RESEARCH PAPER

CNN-Based Intelligent Intrusion Detection for Secure Routing in IoT-Enabled Wireless Sensor Networks

Dipal Khandelwal[1], Dr. Vaishali Gupta[2], Mr. Ved Kumar Gupta[3]

[1] Research Scholar, Department of Computer Science & Engineering, IPS Academy Institute of Engineering & Science

[2] Associate Professor, Department of Computer Science & Engineering, IPS Academy Institute of Engineering & Science

[3] Assistant Professor, Department of Computer Science & Engineering, IPS Academy Institute of Engineering & Science

Received: 2nd Mar, 2026 | **Revised:** 14th Mar, 2026 | **Accepted:** 4th Apr, 2026 | **Available Online:** 20th Apr, 2026

ABSTRACT

New concerns about network security and communication quality have arisen as a result of the rapid expansion of the Internet of Things (IoT), which has greatly aided the notion of Wireless Sensor Networks (WSN) in many areas of life. Due to their resource constraints and the use of multi-hop routing, IoT-enabled WSNs are particularly vulnerable to routing-based attacks such as sinkhole, probe, and denial-of-service (DoS). These attacks can have a devastating effect on the network's performance and integrity and greatly jeopardize data integrity. Current intrusion detection systems (IDS) can be characterized as limited to complex and changing attack patterns because they are usually based on manual feature engineering, coupled with routing-blind analysis.

In order to address these issues, this study will propose a Convolutional Neural Network (CNN)–based IDS that uses deep learning (DL) to implement safe routing in WSNs that incorporate IoT technologies. We can examine the network activity comprehensively using the recommended model, which combines features of the network level and routing specificities. These features include hop count, node energy, rate of packets, delay, and rate of packet drop. An actual dataset is created and pre-processed based on feature scaling and label encoding methods to achieve the best model performance.

The suggested model achieves high values of recall, F1-score, precision, and classification rate (about 97.5%), according to the experimental evaluation data. Results from the confusion matrix, ROC curves, and precision recall metrics show that the model performs well and can be generalized, lending credence to the model's performance analysis in multi-class intrusion detection. Combining routing-aware algorithms with DL can boost detection accuracy, according to the findings. The results suggest that the suggested solution represents an efficient, scalable, and reliable IDS to the IoT-enabled WSNs, which are relevant to enhanced secure routing and resilience in the networks. This research highlights the possibilities of the smart data-driven models in meeting the future cybersecurity issues in the current IoT infrastructures.

Keywords: Internet of Things (IoT), Wireless Sensor Networks (WSN), Convolutional Neural Network (CNN), Intrusion Detection System (IDS), Secure Routing, Deep Learning, Network Security, Routing Attacks, Sinkhole Attack, Anomaly Detection.

How to cite this article: Khandelwal D, Gupta V, Gupta VK. CNN-Based Intelligent Intrusion Detection for Secure Routing in IoT-Enabled Wireless Sensor Networks. Int J Drug Deliv Technol. 2026;16(32s):641-655. DOI: 10.25258/ijddt.16.32s.73

Source of support: Nil.

Conflict of interest: The authors declare no conflict of interest.

1. Introduction

The fast expansion of the IoThas greatly changed the modern communication infrastructures as it allows connection of billions of heterogeneous devices seamlessly. The paradigm shift has enabled development of smart applications in various fields which include smart cities, health systems, environmental monitoring and also automation in industries. The key applications of such applications are Wireless Sensor Networks, which are spatially distributed sensor nodes that sense, process and transmit real time data. WSNs are important in facilitating the use of data to make informed

decisions within IoT ecosystems due to their scalability, cost-effectiveness, and low power consumption (Samal &Gountia, 2020).

1.1 Background and Security Challenges

Irrespective of their strengths, the IoT-enabled WSNs are by nature susceptible to a myriad of security threats, since they have open communication media, resource scarcity, and decentralized network structure. Data traffic in these kinds of networks usually takes the form of multi-hop pathway, in which relay nodes jointly send packets to the target. Although efficient, this routing mechanism presents serious security threats because ill-intentioned nodes can abuse the routing protocols to cause havoc to the normal network activity. Sinkhole, DoS, probe, and blackhole attacks may be used to maneuver routing routes, reduce network throughput and to spoil data integrity (Mali & Govinda, 2023).

Critical IoT applications are some of the worst hit areas of these attacks since reliability and real-time communication is important. Weakened routing may result in loss of packets, latency, unauthorized access of data and low network life. With the increasing scale and complexity of IoT networks, safe routing is now essential for system dependability and efficiency in performance (Reshi &Sholla, 2022; Karie et al., 2021).

1.2 Limitations of Existing Intrusion Detection Approaches

There has been heavy reliance on existing security measures to protect network infrastructures, such as encryption software and traditional IDS. Nevertheless, they are not always effective within a dynamic IoT setting because they are based on pre-defined rules and signatures and cannot identify new and unrecognized attack patterns (Ferrag et al., 2020; Lansky et al., 2021). Moreover, most of the traditional IDS products are made to analyze general network traffic and they do not appropriately address routing specific characteristics which are vital to detect routing-based attacks in WSNs.

With the advent of adaptive learning, ML has greatly improved detection capabilities. Nevertheless, these methods frequently depend on human feature engineering; as a result, they necessitate subject expertise and may fail to detect the intricate, non-linear correlations present in network data. Moreover, many of the current models are limited to binary classification and thus they cannot be used to differentiate between various forms of attacks in the real-world setting. The next significant weakness is that this is based on the use of generic or outdated data that fails to capture the dynamics of the behavior of the IoT-enabled WSNs, especially in the dynamics of the routing and behavior at the level of nodes (Xin et al., 2018).

These problems highlight the need for more advanced IDS that can adapt to evolving cyber threats in the IoT, provide multi-classification, and take routing considerations into account.

1.3 Research Focus and Objectives

To overcome the above challenges, this paper presents a DL-based IDS that uses CNN to do secure routing in the IoT-enabled WSNs. CNNs have proven to have exceptional talent in automatically detecting hierarchical features of complex data, and thus are quite applicable to network traffic analysis and detecting abnormal behavior (Vinayakumar and Soman, 2019; Shone et al., 2018).

The general idea of the current research is to construct a smart IDS, in which the features of routing-awareness (hop count, node energy, packet rate, latency, and packet drop rate) are incorporated into a DLarchitecture. Accurately detecting different sorts of assaults will be possible since the study can capture dynamics at both the network and routing levels.

In this context, the research problem that the study intuitively addresses are the inefficient and non-adaptive detection of intrusion when utilizing routing-centric IoT-WSN environments, and will be informed by the following objectives:

- To build an IDS based on CNN which can automatically derive features based on the network and routing information.
- In order to correctly recognise and classify different types of routing-based attacks, including probing attacks, sinkhole attacks, and DoS assaults.
- For better detection results with respect to F1-score, recall, accuracy, and precision.
- To build and use routing-aware and realistic data to do effective model testing.

1.4 Significance of the Study

This research is important as it contributes to the security mechanism improvement of IoT-based

WSNs by incorporating DLand routing-sensitive analysis. The proposed framework overcomes the drawbacks of traditional and machine learning(ML)-based IDS methods providing a better detection accuracy and a high degree of flexibility to the changes in the network statuses.

What is more, the realistic network and routing properties contribute to the increased realistic applicability of the model to real-life situations. The capability to classify the various types of attacks correctly will be very useful in the development of specific mitigation measures to ensure enhanced resilience of the entire network. This study will therefore lead to the development of smart, scalable and efficient solutions of intrusion detection in next generation IoT infrastructures.

1.5 Organization of the Paper

Here is how the remainder of the paper is going to be organized. Section 2 gives a literature analysis on the subject of IDS, DL methods, IoT security, and routing attack detection, as well as a presentation of current research gaps in this area. Section 3 shows the proposed methodology that comprises system design, dataset preparation, preprocessing, CNN architecture, and evaluation framework. Section 4 outlines the implementation in the form of the experiment, including the setting of the computation process, software, and training settings. In section 5, the performance evaluation and experimental results are presented based on several quantitative and graphical indicators. Section 6 entails the critical discussion of findings, their comparison, implications, and limitations. Section 7 is the last part that summarizes the paper and presents main recommendations to the future research study.

2. Literature Review

The fast development of the IoT has tremendously increased the application of the WSNs, casting serious issues surrounding network security and reliability. IoT-enabled WSNs are susceptible to cyber threats because they are highly dynamic in their topology, resource constrained, and decentralized. This has made development of intelligent and adaptive IDS one of the major research priorities. We discovered the present research gaps by reviewing the literature on DL-based intrusion detection, security measures for theIoT, and routing attack detection in WSNs.

2.1 Deep Learning-Based Intrusion Detection Systems

Late development in DL has made DLsystems much more efficient in their purposes as they allow automatic feature extraction and better pattern recognition. Initial experiments by Shone et al. (2018) established that DLstructures could be trained to learn hierarchical representations of network traffic, leading to enhanced anomaly detection with respect to performance. Equally, Wang et al. (2017) presented a hierarchical spatial-temporal model (HAST-IDS), which encapsulates both spatial and temporal dependencies, which improves the ability to detect far better.

Thereafter, other researchers highlighted the excellence of CNNs in intrusion detection jobs. According to Vinayakumar and Soman (2019), CNN-based models are more effective in comparison to the traditional methods in several datasets, and Ge et al. (2019) demonstrated them to be effective in managing complicated IoT traffic patterns. Still more recent studies by Deshmukh and Ravulakollu (2024) also proved the effectiveness of CNN-based structures in the high detection accuracy with less computational load.

Detailed surveys used by Ferrag et al. (2020) and Lansky et al. (2021) emphasized that DL-based IDS models have a better adaptability and accuracy over traditional methods, and the reason is that they automatically learn more complex feature representations. Moreover, hybrid and sequential models have also been investigated to improve the performance of detection. Emec and Özcanhan (2022) demonstrated superior performance in identifying time-related patterns using mixed frameworks, in contrast to Halbouni et al. (2022) who presented a CNN-LSTM hybrid capable of learning both spatial and temporal data. A deep recurrent neural network was similarly employed by Almiani et al. (2020), demonstrating its usefulness in simulating sequential dependencies of IoT traffic data.

Moreover, Abdel-Ghani et al. (2024) noted that lightweight CNN models can be useful in the deployment to resource-constrained IoT systems. Although these have been developed, the majority of the currently available DL-based IDS systems use benchmark data, and are based mainly on general traffic in a network, which

restricts their application to routing-centric IoT-WSN systems.

2.2 Intrusion Detection in IoT Environments

As the number of connected devices continues to rise and cyber-attack defenses remain inadequate, researchers have focused heavily on the issue of IoT system security. Ahmad et al. (2021) pointed out the existence of the main security challenges in the context of heterogeneity and non-standardization of IoT networks, and Reshi and Sholla (2022) stated that adaptive and intelligent security frameworks are required.

There are a number of works that suggest DL-based IDS solutions that can be adapted to an IoT environment. Banaamah and Ahmad (2022) created a scalable DLIDS that can process heterogeneous data, and Awajan (2023) proposed a better framework of the anomaly detector with better performances. Bhavsar et al. (2023) worked on detecting unknown attack patterns by use of anomaly-based detection and Qawasmeh et al. (2025) used a hybrid CNN-based model to enhance the multi-class classification accuracy.

A recent review article by Aldhaheri et al. (2024) and Liao et al. (2024) came to a similar conclusion that data-driven and DLstrategies would be needed to face new cyber threats in IoT systems. In a similar manner, Ejeofobiri et al. (2024) showed that the AI-based models of IDS were highly effective in changing adaptive threat environments. Nevertheless, the majority of these solutions mainly concentrate on the overall network behaviour and fail to explicitly include the routing properties which are fundamental in WSN-based IoT systems.

2.3 Routing Attack Detection in Wireless Sensor Networks

There is a high susceptibility of WSN to routing-based attacks because of the use of multi-hop communication. Karlof and Wagner (2003) have given some initial information about the vulnerability of routing, and they have introduced sinkhole, wormhole, and selective forwarding as some of the attacks.Later works have examined different methods of routing attack detection. Hasan et al. (2025) used ML techniques to study the impacts of sinkhole attacks, and Sujanthi and Nithya Kalyani (2020) presented a safe routing system that is QoS-sensitive and based on DL. Mali and Govinda (2023) also said that routing attacks are becoming more complex in an IoT environment, and the use of advanced detection mechanisms is essential.

Munaye et al. (2026) more recently formulated an IoT-WSN IDS ML-based system and showed better detection performance when network-level characteristics were employed. With these attempts, the classical methods like trust-based and statistical models still have some problems with scaling as well as false positive rates. Even though certain studies have included parameter routing hop count, packet loss, and node energy, routing aware feature plus sophisticated DLmodels are yet to be integrated.

2.4 Limitations and Research Gap

Even with this tremendous achievement, there are still a number of shortcomings in the current intrusion detection methods. The great problem is the use of signature-based and static detection approaches, which cannot be used against the changing cyber threats. Also, most ML models rely on hand engineering of features, which restrict their capacity to capture complicated non-linear interactions. The other major weakness is the attention to the binary classification, which limits the capability of the IDS models to differentiate among several attack types. In addition, popular benchmark datasets like UNSW-NB15 (Moustafa &Slay, 2015) and CICIDS2017 (Oyelakin, 2023) are ineffective parts of the behavior of IoT-enabled WSNs, specifically routing dynamics.

Above all, the available literature mainly concentrates on general network traffic analysis and ignores routing parameters, which are important in identifying routing and based attacks. Such disintegration of network and routing level analysis points to a major research gap. To overcome these drawbacks, an intelligent and scalable intrusion detectors framework is required, which combinesDL, and routing-knowledge feature analysis. The given work intends to fill this gap by introducing a CNN-based IDS that allows integrating network and routing aspects that will allow classifying data accurately in the multi-class format and enhancing the performance of the detection process in the setting of IoT-enabled WSN.

3. Research Methodology

Following up on the approach used to create the suggested IDS, which is a safe routing of the IoT enabledWSNs based on CNN, this part. Part of

the technique is the strategy, model architecture, preprocessing methods, dataset development, and system design. An effective model for detecting routing-based assaults in ever-changing IoT networks is the overarching objective.

3.1 System Overview

The suggested system is based on a systematic and data-driven pipeline on intrusion detection. To begin with, a real dataset that covers the network traffic and routing behavior is generated to display realistic IoT-WSN situations. Hop count, node energy, packet transmission rate, latency, and packet drop rate are some of the fundamental parameters included in the dataset and are necessary to detect an abnormal routing behavior (Munaye et al., 2026; Hasan et al., 2025).

Data quality and DL model suitability are ensured by the use of the preprocessing approach following data collection. The CNN-based model learns more complex patterns and correlations among characteristics using the processed data that follows in the training process. Lastly, the experimented model is tested based on several measures of performance to determine its efficiency in identifying normal and malicious operations.

3.2 Workflow of the Proposed System

Figure 1 depicts the overall process of the proposed IDS to help illustrate the operational pipeline. The workflow gives a description of the consecutive steps that are used, beginning with the collection of the data, up to the end classification.

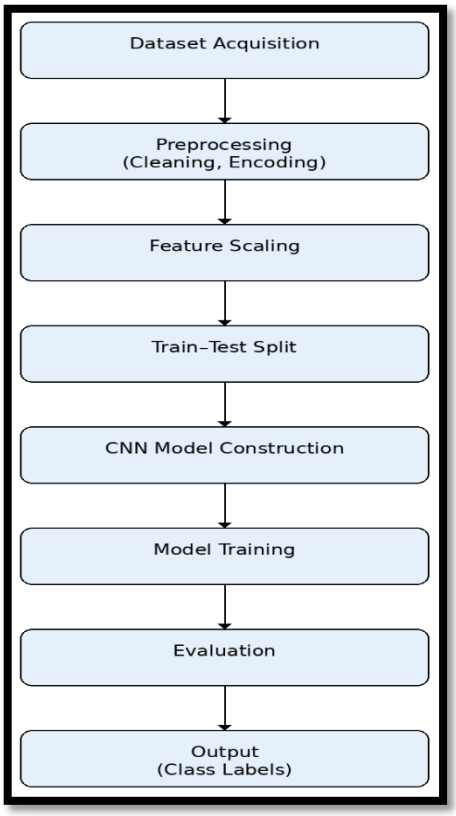

Figure 1: Proposed System Workflow for CNN-Based Intrusion Detection

Data receipt is the first step in the process, which also includes normalization and encoding as preparation. In order to identify and extract characteristics from the retrieved data, a CNN model is used. The last result will be the estimated classifications showing either normal or malicious behavior of the network. This ordered chain of processing guarantees the systematical processing and increases the credibility of the IDS.

3.3 Dataset Description

An example of a realistic dataset in IoT-WSN is created to obtain both network and routing level characteristics. The dataset is modeled in such a way that it tries to replicate real life situations by adding features that directly affect routing performances and network behaviour. The features allow the model to be effective in differentiating normal and anomalous activities. Table 1 provides a full explanation of the dataset's features.

Table 1: Dataset Features and Description

Feature	Description
hop_count	Number of hops in the routing path
energy	Remaining energy level of sensor nodes

packet_rate	Rate of packet transmission
latency	Delay in data transmission
packet_drop_rate	Packet loss indicating reliability of communication
attack_type	Target variable representing attack or normal behavior

The addition of routing-aware parameters makes certain that the dataset reflects the inherent behavior of WSN communication hence enhancing the effectiveness of intrusion detection.

3.4 Data Preprocessing

Preprocessing of data is important in improving the model performance because it provides consistency and quality of the input data. This paper utilizes a number of preprocessing methods to manipulate unprocessed data into a format that can be used to train the model.

Firstly, label encoding is applied to convert categorical labels that represent type of attack into numerical values. This transformation makes the model process classification targets effectively. Following that, feature scaling is applied to equalize the values of the input variables. This ensures that all features contribute equally to the training process and that higher-valued features are not given preferential treatment (Vinayakumar& Soman, 2019; Xin et al., 2018).

In a typical 80/20 split, the dataset is further divided into a training set and a testing set. By dividing the data in this way, the model can learn from the patterns in the training data and see if it can generalize to new data. All these preprocessing steps fall under the umbrella of better converting towards the model, stability and accuracy of prediction.

3.5 Proposed CNN Model Architecture

The proposed system's central component is an IDS based on CNNs. This model is designed to automatically acquire relevant features and perform multi-classification. CNN networks can especially be useful at extracting the spatial association of structured data and, therefore, are applicable to network traffic and routing patterns analysis (Shone et al., 2018; Ferrag et al., 2020).

The layered structure of the CNN framework, as shown in Figure 2, reflects the architecture of the suggested model.

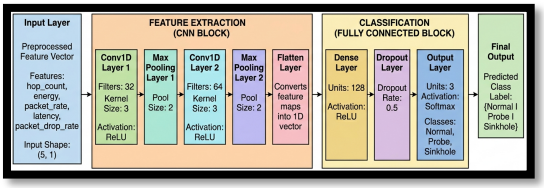

Figure 2: Architecture of the Proposed CNN Model

Feature extraction and categorization are two of the many functions performed by the architecture's many layers. To process filters that recognize local pictures and connections between input elements, the convolutional layer (Conv1D) is utilized. Then, to improve computing efficiency, a max-pooling layer minimizes dimensions while retaining significant information.

The output is flattened into a one-dimensional vector by the convolutional layers, and then it is sent to the densely linked layers for high-level reasoning and classification. A dropout layer is introduced so that overfitting does not occur, and randomly disables neurons in training. Lastly, the output layer employs softmax activation to categorize the inputs into various classes such as normal, probe and sinkhole attacks.

It is this hierarchical structure that allows the model to learn complicated feature representations and perform highly in classification.

3.6 Model Training and Evaluation Strategy

During training, the preprocessed dataset is fed into the CNN model, which then optimizes its features through iterations and obtains feature representations. The model can distinguish between various types of network behavior because it is trained on labelled data.

The model parameters are also updated in the process of training based on backpropagation and optimization to reduce classification error. Performance monitoring and overfitting is prevented with validation data. In order to ensure consistent convergence, training is typically executed in successive epochs with an appropriate batch size.

A number of performance metrics, including recall, accuracy, precision, and F1-score, are employed to evaluate the suggested model's efficacy. In addition, graphical evaluation tools like the confusion matrix, ROC curve, and

precision-recall curve are used to provide a comprehensive assessment of the model.

The multi-metric method of evaluation is used to make sure that a model is not only accurate, but also robust and reliable to work with uneven datasets and various attack scenarios.

4. Experimental Implementation and System Configuration

The present section explains the practical application of the proposed IDS involving the use of CNN in secure routing in the IoT-enabled WSNs. The implementation is aimed at bringing the conceptual model to life into a functioning system with the help of relevant computational tools, software development, and optimized training programs. It includes the development environment, software libraries, model configuration and training processes embraced which have been used to ensure efficient and reliable intrusion detection.

4.1 Computational Environment and Framework Setup

Python was chosen as the programming language to implement the proposed model due to its extensive capabilities in ML and DL. The main DL platform that will be used in the paper is TensorFlow with the Keras API, a high-level neural network architecture framework to develop, train, and evaluate neural networks with ease (Banaamah and Ahmad, 2022; Awajan, 2023).

The experiments were carried out in interactive development platform like Jupyter Notebook and Google Colab. These platforms offer a level of greater computational support, real-time execution, and visualization, whereby data preprocessing, model training and performance evaluation can be executed using the same workflow. This arrangement is reproducible and highly efficient in the computations during the entire experiment.

4.2 Software Libraries and Functional Components

To make various implementation steps easier, Python libraries were used that were well established. These libraries aid numerical calculations, data manipulations, intricate illustration, pre-processing and model creation.

Table 2 presents a summary of the main libraries to be used and their purposes in the system before moving to the detail of the implementation.

Table 2: Software Libraries and Their Functional Roles

Library	Purpose
NumPy	Numerical computations and multi-dimensional array operations
Pandas	Data loading, preprocessing, and manipulation
Matplotlib	Visualization of training and evaluation results
Seaborn	Advanced statistical data visualization
Scikit-learn	Data preprocessing and evaluation metrics
TensorFlow/Keras	Design, training, and evaluation of the CNN model

The combination of these libraries facilitates the proper management of data, the transformation of features, the creation of a model, and the visualization of the results of the experiment. These tools are integrated to make the implementation process to be modular, scalable and computationally efficient.

4.3 Model Training Configuration

In order to optimize learning and generalization, a variety of training factors impact the suggested CNN model's performance. A balanced setup was used to test the model in a way that allows it to avoid overfitting and underfitting.

The training was carried out in several epochs to enable the model to be trained to learn patterns in the dataset iteratively. The size of a batch was moderate to stabilize the gradient updates and speedy usage of computational resources. Thanks to its ability to automatically adjust the learning rate of each parameter, the Adaptive Moment Estimation (Adam) optimizer has been employed to get quicker convergence and improved performance (Lansky et al., 2021; Halbouni et al., 2022).

We used the categorical cross-entropy loss function, which is suitable for classifications based on more than two classes, to measure the discrepancy between the actual and predicted class labels. In addition, the Rectified Linear Unit (ReLU) function provides a non-linear activation in hidden layers, and the Softmax

function generates probability distributions for various classes in the output layer.

4.4 Training Procedure and Learning Process

The training process entails inputting the preprocessed dataset into the CNN model whereby it acquires the feature representations by the convolutional and pooling operations. In every training step, the model will run forward propagation and backpropagation to make predictions and change the weights respectively according to the loss achieved.

In order to have a good model performance, a validation dataset was employed throughout the training to track the learning process and to avoid overfitting. By examining the training behavior through the performance curves (accuracy and loss graph), we can see that the model converges as the number of epochs increases.

The progressive rise in the accuracy and the consecutive decline in the values of losses confirm that the model is relevant in capturing the underlying patterns of the dataset. The suggested model's generalizability is further demonstrated by the close relationship between training and validation performance.

4.5 Implementation Outcome and System Performance

An efficient and effective model that can correctly categorize network behavior was produced by an IDS that used CNNs. With a classification rate of approximately 97.5%, the system proved to be successful in detecting routing-based attacks in WSN scenarios allowed by the IoT.

Some elements that have led to the high performance can be considered to include the routing-aware features, well-used preprocessing techniques and the ability of CNN models to automatically derive meaningful feature representations. Optimal training parameter combinations also increase the model's stability and robustness.

On the whole, the implementation confirms the high level of practicality of the suggested approach and proves its adaptability to implementation in real-life IoT conditions. The system is a scalable and intelligent system to detect intrusion, which is relevant to the enhancement of network security and credible communication in the Wireless Sensor Networks.

5. Experimental Results and Performance Analysis

This section provides an in-depth evaluation of the proposed IDS, which is based on the CNN for secure routing in WSNs that are based on the IoT. To evaluate the model performance, several evaluation metrics and graphical representations are used to analyze the performance of the model to determine its effectiveness on routing-based attacks. The findings are also addressed in depth to point out the strengths, weaknesses, and implications of the suggested approach in practice.

5.1 Model Accuracy Analysis

Figure 3 displays the evolution of training and validation accuracy with increasing epochs, which may be used to evaluate the proposed model's learning performance.

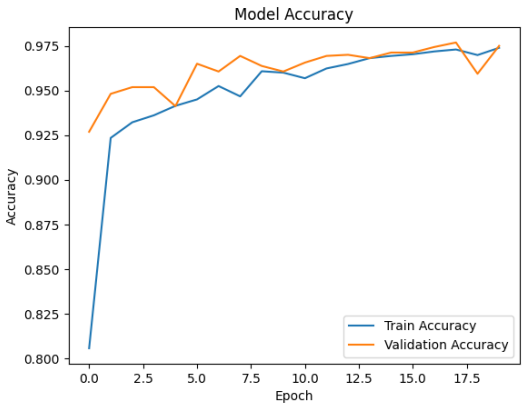

Figure 3: Model Accuracy over Training Epochs

The accuracy curve clearly demonstrates that as the number of epochs rises, both the average training and validation accuracy rise progressively. The training accuracy increases to about 80% in the first epoch and up to almost 97.5%, which means that the feature representations are learned successfully. In the same way, validation accuracy closely replicates the training trend and it tends to stabilize at 97 – 98% indicating the existence of high generalization ability.

With such a small delta between training and validation accuracy, it's safe to say that the model isn't overfitting and can instead pick up generalizable patterns from its training data. Small oscillations in late epochs are also common in DLmodels and represent fine-tuning of weights, as opposed to unsteadiness.

5.2 Model Loss Analysis

Figure 4 provides loss curves, which are further used to examine the convergence behavior of the model.

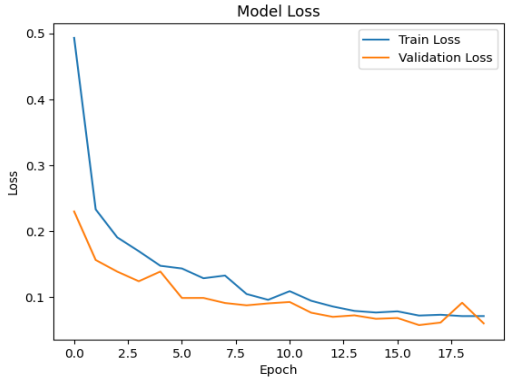

Figure 4: Model Loss over Training Epochs

The values of the loss indicate a substantial reduction throughout the first training stage wherein the training loss declines between around 0.49 and less than 0.08 and the validation loss declines between approximately 0.23 to almost 0.06. This decreasing tendency proves that the model can reduce the classification error to minimum in the course of training.

Stable learning behavior and proper optimization of the model parameters are indicated by the intersection of the two curves. Another evidence that the model performs well when applied to new situations is that the training and validation losses do not differ. As the validation loss grows marginally larger in subsequent epochs, we can see that it is highly sensitive to data variance without substantially impacting performance as a whole.

5.3 Confusion Matrix Analysis

Figure 5 displays the confusion table for the purpose of studying the prediction's performance with classes.

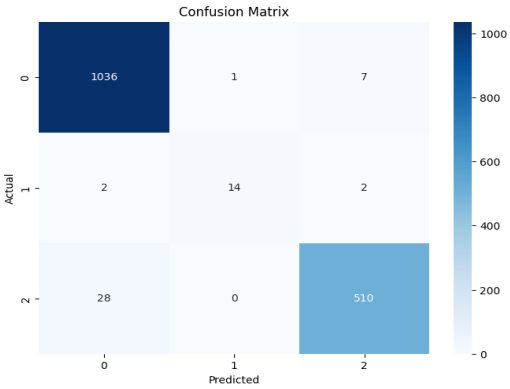

Figure 5: Confusion Matrix of the Proposed Model

The confusion matrix proves this point; the high values along the diagonal indicate that the majority of cases were correctly identified. Specifically, the model correctly classifies:

- 1036 instances of Normal class
- 14 instances of Probe class
- 510 instances of Sinkhole class.

There is minimum misclassifications. An example of this is that on a few Sinkhole instances, the incorrect classification rate is low and on a few Probe instances, the misclassification rate is low. The misclassification in the Probe class is relatively higher which can be explained by the fact that it has a much smaller sample size as was witnessed in the dataset distribution. Altogether, the confusion matrix confirms the model has a high level of recognition of all the classes, and the results are especially good in the categories of Normal and Sinkhole.

5.4 ROC Curve Analysis

Figure 6 shows theROC curves that are used to measure the model's discriminative ability.

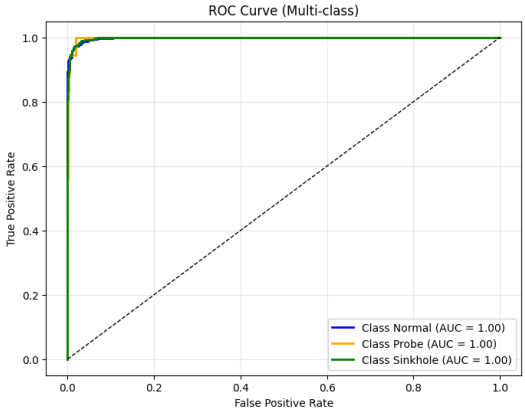

Figure 6: ROC Curve for Multi-Class Classification

The high true positive and false positive rates are indicated by the fact that the ROC curves for all classes are extremely near to the top left corner of the graph. Nearly flawless classification skill is indicated by the Area Under the Curve (AUC) of all classes, which is approximately 1.00.

This outcome will prove that the suggested CNN model is effective in differentiating various kinds of network behavior, such as Normal, Probe and Sinkhole attacks. A high AUC indicates that the model is good at handling multi-class classification problems.

5.5 Precision–Recall Curve Analysis

The precision-recall curves are shown in Figure 7 for a better evaluation of the model's performance, particularly in cases where the classes are imbalanced.

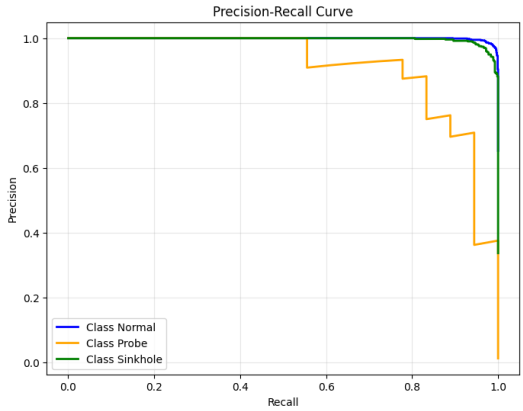

Figure 7: Precision–Recall Curve

The curves give high precision and recall rates of most of the classes, especially the Normal and Sinkhole, where both values are close to 1.0. This exhibits how the model can be able to correctly recognize true positives and also reduce false positives.

The Probe class has however a relatively low precision and recall values, especially those that are higher in the recall levels. Reason being, the small sample size of this class hinders the model's capacity to learn to differentiate between different patterns. The overall performance has been high, demonstrating robustness even in imbalanced settings, despite this disadvantage.

5.6 Class Distribution Analysis

The distribution of classes can be described by Figure 8 to have a better idea about the dataset characteristics.

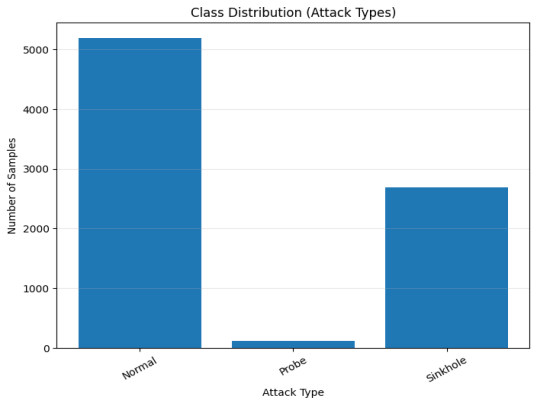

Figure 8: Class Distribution of Dataset

The figure explicitly indicates that the dataset is disproportionate with the largest sample size of the Normal class, which is then succeeded by Sinkhole before Probe which has a substantially smaller number of samples.

Such imbalancing has a direct effect on the work of the model, especially with minority classes. This uneven distribution can explain why the recall of the Probe class was lower than that of the other two analyses. The reason behind this imbalance is important in understanding the results of evaluation and in future its techniques like data augmentation or resampling are essential.

5.7 Performance Metrics Evaluation

In order to measure the effectiveness of the proposed model in a quantitative manner, the most important classification metrics are summarized in Table 3.

Table 3: Performance Metrics of the Proposed Model

Metric	Value
Accuracy	97.5%
Precision	~97%
Recall	~96%
F1 Score	~96%

The findings present an idea that the model has a significant degree of classification accuracy, and it can appropriately classify most of the scenarios. It is effective in detecting actual positive cases, as indicated by the recall value, and there are few false positives, according to the precision value. Additional evidence of the model's dependability in multi-class intrusion detection is provided by the F1-score, which takes precision and recall into account.

5.8 Summary of Experimental Findings

In IoT-enabled WSN-based environments, the experimental results show that the suggested IDS based on CNN is a very effective tool for detecting routing-based attacks. The model is very accurate and highly performing according to various evaluation measures implying that it is effective in transportation of complexities in network and routing data.

A lack of overfitting and excellent generalizability are demonstrated by the concordance between training and validation results. Both the confusion matrix and the ROC analysis show that the model can accurately and somewhat accurately categorize different kinds of attacks.

Nevertheless, the effect of the imbalance in classes especially of the Probe category is that performance in terms of recall and precision is slightly impacted. Nonetheless, the overall performance is high and the model has very good ability to cope with the real-world intrusion detection scenarios despite this weakness.

Based on the findings, it is clear that CNN and other DLmethods provide an effective and

scalable way to strengthen network security. The proposed approach will enhance the intrusion detection performance significantly and help create secure and reliable IoT-enabled Wireless Sensor Networks, because of its ability to integrate the routing-aware feature.

6. Discussion

By establishing a link between the study aims and the existing literature, this section will provide a critical examination of the experimental data presented in the previous section. This section aims to provide an explanation of how the proposed IDS based on CNNs performs in terms of its ability to address research gaps and its implications for secure routing inWSNs enabled by the IoT.

6.1 Interpretation of Model Performance

The suggested model is relatively effective in distinguishing between normal and malicious network activity, as evidenced by a high level of classification (about 97.5%), as well as high levels of recall, precision, and F1-score values. This achievement may be explained by the fact that CNN architectures have the capability of automatically obtaining hierarchical feature representations of structured data.

Because it can learn complex correlations among routing-conscious variables like as hop count, node power, latency, and packet loss rate, the suggested model does not rely heavily on feature engineering like conventional ML approaches. These characteristics are important in terms of detecting defects related to routing-based attacks, which enhances detection.

Since there is a strong relationship between the two variables, it is safe to say that the model did not overfit the data during training or validation. It becomes especially relevant in the IoT settings, where the conditions are unstable and unpredictable on one side of the network.

6.2 Impact of Routing-Aware Feature Integration

The research made a significant addition by incorporating routing-specific properties into the IDS. Other related research does not pay much attention to dynamism of routing when it is necessary in WSN environments, as it is generally considered only as the characteristics of network traffic.

The proposed model integrates network-level behavior and routing-level behavior by incorporating features like hop count, energy levels and packet loss, which can more accurately detect routing-based attacks like sinkhole and probe attacks. This is a dual level analysis that improves the contextual insight of network activity and the classification performance.

The positive outcomes of the ROC analysis and confusion matrix provide credence to the efficacy of this method. The model shows an almost perfect discrimination ability and this clearly shows that IDS should be equipped with domain specific features.

6.3 Effect of Class Imbalance on Detection Performance

Even though there was a good overall performance, the analysis shows that the imbalance among the classes can be seen to affect the ability to detect minority classes, especially the Probe category. The fact that recall and precision in this classification are relatively low can be directly attributed to the small sample representation in the dataset.

It can be noted that this finding is in line with current literature, where skewed datasets tend to result in biased model execution when applied to majority classes is a frequent problem presented in the research on IoT intrusion detection (Bhavsar et al., 2023; Ejeofobiri et al., 2024). Even though the performance of the suggested model can be considered as acceptable in such conditions, additional enhancement can be attained with the help of sophisticated methods, including oversampling, undersampling, or synthetic data generation.

IDS should be made stronger by having a balanced number of classes, which proves difficult in a real-life case where some types of attacks have lower rates, and still, they present a severe threat.

6.4 Comparative Analysis with Existing Approaches

In order to assess the workability of the suggested method, a comparative account on the existing methods of intrusion detection is provided in Table 4. The given comparison identifies the main distinctions among methodology, integration of features, and performance.

Table 4: Comparative Analysis with Existing Intrusion Detection Approaches

Study	Methodolog	Feature	Classifi	Accur	Key

	y	Type	cation Type	acy	Limitation
Shone et al. (2018)	Deep Learning (Autoencoder)	Network Traffic	Binary	~94%	Limited multi-class capability
Vinayakumar& Soman (2019)	Deep Learning (CNN)	Network Traffic	Multi-class	~95%	No routing-aware features
Halbouni et al. (2022)	CNN-LSTM Hybrid	Temporal + Network	Multi-class	~96%	High computational complexity
Banaamah & Ahmad (2022)	Deep Learning IDS	IoT Data	Binary	~93%	Limited routing focus
Munaye et al. (2026)	Machine Learning	Network Features	Multi-class	~94%	Manual feature engineering
Proposed Work	CNN-based Deep Learning	Network + Routing Features	Multi-class	**97.5 %**	Minor class imbalance

The comparison clearly shows that the suggested model outperforms the state-of-the-art approaches in terms of classification accuracy and feature integration. The routing-aware parameters unlike the past studies are explicitly included in the proposed framework and contribute greatly to better performance in detection.

Moreover, the CNN allows extracting the features automatically without overreliance on manual preprocessing and does not affect the computational efficiency unlike hybrid models (Ferrag et al., 2020; Lansky et al., 2021).

6.5 Practical Implications for IoT-WSN Security

The results of this experiment have important implication on the real world IoT-based WSN infrastructure. The suggested model is a scalable and an efficient method of attacking routing-based attacks, which is one of the most serious threats in such networks.

By easing the development of a system that can efficiently and promptly identify harmful actions, the system can aid in the formulation of secure routing protocols and improve the network's overall reliability. It is also possible to implement DLmethods and make the system adaptable to the changing attack patterns, which is why this system can be deployed in dynamic and heterogeneous IoT environments.

Also, the CNN architecture is lightweight which enables it to be implemented in resource-constrained environments as long as proper optimization methods are used.

6.6 Limitations and Future Research Directions

There are a few caveats to think about, despite the fact that the suggested model performs well. The most significant flaw is the fact that the dataset has an imbalance of classes, which affects how well minority classes are detected. Modern data balancing techniques can assist alleviate this worry by enhancing the models to a higher degree.

The other weakness is utilizing a simulated dataset that can be insufficient to reflect the complexity of the IoT reality. Future studies need to be done on the validation of the model with real-life data like TON_IoT or CICIDS to enhance generalizability.

Moreover, the existing model is more aimed at extraction of spatial features. The integration of the temporal dependencies with a hybrid model, i.e., CNN-LSTM architecture, may help increase the performance of detecting time-related attack patterns.Lastly, a continuation of the suggested system to real-time implementation and deployment via edge or fog computing systems would enable its applicability to a large-scale IoT implementation substantially.

6.7 Concluding Remarks

In general, the discussion has proved that the suggested CNN-based IDS is effective in tackling the most significant limitations noted in the current literature. The model's ability to detect routing-based attacks in WSNs of IoT-enabled networks is enhanced by combining routing-aware mathematics withDL.

The findings confirm this research hypothesis that the domain-specific feature engineering methods are highly effective in improving the intrusion detection ability when combined with other advanced DLmethods. The suggested solution can therefore be described as a significant step to secure, intelligent, and scalable infrastructures of IoT networks.

7. Conclusion and Recommendations

The high rate of expansion of the IoT-based WSN has augmented the need to have smart and dynamic security systems that guarantee the security of routing operations against emerging cyber threats. This research introduces a CNN–based intrusion detection architecture for improved safe routing in IoT–WSN networks.

Relying on human feature engineering, supporting a small number of classes, and failing to analyze routing are some of the primary problems of present systems that the suggested method fixes. The model improves the detection of routing-based attacks and effectively defines network behavior by combining features related to routing with network level features (hop count, node energy, latency, packet rate, and packet drop rate).

The reported experimental results show that the model has a great accuracy of about 97.5%, and high values of precision, recall, and the F1-score. Evaluation of performance based on confusion matrix, ROC curves, and precision-recall analysis prove that the model is robust and has generalization abilities, and there is slight overfitting.

One of the main contributions of the present research is that the routing-aware capabilities are built into a DLframework, which allows classifying attacks like sinkhole and probe on the basis of multiple classes. It still needs additional verification in the real world due to the current restrictions, such as an imbalanced data collection and data simulation.

Recommendations can be made based on the findings and are as follows:

- Real-world validation in order to enhance generalizability.
- Data balancing strategies to deal with the imbalance of classes.
- Discovery of hybrid models (e.g. CNN-LSTM) to analyse patterns through time.
- Real-time edge or fog computing implementation.

Creation of lightweight and streamlined models of the resource-constrained WSNs.

Generally, the study shows that a combination of DLand routing-aware analysis is an effective, scalable, and dependable approach to intrusion detection among IoT-enabled Wireless Sensor Networks.

References

1. Abdel-Ghani, M., Zakraoui, J., Belhi, A., Al-Ali, A., Rahme, S., & Bouras, A. (2024, December). Analysis of lightweight CNN-Based Intrusion Detection Models in IoT. In *2024 IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT)* (pp. 314-323). IEEE.
2. Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in iot-based cloud computing: A comprehensive survey. *Electronics*, *11*(1), 16.
3. Aldhaheri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (2024). Deep learning for cyber threat detection in IoT networks: A review. *Internet of Things and cyber-physical systems*, *4*, 110-128.
4. Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., &Razaque, A. (2020). Deep recurrent neural network for IoT intrusion detection system. *Simulation Modelling Practice and Theory*, *101*, 102031.
5. Awajan, A. (2023). A novel deep learning-based intrusion detection system for IOT networks. *Computers*, *12*(2), 34.
6. Banaamah, A. M., & Ahmad, I. (2022). Intrusion detection in IoT using deep learning. *Sensors*, *22*(21), 8417.
7. Bhavsar, M., Roy, K., Kelly, J., & Olusola, O. (2023). Anomaly-based intrusion detection system for IoT application. *Discover Internet of things*, *3*(1), 5.
8. Deshmukh, A., &Ravulakollu, K. (2024). An efficient CNN-based intrusion detection system for IoT: Use case towards cybersecurity. *Technologies*, *12*(10), 203.

9. Ejeofobiri, C. K., Victor-Igun, O. O., & Okoye, C. (2024). Ai-driven secure intrusion detection for internet of things (iot) networks. *Asian journal of mathematics and computer research*, *31*(4), 40-55.
10. Emec, M., &Özcanhan, M. H. (2022). A hybrid deep learning approach for intrusion detection in IoT networks. *Advances in Electrical and Computer Engineering*, *22*(1), 3-12.
11. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, *50*, 102419.
12. Ge, M., Fu, X., Syed, N., Baig, Z., Teo, G., & Robles-Kelly, A. (2019, December). Deep learning-based intrusion detection for IoT networks. In *2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC)* (pp. 256-25609). IEEE.
13. Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). CNN-LSTM: hybrid deep neural network for network intrusion detection system. *IEEE access*, *10*, 99837-99849.
14. Hasan, M. Z., Hanapi, Z. M., Zukarnain, Z. A., Huyop, F. H., & Abdullah, M. D. H. (2025). An efficient detection of Sinkhole attacks using machine learning: Impact on energy and security. *Plos one*, *20*(3), e0309532.
15. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., &Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. *IEEe Access*, *9*, 121975-121995.
16. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks*, *1*(2-3), 293-315.
17. Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., ... & Rahmani, A. M. (2021). Deep learning-based intrusion detection systems: a systematic review. *IEEE access*, *9*, 101574-101599.
18. Liao, H., Murah, M. Z., Hasan, M. K., Aman, A. H. M., Fang, J., Hu, X., & Khan, A. U. R. (2024). A survey of deep learning technologies for intrusion detection in internet of things. *IEEe Access*, *12*, 4745-4761.
19. Mali, S. D., & Govinda, K. (2023). A study on network routing attacks in IoT. *Materials Today: Proceedings*, *80*, 2997-3002.
20. Moustafa, N., & Slay, J. (2015, November). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *2015 military communications and information systems conference (MilCIS)* (pp. 1-6). Ieee.
21. Munaye, Y. Y., Gebeyehu, A. D., Tai, L. C., Abebe, Z. A., Workneh, A. B., Tarekegn, R. B., ... & Tarekegn, G. B. (2026). Machine Learning-Driven Intrusion Detection for Securing IoT-Based Wireless Sensor Networks. *Future Internet*, *18*(2), 113.
22. OYELAKIN, A. M. (2023). Overview and exploratory analyses of CICIDS2017 intrusion detection dataset. *Indonesian Journal of Data and Science*.
23. Qawasmeh, S., Habboush, A., Elzaghmouri, B., Kharma, Q., &Albalawneh, D. A. (2025). Hybrid Convolutional Neural Network-Based Intrusion Detection System for Secure IoT Networks. *Tikrit Journal of Engineering Sciences*, *32*(SP1), 1-11.
24. Reshi, I. A., &Sholla, S. (2022). Challenges for security in iot, emerging solutions, and research directions. *International Journal of Computing and Digital Systems*, *12*(1), 1231-1241.
25. Samal, N., &Gountia, D. (2020). Security and Privacy in IoT. In *Handbook of IoT and Blockchain* (pp. 151-164). CRC Press.
26. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE transactions on emerging topics in computational intelligence*, *2*(1), 41-50.
27. Sujanthi, S., & Nithya Kalyani, S. (2020). SecDL: QoS-aware secure deep learning approach for dynamic cluster-based routing in WSN assisted IoT. *Wireless Personal Communications*, *114*(3), 2135-2169.
28. Vinayakumar, R., & Soman, K. P. (2019). A comparative analysis of deep learning approaches for network intrusion detection systems (N-IDSs): deep learning for N-IDSs. *International Journal of Digital Crime and Forensics (IJDCF)*, *11*(3), 65-89.
29. Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., Huang, Y., & Zhu, M. (2017). HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. *IEEE access*, *6*, 1792-1806.
30. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... & Wang, C. (2018). Machine learning and

deep learning methods for cybersecurity. *Ieee access*, *6*, 35365-35381.