

Comparative Analysis of Machine Learning and Deep Learning Models for Attack Detection in IoT and Conventional Networks

P R Sreya¹ and Dr. Maya Mohan²

^{1,2}Computer Science and Engineering, NSS College of Engineering Palakkad, Kerala, India
Email: prsreya2000@gmail.com, mayamohan@nssce.ac.in

Abstract— The rapid dissemination of IoT devices has brought many benefits, but has also introduced significant cyber security challenges, especially due to their weaknesses for network infiltration. This paper presents a comparative analysis of machine learning and deep learning models to detect network infiltration using IoT-23 and NSL-KDD dataset. The purpose of the study is to assess the performance of the random forest (RF) and Graph Convolutional Network (GCN) models for malicious activity identification in the IoT and traditional network environment. In particular, random forest model showed excellent accuracy, scored 91% on IoT-23 dataset and 99.91% on NSL-KDD Dataset. A good performance was also given by the GCN model, which acquired an accuracy of 71.87% and 96.6% on the respective dataset using the ability to catch complex graph-composed relationships. The results obtained displays the effectiveness of the use of traditional as well as deep learning techniques to detect infiltration, which further provides insight into the IoT ecosystem and their viability to secure the traditional network. Results provide a foundation for the construction of strong, scalable infiltration detection systems and implications for improving cyber security in diverse environments.

Index Terms— Graph Convolutional Network (GCN), Random Forest (RF), IoT-23, NSL-KDD.

I. INTRODUCTION

The Internet of Things (IoT) refers to a collection of concepts that allows various computing devices and sensors to connect through the Internet, improving numerous applications such as smart homes, healthcare, agriculture, and industrial processes. IoT has driven remarkable transformations across numerous sectors and facets of daily life by facilitating the interconnection of billions of devices and generating an unparalleled volume of data [2]. However, the rapidly increasing number of attacks on the IoT system poses severe challenges for individuals and organizations alike. Being self-configuring and open, the IoT is most susceptible to both insider attacks and outsider attacks. IoT devices are self-configuring machines, allowing them to automatically configure and join the network without much human involvement. With the help of various protocols, technologies, and automated processes, these devices allow for smooth and easy connectivity of networks, detection of services, and re-configuration of these devices without taking much user time. Despite this, attackers use them to compromise a user's safety and privacy for unauthorized access of personal information and financial loss, to name a few [4].

Machine Learning has emerged as a rapidly advancing field, offering new research opportunities in addressing current and future IoT issues, as the security challenges IoT systems face continue to heighten [6]. The rest of this paper is organized as follows: Section 2 presents a review of related works, outlining the important contributions and existing methods in the field of network intrusion detection. Section 3 briefs about the existing system and architecture. Section 4 delves into the proposed system with much detail on its architecture, components, and methodologies that have been employed. In Section 5, an evaluation and analysis of the system are done in terms of performance metrics, comparisons, and insights into effectiveness. In the end, Section 6 concludes the paper by with a summary of the findings and emphasizing the contributions.

II. RELATED WORKS

The increasing use of the Internet of Things (IoT) has brought about significant security challenges, especially in large organizations and smart cities. IoT devices, which often lack standardization and exhibit high mobility, create complex traffic patterns that make traditional detection methods less effective. A study proposed a machine learning framework that employs Support Vector Machine (SVM), Gradient Boosted Decision Trees (GBDT), and Random Forest (RF) algorithms for the early detection of malicious traffic. Among these, the RF algorithm demonstrated the highest accuracy (85.34%) on the NSL-KDD dataset, highlighting its effectiveness in detecting malicious IoT traffic [1]. The study in [2] concentrated on assessing different machine learning techniques for detecting anomalies in IoT systems. Methods like SVM, Artificial Neural Networks (ANN), Decision Tree (DT), Logistic Regression (LR), and k-Nearest Neighbors (k-NN) were utilized on established datasets. The neural network model demonstrated the best performance, highlighting its effectiveness in identifying cyber anomalies within IoT networks. Additionally, the research suggested optimizing hyperparameters and evaluating real-world datasets to improve generalizability. IoT-based Distributed Denial of Service (DDoS) attacks pose significant security challenges. In [3], a systematic review examined the application of AI techniques for detecting DDoS attacks, utilizing datasets such as BoT-IoT and CICIDS-2017. The authors noted that supervised deep learning techniques are prevalent in most of the studies reviewed, with Decision Trees being employed in 20% of them. This research highlights the role of AI in addressing DDoS attacks in a scalable and efficient way. [4] introduced an Intrusion Detection System (IDS) that integrates Decision Tree, Random Forest, k-NN, and SVM classifiers along with feature selection techniques like Correlation-based Feature Selection and Genetic Algorithm. The system was trained on the IoTID20 dataset, achieving high detection accuracy, particularly excelling with Decision Tree and Random Forest. The authors concluded that merging anomaly detection with machine learning techniques provides robust defense mechanisms for IoT networks. In [5], the detection of DDoS attacks in extensive IoT networks was enhanced by utilizing correlation-aware architectures. Among the five neural network models tested, Long Short-Term Memory (LSTM) and Transformer architectures yielded the best results, reaching an F1 score of 81% when employing correlation-aware methods. This research highlighted that integrating correlation information across IoT nodes significantly improves the detection of camouflaged attacks. In addition, [6] presented a comprehensive review of machine learning algorithms for IOT security, highlighting Importance of embedded ML techniques for detecting discrepancy. Study in [7] compared to machine learning Classifier on NSL-KDD dataset, feature shows improvement in significant accuracy during preprocessing Methods such as Principal Component Analysis (PCA) were implemented. Random Forest and K-NN Classifier demonstrated extraordinary accuracy, validated their effectiveness in detection of intrusion. The study in [8] presented an ensemble deep learning approach for analyzing IoT-23 network traffic data. By integrating Random Space (RS), Random Tree (RT), XGBoost, and Graph Convolutional Neural Network (GCNN) models, the researchers discovered that GCNN achieved superior accuracy and precision compared to the other models. This approach highlights the promise of advanced neural networks in enhancing IoT cybersecurity. The research in [10] tackles the growing security issues faced by Internet of Things (IoT) devices, especially in smart city settings, where conventional security methods often fall short. The study aims to improve IoT security by leveraging honeypot data alongside machine learning techniques. Honeypots mimic IoT devices to collect real-world cyber-attack data, which is then utilized for threat detection and mitigation. Various machine learning and neural network algorithms were employed on these datasets, with the decision tree algorithm achieving the highest accuracy, between 99.26% and 99.92%. This illustrates the effectiveness of decision trees in analyzing and classifying attack data within IoT networks. The study emphasizes the practical advantages of incorporating honey pot data into IoT security frameworks, such as enhanced system resilience and better attack detection capabilities. These findings have important real-world implications, providing valuable insights for implementing more effective and robust security measures in IoT environments.

Table1 shows a comparison of existing systems. Table1 depicts the comparison of existing systems.

TABLE I. COMPARISON OF LITERATURE SURVEY

Paper	Year	Dataset	Model	Key Finding
[1]	2021	NSL-KDD	SVM, GBDT, RF	RF performed best. Supervised ML can be used to analyze traffic data.
[2]	2024	ToN-IoT, BoT-IoT	SVM, ANN, DT, k-NN, Logistic Regression	Neural Network model best fit.
[3]	2024	N-Balot, BoT-IoT, IoTID20, MedBlot, IoT-23, ToN-IoT, Edge-IIoT	Unsupervised: k-Means, PCA; Semi-Supervised; Supervised: DNN, CNN, RNN; Unsupervised: Deep Encoders, Restricted Boltzmann Machines, Deep Belief Networks	AI is a scalable solution.
[4]	2024	IoTID20	Supervised Classifiers: DT, RF, k-NN, SVM; Feature Selection: CFS, GA	Best performance obtained training DT and RF using features selected by GA.
[5]	2024	Self-created	Architectures: MM-WC, MM-NC, OM-WC, OM-NC; Neural Network Models: CNN, LSTM, TRF, AEN	LSTM/MM-WC & TRF/OM-WC have best performance.
[6]	2024	NSL-KDD	SVM, NN, k-NN, ANN	RF performs best in studies. k-NN takes more time to categorize.
[7]	2024	NSL-KDD	RF, SVM, k-NN, DT, Logistic Regression, NaïveBayes	RF attained highest values for precision, recall, F1 score, accuracy & kappa coefficient.
[8]	2024	IoT-23	Random Tree (RT), Random Space (RS), XGBoost, Graph Convolutional Neural Network (GCNN)	GCNN - best performing method among these.
[9]	2024	UNSW_NB_1, UNSW_NB_2	Classifiers: RNN, BI-GRU, BI-LSTM; Feature Selection: Cat & Mouse Inte- grated HBO	Extant RF model produced the poorest results compared to ANN, DBN, CNN, SVM, and other RF models.
[10]	2024	Self-generated (Dataset presented as log files from 258,871 PCAP files)	NaïveBayes, k-NN, DT, Sequential Neural Network, LSTM	DT showed a near-perfect performance regardless of the iteration or feature selection method used.

III. EXISTING SYSTEM

The existing system for attack detection systems depends on traditional machine learning and deep learning models. Its intention is to reduce some challenges arising out of the number of attacks in the IoT and traditional network environment. A supervised learning algorithm, for instance, Decision Trees, Support Vector Machines (SVM), Naive Bayes, and Random Forest, has widely been used because they are very simple and also have a great efficiency in classification. For example, the models of Decision Tree had proved to be effective with high accuracy in detecting malicious activities because it could handle the complex decision boundary. Similarly, ensemble models such as Random Forest have shown to be robust in intrusion detection with a balance between precision, recall, and computational efficiency.

Deep learning approaches, such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Graph Convolutional Networks (GCN), have also been extensively explored. These models are highly effective in learning complex patterns from high-dimensional data and are, therefore, suitable for complex datasets like IoT23 and NSL-KDD. Several studies have highlighted the ability of GCNs to model graph-structured data, representing network interactions, and improving detection rates for advanced attacks. Hybrid systems that integrate honeypot generated data with machine learning models have also gained popularity, as they provide real-world insights into attacker behaviors, further enhancing the efficacy of detection systems.

Despite the tremendous advancements, existing systems pose scalability challenges, along with generalization over diverse network environments and accommodation over unique characteristics of the IoT networks, including limited computational resources and heterogeneous devices. These limitations underscore a need for further research that could lead to the creation of applicable systems capable of effectively securing both

traditional and IoT network environments with high performance and reliability. Fig. 1 shows the architecture of the existing system.

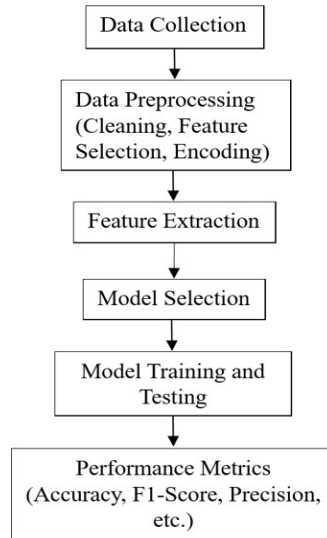


Figure 1. Existing System Architecture

III. PROPOSED METHODOLOGY

The proposed method for network intrusion detection combines classic machine learning and deep learning approaches to enhance detection accuracy. It consists of three major components: data preprocessing, machine learning based detection, and graph neural network-based detection. The system uses two benchmark datasets, IoT23 and NSL - KDD, to test two different models: RF and GCN. The following subsections provide a detailed description of each component's architecture and functionality. Fig. 2 is the architecture of the proposed system.

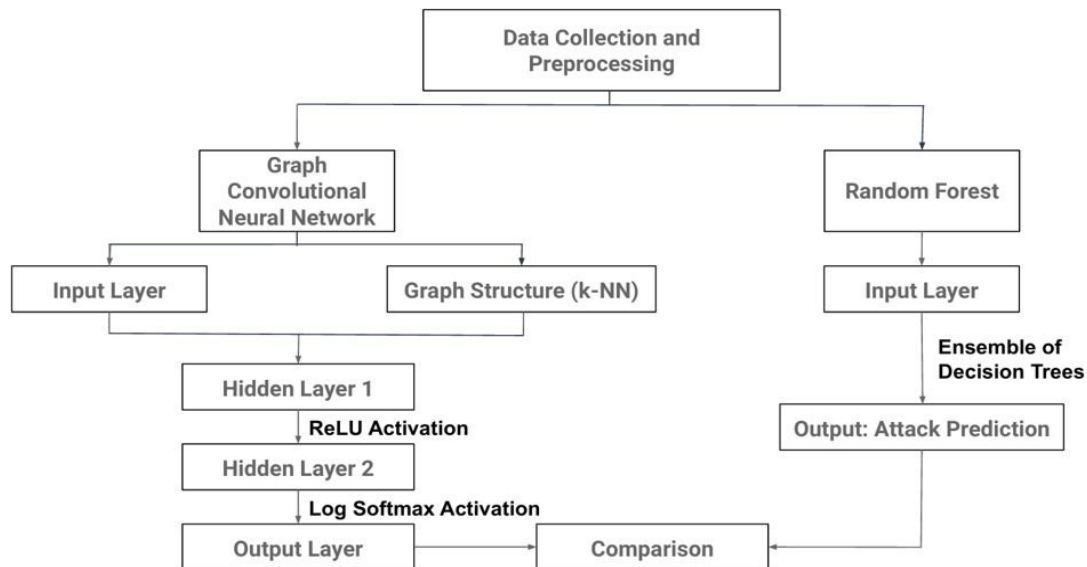


Figure 2. Proposed System Architecture

A. Data Preprocessing

Data preprocessing is an essential foundational step in the development of any machine learning or deep learning model, ensuring that the input data is clean, structured, and ready for effective training. For the IoT23 dataset, network traffic data is classified into seven distinct categories: Benign, Attack, CC, DDoS, FileDownload, Okiru, and PartOfAHorizontalPortScan. These categories encompass an extensive range of network behaviors, beginning with normal traffic (Benign) and extreme malicious activities. The NSL-KDD dataset also categorizes

network intrusions into four main classes: DoS (Denial of Service), Probe (probing attacks), R2L (Remote-to-Local attacks), and U2R (User-to-Root attacks). The datasets are prepared for modeling by converting categorical features into numerical formats. This step is crucial since most machine learning models need numerical inputs for their calculations. Additionally, all features are scaled and normalized to maintain consistency in their magnitudes, preventing any single feature from overshadowing the model's learning process. A key preprocessing step for the GCN involves constructing a graph structure from the dataset. This is done by using a k-NN algorithm to identify data samples with similar features and establish edges between them. In this graph, each data sample is depicted as a node, while the edges represent the relationships based on feature similarity. This graph representation enables the GCN to grasp both the unique features of the nodes and their structural connections, improving its capacity to identify patterns that signal network intrusions.

B. Random Forest

The Random Forest (RF) classifier is a well-established and effective machine learning method utilized for network intrusion detection. It operates by forming an ensemble of decision trees, with each tree being trained on a random selection of the data and features. The RF model then combines the predictions from all the trees using majority voting, resulting in strong and dependable classifications. This approach is effectively applied to the IoT23 and NSL-KDD datasets, as their large, structured nature makes them particularly interesting. Generally, the network intrusion data suffers from mixed type data and data distribution imbalance conditions, for which the RF is best suited with handling the unbalanced distributions better than most techniques. The performance analysis of the given RF model evaluates its classification accuracy against the metrics precision, recall, and F1-score. One of the advantages of the RF model is interpretability, since it provides information about feature importance, which allows one to determine which features contribute most significantly to the detection of intrusions. This property makes RF not only an effective classifier but also a valuable tool for understanding the underlying characteristics of the datasets.

C. Graph Convolutional Network (GCN)

The Graph Convolutional Network (GCN) is a deep learning model specifically adapted to work on graph structured data, making it an appropriate tool for the analysis of network traffic that is represented as graphs. In the case of the IoT23 dataset, a k-NN-based graph structure is established. This graph structure connects nodes across similar features and captures the individual attributes of data samples along with their relational patterns. This is a model consisting of two convolutional layers. The first layer is defined using a ReLU activation function so that the model could learn to look for more non-linear patterns among the features. The log-softmax is applied to the second layer with outputs that consist of class probabilities in final classification. The architectural setup of this model allows for GCNs that analyze both feature-based patterns within the nodes as well as complex topology in a graph. The performance of the GCN model is verified by accuracy metrics and confusion matrices, showing that it is able to identify very subtle and intricate intrusion behaviours. The GCN introduces a fresh perspective to network intrusion detection by leveraging graph structures, particularly in identifying patterns that emerge from related network events.

D. Integrated System Framework

The proposed system is a hybrid approach that uses the best characteristics of traditional machine learning and graph-based deep learning that is a structure to detect a composite network infiltration. In this system, the flexibility of random forest is combined with innovative capabilities of the graph convolutional network, exploiting their complement, so that accuracy and strength can be increased. System IoT23 and NSL-KDD demonstrate their adaptability in the diverse network environment using dataset. The RF model is efficient in handling the structured tabular data and provides rapid and reliable classification, while the GCN model discovers deep insight by analyzing graph-based relationships, exposing the complex intrusion pattern. Together, these models provide a versatile approach to detect infiltration, which address a wide range of challenges faced in modern cyber security scenarios. This integrated system ensures scalability and effectiveness, so it is good for deployment within the dynamic network environment such as IoT ecosystem and traditional network infrastructure. This will not only give more accurate detection, but will also provide valuable insight into the nature and behavior of the network infiltration, giving a route towards more flexible safety solutions.

V. RESULTS AND DISCUSSION

Evaluation of the proposed system on IOT-23 and NSL-KDDD dataset suggests that Random Forest (RF) and Graph Convolutional Network (GCN) models perform well in detecting and classifying networks. On IOT-23

dataset, the RF model scored 91% accuracy surprisingly, which proved to be the ability to deal with the deviation of IOT network traffic and dynamic nature. The model obtained 0.90 to Macro and weighted average F1-score, accurately detected of fake activity in many traffic classes. Conclusions display the ability of random forest models to evaluate convenience-rich datasets, making it ideal for detecting intrusion in complex IOT contexts, where various traffic patterns and large amounts of data are specific.

On NSL-KDD Dataset, the random forest model performed from the amenity, with a closely-perfect accuracy of 99.91%. The classification report demonstrated high precision, recall and F1-score for all traffic classes, which demonstrates model's dependence and strength in benign discrimination with malicious data. Its remarkable performance in all parameters reveals its ability as a very effective network safety tool, especially in network infrastructure installed with patterns of well-defined attack. The GCN model demonstrated its ability to detect infiltration using the graph-based representation of network data. The GCN model acquired an accuracy of 71.87% on IoT-23 dataset.

While the complexity of the dataset presented the obstacles, the model classified the successively classified attack using the underlying relationship in network traffic. The GCN model created a high testing accuracy of 96.60% on the NSL-KDD dataset, which reflects its ability to explain structured data and detect hidden patterns in traffic. This shows the ability to identify the GCN facility and its ability to succeed in contexts where the relationship is important to detect discrepancies or malicious behavior. Overall, both dataset results highlight the effectiveness of random forest and GCN models in identifying network infiltration. The random forest model exhibited especially better accuracy and accuracy on the NSL-KDD dataset, giving it a reliable and optimistic solution to detect an attack in both IOT and traditional networks. In contrast, the GCN model demonstrated its ability to take advantage of data linkage, making it a useful technique for the structured dataset found in the IoT network. These findings highlight the ability to combine several machine learning algorithms to create strong and scalable intrusion detection systems that can protect both IoT settings and traditional network infrastructure. Table 2 shows the performance of RF and GCN models on IoT-23 and NSL-KDD dataset.

TABLE II. COMPARISON OF THE PERFORMANCE OF RF AND GCN MODELS ON THE IoT-23 AND NSL-KDD DATASETS

Dataset	Random Forest Accuracy	Graph Convolutional Net- work Accuracy
IoT-23	91	71.87
NSL-KDD	99.91	96.6

VI. CONCLUSION

This study suggests how machine learning and deep learning models can be useful in solving the challenges of detecting attacks in IOT and traditional network environment. Models, RF and GCN, were evaluated on two major datasets: IOT-23 and NSL-KDD to assess their ability to detect cyber threats. The random forest model gained the best accuracy in both datasets, where it obtained 91% accuracy in IOT-23 and notable 99.91% on NSL-KDD, highlighted its strength and credibility for use in the odd network environment. Similarly, the GCN model was impressive and with its strength to modeling complex relationships in the yield graph-composed data of 71.87% on IOT-23 and 96.6%. These findings highlight the strength of a combination of deep and traditional learning plans to detect intrusion, depending on the nature of network settings. With the use of such models, extensive improvements can be made to detect infiltration and suppression of complex attacks. Studies hold a starting point for hybrid safety architecture that will protect the core IoT infrastructure and traditional systems. Future work may include inclusion of other datasets, adaptation of model parameters, and more sensitive and scalable for real-world deployment.

REFERENCES

- [1] Anwer, Maryam, S. Mahmood Khan, and M. Umer Farooq. "Attack detection in IoT using machine learning." *Engineering, Technology Applied Science Research* 11.3 (2021): 7273-7278.
- [2] Inuwa, Muhammad Muhammad, and Resul Das. "A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks." *Internet of Things* 26 (2024): 101162.
- [3] Bala, Bindu, and Sunny Behal. "AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges." *Computer science review* 52 (2024): 100631.
- [4] Altulaihan, Esra, Mohammed Amin Almaiah, and Ahmed Aljughaiman. "Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms." *Sensors* 24.2 (2024): 713.
- [5] Hekmati, Arvin, et al. "Correlation-aware neural networks for DDOS attack detection in IoT systems." *IEEE/ACM Transactions on Networking* (2024).

- [6] Farooq, Mansoor, and Mubashir Hassan Khan. "Cyber Attack Detection Using Machine Learning Techniques in IoT Networks." *International Journal of Innovative Research in Computer Science Technology* 12.2 (2024): 32-38.
- [7] Dash, Sanjit Kumar, et al. "Enhancing DDoS attack detection in IoT using PCA." *Egyptian Informatics Journal* 25 (2024): 100450.
- [8] Malathi, S., and S. Razool Begum. "Enhancing trustworthiness among iot network nodes with ensemble deep learning-based cyber attack detection." *Expert Systems with Applications* (2024): 124528.
- [9] Brindha Devi, V., Nihar M. Ranjan, and Himanshu Sharma. "IoT attack detection and mitigation with optimized deep learning techniques." *Cybernetics and Systems* 55.7 (2024): 1702-1728.
- [10] Ahmed, Yussuf, Kehinde Beyioku, and Mehdi Yousefi. "Securing smart cities through machine learning: A honeypot-driven approach to attack detection in Internet of Things ecosystems." *IET Smart Cities* (2024).