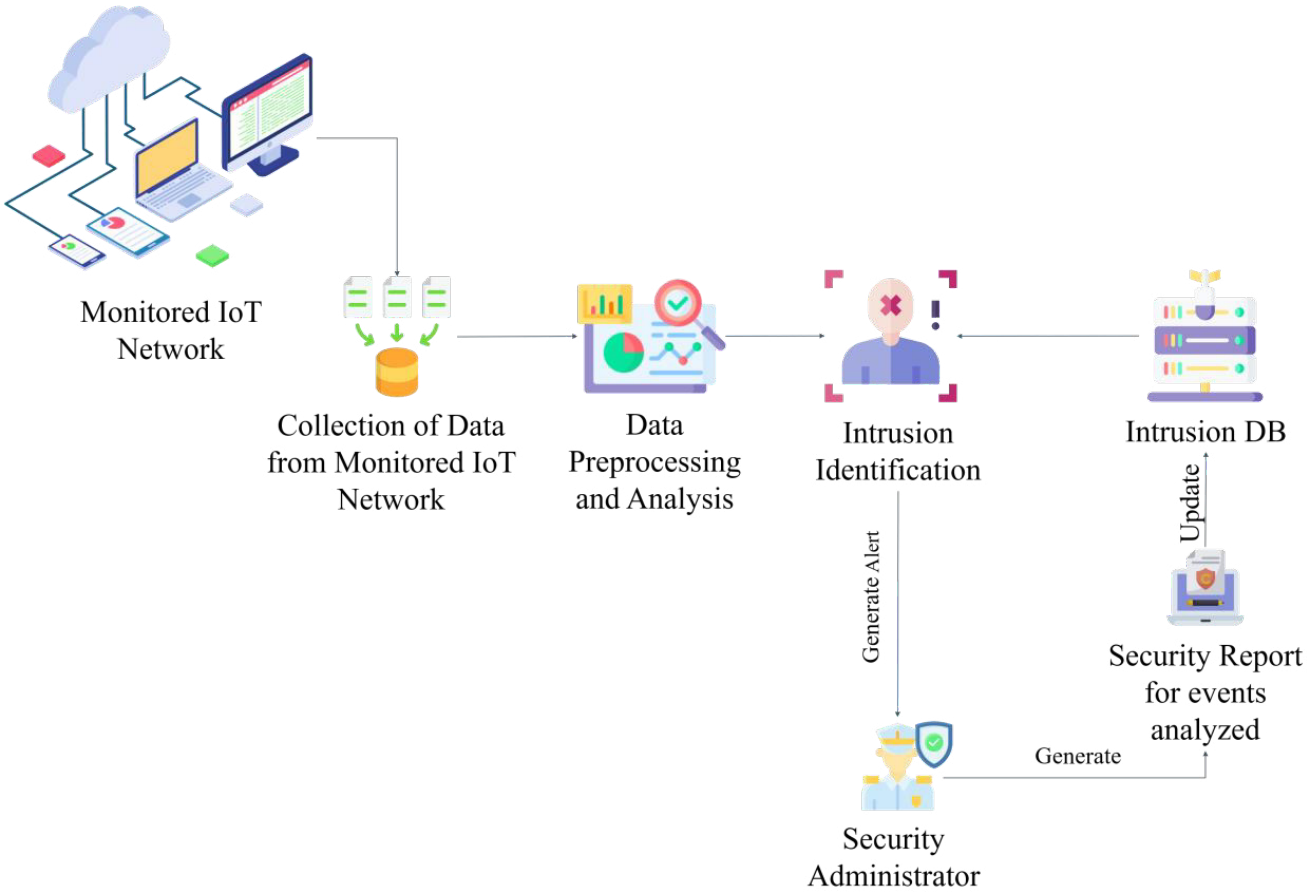

Figure 1: Typical Model of Intrusion Detection System in IoT Network

Intrusion detection system can be developed in two principal forms according to the detection mode; signature-based detection and anomaly-based detection. Signature based intrusion detection (SIDS) also known as knowledge-based detection. In this mode of detection, the IDS match the knowledge stored in its database with the detected threat to recognize intrusions [2]. The most common detection method is, Anomaly-based intrusion detection (AIDS), which identify malicious activities by comparing it with the normal behavior profile and in this step, it can be interpreted as an intrusion [3].

In this paper, we propose a new approach to enhancing the security of smart agriculture networks through the development of deep learning-based network intrusion detection system (DL-NIDS). The primary objective of our research is to design and evaluate a DL-NIDS capable of effectively detecting and mitigating intrusions in smart agriculture networks. NIDS act as a crucial line of defense in SA networks, since agricultural devices are online most of the time, which is necessary to monitor network activity and report any malicious, unauthorized or unusual events that might endanger the information, availability, or security of data.

The remainder of this paper is organized as follows: Section 2 present an overview of agriculture 4.0 evolution, technology integrated, advantages, and challenges related to cybersecurity of smart devices. Section 3 include a comprehensive review of related works in the field of IoT security and intrusion detection. In section 4, we present the design and the implementation of our proposed DL-NIDS in SA network, detailing the algorithms employed. Section 5 describes the methodology followed to evaluate the performance of DL-NIDS, evaluation metrics, and validation environment. Then, we present and discuss the results of our experiments followed by critical analysis of the findings and implications in section 6. Finally, in section 7 we present the conclusion of our work.

2. Agriculture 4.0

The development of agriculture from agriculture 1.0 to agriculture 4.0 has played an important role in shaping global food production [1]. The integration of innovative technologies such as the internet of things, artificial intelligence, and smart devices have revolutionized traditional farming practices into data-driven, automated, and efficient.

The integration of smart devices in agriculture has significantly improved productivity, efficiency, and sustainability. Smart sensors and automated irrigation systems have significantly served as essential components of these technologies. Automated irrigation systems control water distribution based on real-time soil moisture data recorded using soil sensors in order to minimize water waste and conserving resources. Beyond of these technologies, Unmanned Aerial vehicles (UAVs), another revolutionary technology in modern agriculture playing a crucial role in enhancing agricultural productivity and food production. These UAVs are commonly used for crop health assessment, field mapping, and they are also allowing for rapid and accurate monitoring of large farmlands. Which one of their ability is to assess crop conditions in real time contributes significantly to improving food production efficiency and reducing resource waste? Together, these smart devices not only increase agricultural productivity but also support the global effort to meet the increasing demand for food in a sustainable manner.

While the adoption of smart agriculture technologies offers numerous advantages in optimizing food production and resource management, it also presents significant challenges particularly related to security and data privacy. However, the large-scale utilization of smart devices in SA also increases the risk of cyberattacks on smart devices. For instance, Distributed Denial of service (DDoS) attacks have the ability to overwhelm systems and make them unusable, while ransomware attacks may negatively impact on farm operations by preventing access to vital data. To ensure the resilience and reliability of SA systems, advanced cybersecurity solutions must be implemented to address these security threats, which remains a critical challenge.

3. Related Works

Researchers have achieved great progress in the field of intrusion detection with machine learning. They are developing more accurate and effective machine learning methods for detecting cyber-attacks. Several studies have explored this potential, including which proposes an ML-IDS for IoT that use two type of algorithm named k-means and decision tree, and employs a new hypervisor-based cloud IDS which employs the effectiveness of logistic regression (LR), random forest (RF), and support vector machine (SVM) [4,5].

Even though machine learning is an effective technique for intrusion detection, system that rely exclusively on ML algorithm may suffer from performance deficiencies. This is due to the irrelevant or redundant features that can decrease accuracy and increase false alarm rate. To address this issue many researchers have incorporated feature selection or optimization technique before model training. In this area, several studies have been conducted to prove the impact of feature selection on the accuracy of IDS, including which we have employed correlation-based feature selection (CFS) technique to discard irrelevant features from the NSL-KDD dataset and implemented the IDS model based on SVM algorithm. Gradient boosting is proposed in as feature selection technique to improve the performance of the model, which they implement and evaluate various decision tree-base classifier [6,7].

Al-Janabi et al. employs new teaching learning-based optimization algorithm (NTLBO) for feature selection and three different machine learning model such as SVM, extreme learning machine (ELM) and LR for classification purposes [8]. Reyes et al. evaluated a wireless network intrusion detection system (WNIDS) for WiFi networks on different machine learning techniques; boostrap aggregation (Bagging), random forest, extra trees, extrem gradient boosting (XGBoost), and naive bayes (NB). The authors proposed several feature selection techniques such as recursive feature elimination (RFE), feature importance, chi-square test, feature correlation, and particle swarm optimization (PSO) to identify the best features set. In another research paper presented by Naseri et al. the feature selection called binary version of farmland fertility algorithm (BFFA) with the v-shaped function plays an important role in increasing model performance [9,10].

Deep learning algorithm comes to offer some distinct advantages over traditional machine learning including better handling of complex data, automatic feature extraction, and higher accuracy in specific tasks. Researchers have benefits from the advantages to enhance the security in IoT network, particularly in the field of intrusion detection system. for example, Nguyen et al. proposed a multimodal classifier that includes three DL models to distinct between normal and abnormal data. Their approach includes an optimization algorithm called chaotic butterfly optimization (CBO) applied for feature selection before training [11]. The authors analyzed the performance of proposed model using NSL-KDD dataset. Zhiqiang et al. proposed an empirical based component analysis to discard irrelevant features from dataset, and long short-term memory (LSTM) as algorithms to train the model [12]. The performance validation of this model. The performance validation of this model was evaluated on four well known dataset called; KDDCUP-99, CICIDS-2017, UNSW-NB15, and NSL-KDD.

Mayuranathan et al. developed and effective optimal security solution for intrusion detection system (EOS-IDS). In EOS-IDS model, authors suggested two optimization technique; one for removing unnecessary feature called improved heap optimization (IHO), and the other was for dimensionality reduction called chaotic red deer optimization (CRDO) [13]. This study aimed to identify cyber-attacks by using deep kronecker natural network (DKNN) technique applied on CSE-CIC-IDS2018 and DARPA datasets.

In the authors presented a strategy to improve the efficacy of deep neural networks (DNNs) for intrusion detection [14]. Their approach employs feature selection through the integration of statistical significance criteria, such as standard deviation and the disparity between mean and median. To illustrate the effectiveness of their proposed model, the researchers assessed it on three intrusion detection benchmark datasets: NSL-KDD, CICIDS-2017, and UNSW-NB15. Their goal was probably to attain enhanced performance on these datasets.

Kanna et al. proposed an IDS model built based on deep learning algorithm named black window optimized convolutional long short-term memory (BWO-CONV-LSTM) [15]. They employed an artificial bee colony algorithm for feature selection in order to perform the accuracy of the model. Their model was tested on different dataset including NSL-KDD, UNSW-NB15, and ISCX-IDS.

To effectively identify and thwart cyber-attacks, a hybrid metaheuristic method named GTO-BSA for feature selection was developed were GTO refers to gorilla troops optimizer and BSA refers to bird swarm's algorithm. The authors of this work tested the reliability of this hybrid metaheuristic method on four IoT dataset named NSLKDD, CICIDS-2017, UNSW-NB15, and Bot-IoT [16].

In fatani et al. proposed an intrusion detection system based on deep learning and optimization technique. In their research strategy, the authors lunched the search of optimal features by applying CNN to extract features, then they used modified version growth optimizer (MGO) for feature selection and to boost the search process of GO they used whale optimization algorithm (WOA) [17]. They used CNN algorithm to analyse traffic stored in IoT and cloud environments datasets named KDD-CUP99, NSL-KDD, CICIDS2017, and BoT-IoT.

Researchers are making significant strides in the field of intrusion detection using machine learning. By leveraging the power of machine learning algorithms, researchers are developing more accurate and efficient methods for identifying and preventing cyber-attacks. One promising approach involves using machine learning to classify network traffic into normal and anomalous patterns. This allows researchers to identify malicious activity in real time and take immediate action to protect networks from harm.

In addition to developing new intrusion detection techniques, researchers are also working on improving the performance of existing methods. this includes reducing false positives, which can occur when a legitimate activity is mistakenly identified as an attack. Researchers are also working on making intrusion detection system more scalable, so that they can be deployed on large and complex networks.

The use of machine learning for intrusion detection is a rapidly evolving field with the potential to recognize cyber-security. As researchers continue to make progress, we can expect to see even more effective and efficient methods for protecting networks from cyber-attacks.

Ferrag et al. analyzed seven deep learning models named RNN, DNN, RBM, DBN, CNN, DAE, and DBM. They studied the performances of the realistic datasets named CSE-CIC-IDS2018 and Bot-IoT [18]. They compared the previous model based on the following metrics, named, accuracy, false alarm rate, and detection rate.

Gamage et al. conducted an extensive survey on relevant literature, synthesizing key findings and methodologies. Moving beyond a review, they train and evaluate four critical deep learning architectures named feed forward neural networks, autoencoders, deep belief networks, and long short-term memory networks on a variety of datasets [19]. They specifically evaluated the performance of these models on KDD-CUP99, NSL-KDD, CIC-IDS2017, and CIC-IDS2018. Their experiments provide clear conclusions: FFNN perform well on all datasets, while autoencoders and DBN, which are semi-supervised methods, are not effective as supervised ones.

Ge et al. proposed an innovative intrusion detection approach for the security of internet of things based on a customized deep learning algorithm. They developed a feed-forward neural network model with embedding layers to efficiently encode high-dimensional categorical data for multi-class classification. Subsequently, they employed transfer learning techniques to autonomously encode these attributes for binary classification task, utilizing a second feed-forward neural network model [20]. For the assessment of the suggested strategy, they employed Bot-IoT, an advanced IoT dataset that contains IoT traces.

4. System Model and Methods

In this section, we present the system model and the methods employed in this paper while highlighting their essential role for securing smart agriculture network.

Figure 2 illustrates the integration of NIDS in SA environment. The architecture includes multiple smart interconnected devices such as sensors, drones and edge gateways that establish connections across agricultural fields for the monitoring and the automation of farming procedures. The system integrates centralized network intrusion detection system for continuous traffic monitoring which detects suspicious behavior to handle potential attacks such as denial of service. The merged system establishes a protected agricultural network with data integrity protection alongside system availability security and protection of operation sensitive data from cyberattacks. The model presented in the illustration creates a base for the threat mitigation approaches which will be described in upcoming sections of this work.

In this study we employ two machine learning models: Convolutional Neural Network and Support Vector Machine. The selected methods suited this application because they support each other in solving intricate classification problems. The structure of CNNs enables them to identify sophisticated hierarchical patterns in data structures which results in effective detection of concealed malicious patterns within network traffic data. SVMs excel in high dimensional spaces along with handling small and balanced datasets which results in robust generalization capabilities. Both models used together create a platform to analyze deep learning and classic machine learning approaches for intrusion detection evaluation purposes. The researchers exclude alternative techniques because they encountered scalability issues or implemented analytical methods with sub-optimal results when detecting intrusions within similar network defense environment.

a. Convolutional Neural Network

Convolutional Neural Networks (CNNs) are a class of deep learning models widely developed for image recognition tasks. They have demonstrated exceptional performance in extracting special hierarchies of features through layers of convolution, pooling, and nonlinear transformations. In a CNN architecture, raw input data passes through multiple processing layers, starting from low-level extraction to high level decision making in fully connected layers, ultimately to classification.

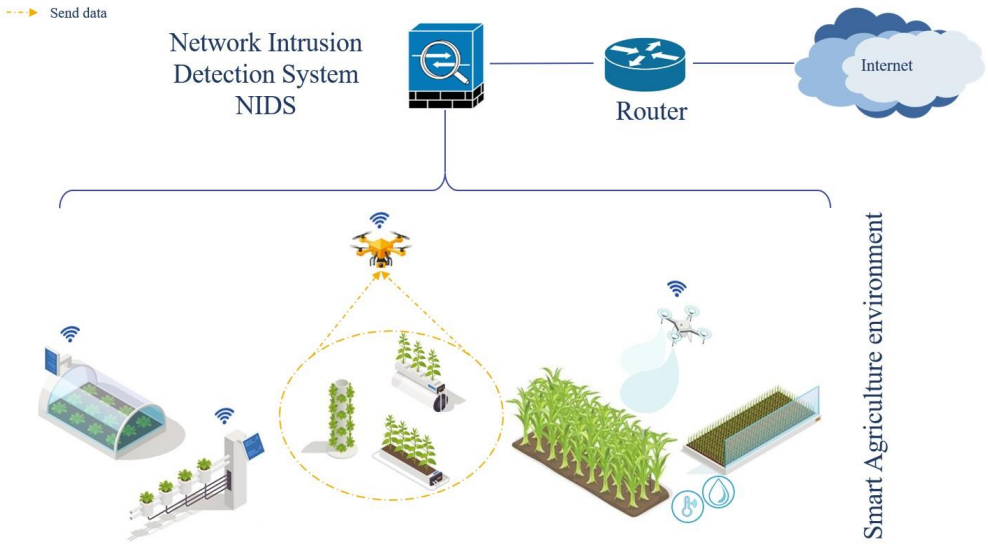

Figure 2: System Overview of Network Intrusion Detection System in Smart Agriculture Networks

The main element of CNN is the convolution layer, which apply a set of learnable kernels to process the input. The equation behind convolution layer can be written as follow; $h_j = f(h_{j-1} * w_j + b_j)$, where $*$ is the convolution function, f is the activation function (typically ReLu used defined as $f(x) = max(0, x)$), w_j is the weight value of the kernel function of layer j, b_j is the bias of the layer j, h_{j-1} is the output or the Feature Map, and h_{j-1} is the input sample. Following convolution, data processing continues through pooling layers which is responsible of reducing the dimension of each Feature Map by keeping the most important information for better generalization of the Feature Map (h_j) [21]. After several convolution and pooling layers, the output flows through one or multiple fully connected layers with connections to all previous layer activations before reaching the final output layer which makes classification decisions (normal or malicious traffic) using a Softmax function mathematically expressed as

$$\sigma(z_i) = \frac{e^{z_i}}{\sum_{j=1}^{K} e^{z_j}} \quad \text{for } i = 1, 2, \ldots, K \text{, where } K \text{ is the total number of classes.}$$

In the context of network traffic analysis, CNN can be adapted to analyze network traffic data. This data is often represented in structured format, such as matrices derived from network flow features, enabling CNNs to treat network activity like special data or "image". This unique interpretation allows CNNs to learn both local and global patterns in the traffic data, distinguishing between normal and abnormal behavior.

The application of CNN in the process of intrusion detection succeeds in different real word situation. CNN-based IDS succeed in identifying different type of attacks such as Denial of service, port scans and botnet traffic in enterprise networks and critical infrastructure systems [22].

b. Support Vector Machine

Support Vector Machine (SVM) finds extensive use in classification tasks including intrusion detection. The SVM algorithm employs optimization methods to discover the perfect boundary plane that procedures maximum separation between assigned data points. In binary classification scenario, when the objective is to differentiate between normal and malicious traffic, SVM develops its decision boundary hyperplane to maximize the separation distance between the closest points from each category known as support vectors. This makes SVM effective in generalizing well to unseen data, especially in high-dimensional feature spaces commonly encountered in network traffic analysis.

The main purpose of SVM is to create weight vector w and bias term *b* for establishing a decision boundary (hyperplane), which can be written as follow:

$$f(x) = w^T * X + b \quad (1)$$

Where, X represent the set of feature vector X_i in the dataset (i represent the dataset dimension).

In case of non-linearly separable data, SVM use kernel function like radial basic function (RBF) or polynomial kernels to create high-dimensional space where linear separators apply. This option proves the adaptability of SVM during operation and makes it suitable for complex intrusion patterns.

5. Methodology

In this section, we present the adopted methodology in this approach to detect and classify intrusions over SA network. Figure 3 illustrates the process leading to the classification of network attacks using our model which involves multiple necessary preprocessing steps designed to refine the raw data for efficient and accurate analysis.

Initially, we examined the dataset to check data integrity through a preliminary review which removed any corrupted or missing data points. In the next step, the redundant and the irrelevant features were deleted in order to reduce noise in the system and improve model performance.

Then, categorical features were encoded into numerical format helped machine learning algorithms accept it, while numerical features received normalization treatment for unified measurement across all features using *StandardScaler* mathematically defined as z = (x − u)/s, where u is the mean of samples, s is the standard deviation of samples, and x represent the sample itself. The preprocessing ended by splitting data into train and test parts, with 80% of the data used for training and the remaining 20% reserved for testing enabled the assessment of model generalization performance.

In the case of CNN model, the data required to be transformed to match convolution layers, while for SVM classifier demand vector-form data. Finally, the preprocessed data entered the models which were followed for training and evaluation purposes to perform network intrusion detection and classification with improved accuracy.

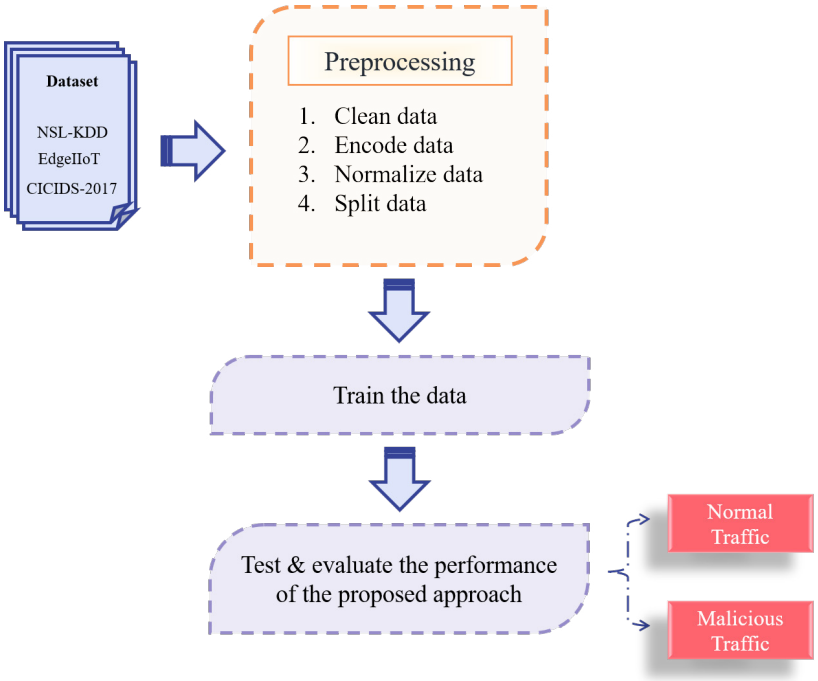

Figure 3: Road map of the proposed methodology for intrusion detection system.

a. Datasets Description

In this paper, all the datasets require several preprocessing steps to provide comprehensive and high-quality data to be used in training and testing deep learning models; including data cleaning, noise reduction, encoding categorical feature, and normalization. The following subsections contains a brief description of datasets used in this work.

i. NSL-KDD Dataset

The NSL-KDD Dataset is a trustworthy benchmark for assessing intrusion detection systems and cybersecurity tasks. Tavallaee et al. created it in 2009 as an udates to the KDD-CUP99 dataset, addressing problems like duplicated packets. It contains *147907* rows data and *41* features, which were a simulated data. The traffics are divided into five groups by the NSL-KDD dataset to reflect various kinds of network invasions named Denial of service attack (DoS), Probe attack, User to Root attack (U2R), Remote to Local attack (R2L), and Normal traffic [23]. This dataset was chosen because it is used to evaluate and compare intrusion detection methods.

ii. Edge-IIoTset Dataset

In the field of cybersecurity of IoT network, the Edge-IIoTset dataset becomes a key resource, giving us perfectly organized and varied information on real-word cyber threats. This dataset enables researchers to build advanced intrusion detection systems. It comprises *2 219 201* rows and *63* attributes, acquired from various IoT devices (more than 10 types) [24]. This dataset uses 14 classes to describe the range of possible attacks on computer networks.

iii. CIC-IDS-2017 Dataset

The CIC-IDS-2017 dataset emerges as a cornerstone in modern cybersecurity research, offering a meticulously curated and diverse collection of network traffic data representative of real-word cyber-threats. Comprising a wide array of benign activities and malicious behaviors. This comprehensive coverage enables researchers to develop sophisticated intrusion detection systems. It contains *2 830 743* rows and 78 attributes, which were collected over five days of network activity. This dataset categorizes attacks into 15 classes to represent different types of network intrusions, detailed in this work [25].

b. Validation Environment

The proposed approach was validated in the laboratory using a PC with the following specifications; Intel(R) Core (TM) i7-7700 CPU @ 3.60 GHz and Windows for operating system. Python 3.11 with the TensorFlow framework for deep learning techniques is used to develop the algorithm.

c. Performance Metrics

Various performance indicators, such as Accuracy (AC), Detection Rate (DR), Precision, and F-score, were utilized to evaluate the performance of our intrusion detection system. These metrics are defined below based on True Positives (TP), True Negatives (TN), False Positives (FP) and False Negatives (FN).

• **Accuracy:** It is the percentage of the number of instances correctly classified in relation to the total number of instances. Its equation is shown below:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (2)$$

• **Recall:** it is also called the Detection rate, it represents the percent of properly identified cases divided by the total number of abnormal cases.

$$Recall = \frac{TP}{TP + FN} \quad (3)$$

• **Precision:** It measures the number of correct positive predictions made by the model, relative to the total number of positive predictions it made.

$$Precision = \frac{TP}{TP + FP} \quad (4)$$

• **F-Score:** It is used to calculate derived efficiency by measuring harmonic mean precision and recall.

$$F - score = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (5)$$

6. Results and Discussion

Based on the experiments realized in this approach, the CNN model demonstrates strong generalization performance across all three imbalanced datasets. As shown in table 1, with the NSL-KDD dataset, the model showed a training accuracy of 98.431% and corresponding loss values of 0.051 and 0.055. The slight gap between training and testing results suggests that the model successfully generalized what was learned without overfitting. For the Edge-IIoTset, perfect accuracy was reached by the CNN model on all the data, with minimal loss on both training and testing, 5.306e-12 and 4.298e-12 respectively. Even though these results are impressive, they could also indicate that the dataset is straightforward and the model can easily understand its patterns. On the CIC-IDS-2017 dataset, the model maintained high performance with a training accuracy of 98.642% and a test accuracy of 98.686%, and minimal loss values of 0.031 and 0.032, respectively.

Dataset	Train_Acc	Test_Acc	Train_Loss	Test_Loss
NSL-KDD	98.431 %	98.363 %	0.051	0.055
Edge-IIoTset	100 %	100 %	5.306 e-12	4.298 e-12
CICIDS-2017	98.642 %	98.686 %	0.031	0.032

Table 1: Performance Analysis of CNN Model

Although these outcomes confirm the model's strong ability to detect intrusions on imbalanced data. because the main task is to spot any type of attack, these performance metrics prove that the model does its job successfully.

To comprehensively evaluate the generalization ability of the two CNN-based models, their performance was assessed on three widely used intrusion detection datasets: NSL-KDD, EdgeIIoT, and CICIDS-2017. The comparison is based on key classification metrics, including precision, recall, F1-score, and overall accuracy, as shown in tables 2 and 3. Across all datasets, CNN-SVM consistently outperformed the baseline CNN with softmax classifier. On the NSL-KDD dataset, CNN-SVM achieved higher accuracy and better balance between precision and recall, resulting in an improved F1-score. For EdgeIIoT, both models performed well; however, CNN-SVM showed greater robustness by achieving higher recall. On the more complex CICIDS-2017 dataset, CNN-SVM demonstrated a clear advantage with significantly higher F1-score and accuracy, particularly in detecting attack samples. These improvements were attributed to the SVM classifier applied in the last layer of CNN instead of softmax classifier. Overall, the consistent performance gains across all three datasets highlight the superior generalization capability of the improved model, making it more suitable for real-world intrusion detection scenarios where traffic characteristics and attack types vary widely.

Metric	**NSL-KDD**		**Edge-IIoTset**		**CICIDS-2017**	
	Normal	Attack	Normal	Attack	Normal	Attack
Precision (%)	97.05	98.92	100	100	95.27	99.40
Recall (%)	99.01	96.77	100	100	97.05	99.02
F-score (%)	98.01	97.83	100	100	96.15	99.20
Accuracy of the overall model	98.31 %		100 %		98.67 %	

Table 2: Classification Report of Binary Classification for CNN-Softmax Approach Across All Datasets

Metric	NSL-KDD		Edge-IIoTset		CICIDS-2017	
	Normal	Attack	Normal	Attack	Normal	Attack
Precision (%)	97.05	98.92	100	100	95.27	99.40
Recall (%)	99.01	96.77	100	100	97.05	99.02
F-score (%)	98.01	97.83	100	100	96.15	99.20
Accuracy of the overall model	98.31 %		100 %		98.67 %	

Table 3: Classification Report of Binary Classification for CNN-SVM Approach Across all Datasets

According to the results illustrated in Table 4, Table 5 and Table 6, the proposed approach outperforms the state-of the-art approaches in terms of accuracy across all the datasets used. This proves that our strategy is powerful and effective in managing different data and detecting intrusions more accurately that the other presented methods.

References	Year	Detection Model	Accuracy
[26]	2022	CNN	78.8 %
		CNN (Smote)	79.3 %
[27]	2023	CNN-CapSA	77.205 %
[28]	2023	CNN-Transformer	91.54 %
[29]	2023	GMM-WGAN-IDS	86.59 %
[30]	2024	CNN-LSTM	86.24
[31]	2025	CNN	97%
Proposed Model		**CNN-SVM-IDS**	**98.532 %**

Table 4: Accuracy Comparison of Models on the NSL-KDD Dataset

References	Year	Detection Model	Accuracy
[28]	2023	CNN-Transformer	91.06 %
[32]	2024	FFL-IDS	95.8 %
[33]	2025	FA-CNN	92 %
[34]	2025	CNN	98 %
[35]	2024	CNN	91.10 %
[36]	2024	CNN	98 %
Proposed Model		**CNN-SVM-IDS**	**98.97 %**

Table 5: Accuracy Comparison of Models on the CIC-IDS-2017 Dataset

References	Year	Detection Model	Accuracy
[32]	2024	FFL-IDS	97 %
[37]	2024	CNN	99.98 %
[38]	2024	CNN-GA	100 %
Proposed Model		**CNN-SVM-IDS**	**100 %**

Table 6: Accuracy Comparison of Models on the Edge-IIoTset Dataset

7. Conclusion

This article proposes a Network Intrusion Detection System (NIDS) based on deep learning learning model named Convolution Neural Network (CNN) combined by a Support Vector Machine (SVM). The use of SVM in the decision layer of CNN model instead of Softmax is a theoretically sound and empirically justified choice, particularly for binary classification tasks like our system. Our model has been evaluated on three different datasets NSL-KDD, CIC-IDS-2017, and Edge-IIoTset and demonstrate its performance in identifying and distinguishing between a normal traffic and attack traffic. The CNN-SVM-based IDS model achieves 98.532 %, 98.97 %, and 100 % accuracy on NSL-KDD, CIC-IDS-2017, and Edge-IIoTset datasets, respectively.

References

1. Alahe, M. A., Wei, L., Chang, Y., Gummi, S. R., Kemeshi, J., Yang, X., & Sher, M. (2024). Cyber security in smart agriculture: Threat types, current status, and future trends. *Computers and Electronics in Agriculture, 226*, 109401.
2. Khan, K., Mehmood, A., Khan, S., Khan, M. A., Iqbal, Z., & Mashwani, W. K. (2020). A survey on intrusion detection and prevention in wireless ad-hoc networks. *Journal of Systems Architecture, 105*, 101701.
3. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity, 2*(1), 1-22.
4. Shukla, P. (2017). ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things. In *2017 intelligent systems conference (IntelliSys)* (pp. 234-240). IEEE.
5. Nwamuo, O., de Faria Quinan, P. M., Traore, I., Woungang, I., & Aldribi, A. (2019). Arguments against using the 1998 DARPA dataset for cloud IDS design and evaluation and some alternative. In *International Conference on Machine Learning for Networking* (pp. 315-332). Cham: Springer International Publishing.
6. Henda, N. B., Msolli, A., Hagui, I., Helali, A., Maaref, H., & Mghaieth, R. (2023). A novel SVM based CFS for intrusion detection in IoT network. In *2023 IEEE International Conference on Advanced Systems and Emergent Technologies (IC_ASET)* (pp. 1-5). IEEE.
7. Upadhyay, D., Manero, J., Zaman, M., & Sampalli, S. (2021). Gradient boosting feature selection with machine learning classifiers for intrusion detection on power grids. *IEEE Transactions on Network and Service Management, 18*(1), 1104-1116.
8. Al-Janabi, M., & Ismail, M. A. (2021). Improved intrusion detection algorithm based on TLBO and GA algorithms. *Int. Arab J. Inf. Technol., 18*(2), 170-179.
9. Reyes, A., D. Vaca, F., Castro Aguayo, G. A., Niyaz, Q., & Devabhaktuni, V. (2020). A machine learning based two-stage Wi-Fi network intrusion detection system. *Electronics, 9*(10), 1689.
10. Naseri, T. S., & Gharehchopogh, F. S. (2022). A feature selection based on the farmland fertility algorithm for improved intrusion detection systems. *Journal of Network and Systems Management, 30*(3), 40.
11. Nguyen, P. T., Huynh, V. D. B., Vo, K. D., Phan, P. T., & Le, D. N. (2021). Deep Learning based Optimal Multimodal Fusion Framework for Intrusion Detection Systems for Healthcare Data. *Computers, Materials & Continua, 66*(3).
12. Zhiqiang, L., Mohiuddin, G., Jiangbin, Z., Asim, M., & Sifei, W. (2022). Intrusion detection in wireless sensor network using enhanced empirical based component analysis. *Future Generation Computer Systems, 135*, 181-193.
13. Mayuranathan, M., Saravanan, S. K., Muthusenthil, B., & Samydurai, A. (2022). An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique. *Advances in Engineering Software, 173*, 103236.
14. Thakkar, A., & Lohiya, R. (2023). Fusion of statistical importance for feature selection in deep neural network-based intrusion detection system. *Information Fusion, 90*, 353-363.
15. Kanna, P. R., & Santhi, P. (2022). Hybrid intrusion detection using mapreduce based black widow optimized convolutional long short-term memory neural networks. *Expert Systems with Applications, 194*, 116545.
16. Kareem, S. S., Mostafa, R. R., Hashim, F. A., & El-Bakry, H. M. (2022). An effective feature selection model using hybrid

metaheuristic algorithms for iot intrusion detection. *Sensors, 22*(4), 1396.
17. Fatani, A., Dahou, A., Abd Elaziz, M., Mohammed A. A. Al-qaness, Songfeng, Lu., Ali Alfadhli, S., and Alresheedi, S. S. (2023). Enhancing intrusion detection systems for iot and cloud environments using a growth optimizer algorithm and conventional neural networks. *Sensors, 23*(9):4430.
18. Ferrag, M. A., Maglaras, L., Moschoyiannis, S and Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50:102419.
19. Gamage, S and Samarabandu, J. (2020). Deep learning methods in network intrusion detection: A survey and an objective comparison. *Journal of Network and Computer Applications*, 169:102767.
20. Ge, M., Firdous Syed, N., Fu, X., Baig, Z and Robles-Kelly, A. (2021). Towards a deep learning-driven intrusion detection approach for internet of things. *Computer Networks*, 186:107784.
21. Potluri, S., Ahmed, S and Diedrich, C. (2018). Convolutional neural networks for multi-class intrusion detection system. In *International Conference on Mining Intelligence and Knowledge Exploration*, pages 225–238. Springer.
22. Kaissar, A., Nassif, A. B and Injadat. M. N. (2022). A survey on network intrusion detection using convolutional neural network. In *ITM Web of Conferences*, volume 43, page 01003. EDP Sciences.
23. Tavallaee, M., Bagheri, E., Lu, W and Ghorbani, A. A. (2009). A detailed analysis of the kdd cup 99 data set. In *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, pages 1–6.
24. Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., and Janicke, H. (2022). Edge-iiotset: A new comprehensive realistic cyber security dataset of iot and iiot applications for centralized and federated learning. *IEEe Access*, 10:40281–40306.
25. Sharafaldin, I., Lashkari, A. H., Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp*, 1:108–116.
26. Meliboev, A., Alikhanov, J., and Kim, W. (2022). Performance evaluation of deep learning-based network intrusion detection system across multiple balanced and imbalanced datasets. *Electronics, 11*(4):515.
27. Elaziz, M. A., Al-qaness, M. A. A., Dahou, A., Ibrahim, R. A., and Abd El-Latif, A. A. (2023). Intrusion detection approach for cloud and iot environments using deep learning and capuchin search algorithm. *Advances in Engineering Software,* 176:103402.
28. Yao, R., Wang, N., Chen, P., Ma, D and Sheng, X. (2023). A cnntransformer hybrid approach for an intrusion detection system in advanced metering infrastructure. *Multimedia Tools and Applications, 82*(13):19463–19486.
29. Cui, J., Zong, L., Xie, J and Tang, M. (2023). A novel multimodule integrated intrusion detection system for high-dimensional imbalanced data. *Applied Intelligence, 53*(1):272–288.
30. Genuario, F., Santoro, G., Giliberti, M., Bello, S., Zazzera, E and Impedovo, D. (2024). Machine learning-based methodologies for cyber-attacks and network traffic monitoring: A review and insights. *Information, 15*(11):741.
31. Sheikh, Z. A., Verma, N., Singh, Y., Tanwar, S and Alabdulatif, A. (2025). Generalizability assessment of learning-based intrusion detection systems for iot security: Perspectives of data diversity. *Security and Privacy, 8*(2): e70014.
32. Rehman, T., Tariq, N., Khan, F. A., and Rehman, S. U. (2024). Ffl-ids: a fog-enabled federated learning-based intrusion detection system to counter jamming and spoofing attacks for the industrial internet of things. *Sensors, 25*(1):10.
33. Attack, W. (2025). Infiltration Attack, Brute Force Attack, et al. Ensemble of feature augmented convolutional neural network and deep autoencoder for efficient detection of network attacks. *Scientific Reports*, 15:4267.
34. Ali, L., Thakur, K., Schmeelk, S., Debello, J and Dragos, D. (2025). Deep learning vs. machine learning for intrusion detection in computer networks: A comparative study. *Applied Sciences, 15*(4):1903.
35. Alzahrani, A. (2024). Novel approach for intrusion detection attacks on small drones using convlstm model. *IEEE Access*.
36. Gul, S., Arshad, S., Muhammad Umar Saeed, S., Akram, A and Azam, M. A., Wgan-dl-ids. (2024). An efficient framework for intrusion detection system using wgan, random forest, and deep learning approaches. *Computers, 14*(1):4.
37. Javeed, D., Saeed, M. S., Adil, M., Kumar, P and Jolfaei, A. (2024). A federated learning-based zero trust intrusion detection system for internet of things. *Ad Hoc Networks,* 162:103540.
38. Saadouni, R., Khacha, A., Gherbi, C., Harbi, Y., Aliouat, Z., and Harous, S. (2024). Fine-tuning cnn for enhanced security in wsn-based forest fire detection. In *2024 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, pages 1–7. IEEE.