National College of Ireland

Enhancing IoT Security through Anomaly-based Intrusion Detection Systems

MSc Research Project
MSc in Data Analytics

Muhammed Musthafa Keloth Poyil
Student ID: x23162112

School of Computing
National College of Ireland

Supervisor: Furqan Rustam

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Muhammed Musthafa Keloth Poyil
Student ID:	x23162112
Programme:	MSc Data Analytics
Year:	2024-2025
Module:	Research Project
Supervisor:	Furqan Rustam
Submission Due Date:	12/12/2024
Project Title:	Enhancing IoT Security through Anomaly-based Intrusion Detection Systems
Word Count:	XXX
Page Count:	24

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Muhammed Musthafa Keloth Poyil
Date:	29th January 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhancing IoT Security through Anomaly-based Intrusion Detection Systems

Muhammed Musthafa Keloth Poyil
x23162112

Abstract

The advancement of the Internet of Things (IoT) has seen rapid growth in the industrial connectivity and automation rates considerably. However, this growth has also created important concrete cybersecurity threats as IoT networks are now in the crosshairs of highly developed cyber attacks. The first problem is that, unlike more traditional networks, the emerging IoT networks exhibit high levels of heterogeneity and low available resources; and the second is that most current IDSs have rigid architecture and are not suitable for the IoT networks. This work offers an anomaly-based IDS for improving the security of IoT networks that exploits state-of-the-art ML and DL methodologies. The proposed system includes Gradient Boosting Machine (GBM), k-Nearest Neighbour (KNN), and Naïve Bayes with Graph Neural Networks (GNNs): Graph Convolutional Networks (GCNs) and Graph Isomorphism Networks (GINs). In results of experiments, Random Forest and KNN surpass competitors with such diagrams as 96.30% and 98.19% correspondingly, while GNNs are also combined with GIN and give excellent results in resect of complex traffic pattern detection with 79.12% of accurate classification. These results prove that hybrid anomaly-based IDSs are useful to achieve a steady and efficient IoT cybersecurity model.

1 Introduction

The IoT devices have already enabled a fast and fast-growing connected environment that defines social life, connectivity, automation, and ways of functioning in multiple industries Rane et al. (2024). From smart homes to healthcare and industrial, IoT ecosystems have become common places with IoT devices making up 30% of total devices on enterprise networks today *What is IoT Security?* (n.d.). The total value of industrial Internet of Things (IIoT) through the worldwide market averaged above 544 billion U.S. dollars in 2022. The market is projected to expand over the years, with potential worth of about 3.3 trillion U.S. dollars in 2030 *Industrial IoT - market size worldwide 2020-2030* (2024).

(IoT) cyberattack incidences rose to over 112 million in the world in the year 2022. This number has risen steadily over the recent years from an approximate of 32 million detected cases in 2018. In the latest measured year, the year-over-year growth of IoT malware incidents has been recorded as 87% *Industrial IoT - market size worldwide 2020-2030* (2024). But this exponential growth has brought a number of new and unprecedented challenges in the realm of cybersecurity. Due to the continuously growing number of IoT devices that have constrained resources, and numerous operational environments, new and more advanced types of cyber threats are becoming major threats

to privacy, data integrity, and critical infrastructures Farooq et al. (2023); Inayat et al. (2022).

1.1 Motivation

Although enhancement in the so-called Conventional IDS has been made, it cannot truly function in the IoT setting because of its lack of flexibility to grow and fully optimize itself to the characteristics of IoT networks. These systems were originally developed for conventional networks and fail to properly handle the highly dynamic and distributed, heterogeneous, non-trivial, and often limited resource IoT devices Farooq et al. (2023); Alsoufi et al. (2021). As such, there is a pressing demand to design new security models that will be suitable for implementing in IoT environments Yaseen (2023).

Anomaly-based IDS has proved to be effective, and thus considered as the best choice to improve security in IoT. Since these systems are based on the recognition of certain variations in a typical flow of behaviour, they can, in theory, identify types of attack that the original behaviour model did not recognise. In addition, the introduction of ML and DL into the identification of anomalous behaviour has been seen to yield promising results in terms of the achievement of high levels of anomaly detection accuracy and minimisation of false positives Ullah and Mahmoud (2021); Alsoufi et al. (2021). These methodologies continue to present limitations in achieving an optimal solution and scalability and flexibility within IoT environments Alsoufi et al. (2024, 2021).

This paper provides a solution to the growing problem of how to establish effect and resilient intrusion detection to IoT networks. It suggests a new anomaly-based IDS with the help of approaches based on ML, the Gradient Boosting Machine, the k-Nearest Neighbor, and Naive Bayes algorithms. Moreover, it uses deep learning architectures like Graph Convolutional Networks and Graph Isomorphic Networks. The research also assesses the performance comparison of these algorithms in terms of accuracy, precision, recall, F1 score, and ROC–AUC.

1.2 Research Question and Objectives

Research Question (RQ): How effective are the variants of Graph Neural Networks, specifically Graph Convolutional Networks (GCN) and Graph Isomorphism Networks (GIN), compared to the traditional machine learning algorithms in detecting network intrusion in terms of evaluation metrics such as Accuracy, Precision, Recall, F1-score, and AUC-ROC?

Research Objectives:

1. Develop and assess a holistic anomaly-based IDS tailored to the unique characteristics of IoT environments.

2. Conduct a systematic comparison of traditional ML algorithms (e.g., Gradient Boosting Machine, k-Nearest Neighbor, and Naive Bayes) with advanced graph-based DL architectures like GCN and GIN.

3. Evaluate the performance of GCNs and GINs in detecting intricate network arrangements that traditional methods struggle to analyze.

4. Analyze and compare the effectiveness of these approaches using key evaluation metrics, providing insights into their potential for IoT security solutions.

The first major contribution of this study is the creation and assessment of a holistic anomaly-based IDS specifically for the IoT environment. From the study, the systematic comparison of the traditional machine learning with that of the graph-based deep learning algorithms to explain certain aspects of IDS is made clearer. Furthermore, the integration of GCNs and GINs is a new approach to graph analysis that distinguishes intricate network arrangements, which are difficult to track with standard approaches.

The remainder of this document is structured as follows:

- **Chapter 2: Related Work** – Summarizes the current state of IoT security publications as well as evaluates anomaly detection frameworks, machine learning methods, and graph-based intrusion detection systems. Presents a brief overview and highlights the research gap of this study, revealing the niche covered in this research.
- **Chapter 3: Methodology** – Explains the proposed IDS framework as far as data acquisition, data preprocessing, choice of algorithms, and techniques for model assessment are considered. Describes how GCNs and GINs can be incorporated to gain the ability to detect stronger and multiple threats.
- **Chapter 4: Results and Discussion** – Summarizes the results of the study and evaluates the proposed models based on the results attained during experimentation.
- **Chapter 5: Conclusion and Future Work** – Presents a brief conclusion of the research together with recommendations for future research regarding IoT security.

2 Related Work

The advancement of companies with the IoT devices is making industries fast to connect and automate industries. However, this growth has brought about new cybersecurity threats due to IoT systems that are comprised of worldwide and heterogeneous networks and are resource-constrained, along with the threats arising from advanced cyber threats. Current Intrusion Detection Systems (IDS) do not fit these dynamic requirements; therefore, special approaches suitable for IoT are necessary. These threats are partially preventable by Anomaly-based IDS, especially where it is strengthened with ML and Deep Learning DL, in that it can identify new attack patterns and has minimal false alarms. This literature review focuses on IoT cybersecurity issues and IDS development trends with ML/DL components to inform current and future research.

2.1 Challenges in IoT Cybersecurity

Bernabe and Skarmeta have also described ten major European cybersecurity and privacy threats in Bernabe and Skarmeta (2022), which include efficient security solutions apropos of diverse and distributed networks, accurate detection of new forms of cyber threats, and privacy-sensitive identity assertion. They also identify that there are ways for designing the holistic approaches to IoT/CPS systems from the security point of view, but those inherent gaps will require more advanced technologies such as SDN/NFV, efficient/lightweight cryptographic protocols, and real-time risk assessment. The study also assesses 14 Horizon 2020 funded European projects related to these challenges, including ANASTACIA and RED-ALERT that help improve the self-healing of cybersecurity and

threat intelligence. These projects reflect vast improvements in protecting IoT environments and important assets.

Marshal et al. (2021) discuss the security threats emerging in IoT-based smart healthcare networks and provide a framework for avoiding them. Due to weak security and size constraints in the construction of critical devices like the infusion pump and cardiac monitor, the study identifies vulnerabilities. Specific threats include the following: Denial of Service (DoS) attacks, outdated software, and lack of IT-OT integration. The authors say that organizations should hire cybersecurity workers, keep track of all devices, and have safe methods for updating devices to enhance security. Concerns are raised concerning stringent standards such as ISO/IEC 82304 and usage of micro-segmentation, especially to secure the sensitive health information and ensure minimal spread throughout the huge networks.

As pointed out by Choo et al. (2021), a multidisciplinary approach to current and future IoT cybersecurity and risk management is called for to effectively address the numerous and complex threats posed by the IoT. Different IoT security threats are outlined in their study where the authors recognize various threats such as device authentication, data protection, and network security, yet point out promising techniques such as blockchain and federated learning. Their most important contribution is the multi-layer taxonomy they proposed for the classification of cyberattacks leaning on the IoT environment, and their system was examined on realistic scenarios, such as the case of the German steel plant. The authors reaffirm the role of cooperation on the international level and scholarly governance while stressing that modern IoT security threats should be managed with the help of integration of modern technologies.

Chopra (2020) analyses the change of perspective in IoT security and focuses on difficulties in operational and information technology (OT & IT). It describes weak links inherent in legacy systems together with other protocols such as Modbus and Distributed Network Protocols that make IoT systems an open book to cybercriminals. Deriving the focus on the Purdue Model for Control Hierarchy, Chopra calls for barb firewalls, business DMZs, and multiple layered security measures to protect IoT contexts. This paper highlights the need to establish IT and OT security frameworks and implement the best security practices for legacy systems to improve IT/OT convergence security for IIoT applications.

Ahmad et al. (2021) give a systematic review of cybersecurity in the IoT-based cloud computing system and stress the threats in the PaaS and SaaS hybrid model. They classify cloud security concerns into four categories: content, network and services, application, and people issues. This work discusses key issues such as data leakage, malware, and improper utilization of resources, and further discusses the application of deep learning (DL) for anomaly detection and resiliency. Still, the authors reveal some limitations in terms of IoT-cloud future scalability, privacy protection, and changing security models, calling for additional research concerning the AI-driven protection of IoT-cloud structures against new threats.

2.2 Advancements in Intrusion Detection Systems

Mendhurwar and Mishra (2021) introduced an elaborate component-based architectural model for hybrid social and IoT environments with discussions on digital business change and cybersecurity. By examining how this integration occurs, it extends the work to consider the opportunities of the resulting Cyber Physical Social Systems (CPSS) in

business innovation while stressing the importance of security and privacy. The significant contributions include a clear architectural model with the focus on device, connectivity, applications, and analytical layers, with the measures of security to be implemented for all these layers highlighted. The authors also point out that such technology convergence is relatively risky and highlight the need for contingency-oriented security and improved governance for risk management in IoT environments.

A plethora of cybersecurity issues and approaches are discussed in the recent work of Raimundo and Rosário (2022), where the focus is on the Industrial Internet of Things (IIoT). Stressing factors like constraints in resources, decentralised settings, and dynamic IoT systems, they argue that conventional security measures are insufficient. Based on their own research, the study analyses 70 core articles. The authors concluded that novel technologies such as blockchain and machine learning can be considered indispensable for managing risks. While blockchain helps to strengthen data protection and identification, machine learning coordinates the identification of invasions and threats. In their work, however, the authors identify that there remain issues in scalability and integration, which suggests that more work needs to be done to improve the reliability of IIoT systems and their management of risk.

Alajlan et al. (2023) discuss IoT systems and the ability to introduce blockchain techniques to enhance cybersecurity. Some of these they group under IoT device security, others under blockchain security, and others under network security categories with specific problems, including device authentication, the existence of significant limitations in consensus mechanisms, and scalability, among others. For improving IoT data integrity and privacy, the study underlines the decentralised and unchangeable nature of the blockchain. It also revisits applications such as secure data management and smart contracts and analyzes the research opportunities in smart cities: interoperability and energy efficiency. It is for this reason that this extensive literature review emphasizes the significance of blockchain while calling for more studies in an effort to surmount enduring challenges.

In the literature review work by Lee (2020), a four-layer risk management model that is suitable for IoT systems is introduced. It proposes a cybersecurity framework that encompasses theoretical and practical elements of IoT cyber ecosystems regarding the dynamic environment, infrastructure, risk assessment, and performance evaluation. Using linear programming, the work presents a perfect method of efficiency in distributing the financial resources amidst various IoT cybersecurity ventures. Explaining the smart hotel room case, the framework shows how to prioritize and avoid these risks cost-optimally. Nevertheless, the study has not concealed some of the limitations such as a confined and static nature of the IoT testbed, potential difficulties in adjusting the proposed training approach in large-scale and dynamically changing IoT environments. Although, it has advocated for the enhanced flexibility of the proposed method for IoTA applications with a certain configuration of characteristics.

2.3 Integration of Machine Learning and Deep Learning in IoT Security

Li et al. (2023) present a detailed and important survey on the class of graph-powered learning with examples of its use in IoT systems. This they do to explain how graph neural networks (GNNs), graph embedding, and related technologies help in solving IoT issues such as network anomaly detection, malware detection, and service recommendations.

What their work demonstrates is that GNNs are indeed capable of operating within IoT's dynamic and diverse environments, especially in smart transport, industrial IoT, and smart cities. Nevertheless, to the authors' knowledge, obstacles such as scalability, heterogeneity, or resource limitations still persist. Scholars propose further developments of the presented approach, such as dynamic graph analysis and the implementation of digital twins to improve IoT system performance and protection.

Alsoufi et al. (2024) proposed a new anomaly-based intrusion detection system (AIDS) for IoT using a Sparse Autoencoder (SAE) and Convolutional Neural Network (CNN) in their paper of 2024. The SAE works to eliminate attributes while the CNN works to classify data into binary classes. Validated on the Bot-IoT dataset, the model achieves exceptional results: it achieved 99.9% accuracy, 100% of the 50 sample data points were correctly retrieved, and only 3 in 10,000 data points were falsely identified as belonging to the class. Indeed, it does not require as much computational power as different approaches, including CNN+LSTM and SAE+ANN, and it is faster when it comes to training. In the study, the flexibility and effectiveness of the proposed SAE-CNN model are highlighted in protecting resource-scarce IoT systems from current-day cyber threats.

Based on the GNN architecture, Altaf et al. (2023) present a network intrusion detection framework for IoT network systems. Their model is a contribution to GNNs and eliminates problems associated with previous models by embracing multi-edge graph structures in addition to applying spectral and spatial convolution operations. It is designed to capture interactions between nodes and traffic distribution and demonstrates performance improvements across the benchmark datasets with accuracy of over 99% in some cases. From the comparative analysis, it is found that the proposed framework is better than E-GraphSAGE in terms of accuracy, precision, recall, and F1-score, with fewer false alarms than E-GraphSAGE. Based on these insights, this research emphasizes that far more progressive GNN designs hold great promise for IoT security.

The authors, Lo et al. (2022), proposed E-GraphSAGE, a Graph Neural Network (GNN) that aims to implement Network Intrusion Detection Systems (NIDS) in IoT systems. Compared to traditional GraphSAGE, E-GraphSAGE is specifically designed to identify both edge features and node topologies in the flow-based structure, improving its vigilance against threatening network behaviours. Evaluation metrics on four datasets, such as BoT-IoT and ToN-IoT, clearly confirm the enhanced performance of E-GraphSAGE with F1 scores as high as 1 for multi-classification on BoT-IoT and 0.87 on ToN-IoT. Binary classification offers accuracy as high as 99.99% with a very low false positives rate. Such outcomes prove that the proposed solution is better than the existing state-of-the-art on IoT cybersecurity.

Wu et al. (2021) propose the concept of GNNs for anomaly detection in IIoT. They also divide anomalies into point, context, and collective, using GNNs in smart transport, energy, and manufacturing IIoT applications. The work proves that GNNs work and can achieve up to 97.5% in smart energy systems for fault detection and 96.2% in contextual traffic anomaly detection. Collective anomaly detection in manufacturing processes also yields new promising results and increases classification precision. However, there are several issues that have been raised by this study: the issues of data heterogeneity and scalability, among other issues, which present the researchers with the need to develop new designs of GNNs for the IIoT platform in the future.

It is evident from the reviewed literature that there is a need for proper improvement of cybersecurity in IoT due to the limitations of resources and heterogeneity in IoT systems and their global distribution. Traditional anomaly-based intrusion detection systems

Table 1: Comparison of Literature Studies

Ref.	Year	Study Purpose	ML/DL	Dataset	Target Size	Classes	Algorithm
Bernabe & Skarmeta	2022	Examined European cybersecurity threats and proposed holistic approaches with SDN/NFV and cryptographic protocols.	ML	Various	Not Specified	Anomalous, Normal	Various ML Techniques
Marshal et al.	2021	Analyzed IoT smart healthcare vulnerabilities and proposed a security framework.	ML	Medical IoT Dataset	Not Specified	Intrusion, No Intrusion	Decision Trees, SVM
Choo et al.	2021	Proposed a multilayer taxonomy for IoT cyberattacks and tested it on realistic scenarios.	DL	IoT Network Dataset	Not Specified	Anomalous, Normal	CNN, RNN, Autoencoders
Chopra	2020	Analyzed IoT operational and information technology (OT & IT) vulnerabilities.	ML	Various	Not Specified	Anomalous, Normal	Various ML Techniques
Ahmad et al.	2022	Systematic review of IoT-cloud security concerns, focusing on PaaS and SaaS models.	ML	IoT Network Dataset	Not Specified	Anomalous, Normal	Autoencoder Techniques
Mendhurwar & Mishra	2019	Comparative analysis of intrusion detection systems and machine learning-based model analysis.	ML	Various Surveillance	Not Specified	Intrusion, No Intrusion	CNN, LSTM, SVM
Raimundo & Rosário	2022	Proposed anomaly-based IDS for IoT using Sparse Autoencoder and CNN.	DL	IoT Network Dataset	Not Specified	Anomalous, Normal	CNN, Sparse Autoencoder
Alajlan et al.	2023	Proposed a layered architectural model for IoT cybersecurity and risk management.	ML	Industrial Dataset	Not Specified	Anomalous, Normal	SVM, Random Forest
Lee	2020	Reviewed IIoT security with 70 core articles; emphasized blockchain and ML as key solutions.	ML	IIoT Dataset	Not Specified	Anomalous, Normal	Decision Tree, SVM
Li et al.	2023	Surveyed graph-powered learning for IoT using GNNs for anomaly detection and service recommendations.	ML	GNN Dataset	Not Specified	Intrusion, No Intrusion	GNN, Neural Networks
Alsoufi et al.	2024	Developed anomaly-based IDS using Sparse Autoencoder and CNN for IoT systems.	DL	IoT Network Dataset	Not Specified	Anomalous, Normal	CNN, Autoencoder
Wang et al.	2023	Proposed GNN-based intrusion detection framework with multi-edge graph structures.	ML	IoT Network Dataset	Not Specified	Anomalous, Normal	GNN, Multi-Edge Models
Lo et al.	2022	Developed E-GraphSAGE for NIDS in IoT systems, addressing edge and node topology detection.	DL	IoT Network Dataset	Not Specified	Anomalous, Normal	E-GraphSAGE, GraphSAGE
Wu et al.	2021	Studied GNNs for anomaly detection in IIoT systems, classifying point, context, and collective anomalies.	ML	IIoT Dataset	Not Specified	Anomalous, Normal	GNN, Traffic Models
Our Study	2024	IoT Security through Anomaly-based Intrusion Detection Systems.	ML/DL	IoT Botnet Attacks	Various	Malicious, Benign	GCN, GIN, Naïve Bayes, KNN, GBM

(IDS) become complemented with the use of machine learning (ML) and deep learning (DL) and look suitable for discovering unknown threats and filtering excessively frequent false positives. Generally, IDS developments, especially with the indication of enhanced technologies such as blockchain, GNNs, and sparse autoencoders, bespeak a promising capability to meet IoT-specific issues. This foundation points to the need for efficient and scalable methodologies, which is why the next chapter will focus on identifying and proposing these improved strategies.

3 Methodology

The objective of this study is to create an effective method to classify the IoT network traffic accurately and detect different types of behaviours – normal and abnormal – in IoT networks. This chapter then provides a brief overview of the method: data acquisition and preparation, data exploration, and feature construction. Last but not least, the chapter contains the description and analysis of the modelling and evaluation techniques that constitute the subject of research. The typical flow of a machine learning-based cybersecurity analysis system is shown in Figure 1 below.

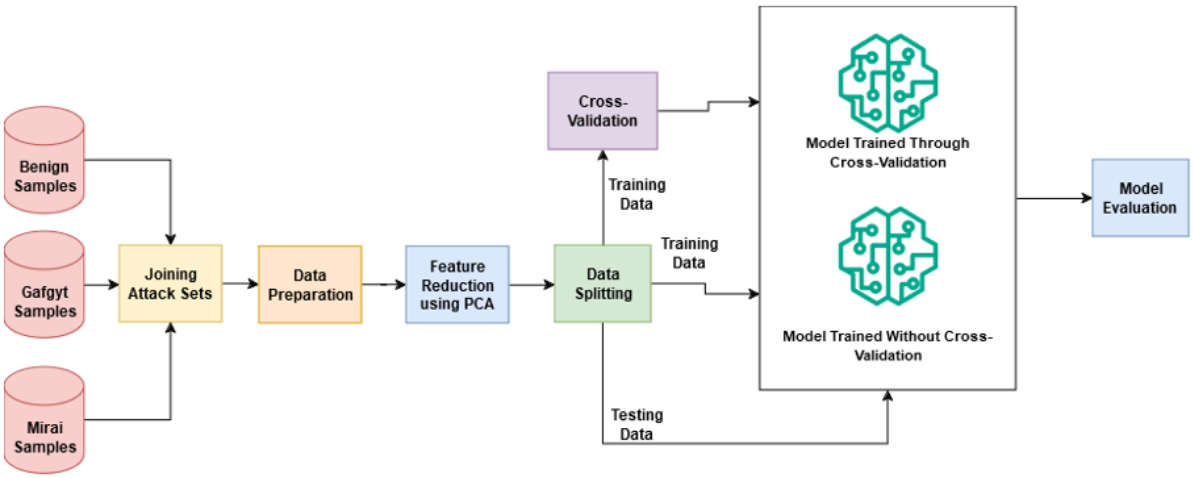

Figure 1: Cybersecurity Analysis using Machine Learning Flow

3.1 Dataset Description

The dataset used in the analysis for this study is obtained from the UCI Repository *UCI Machine Learning Repository* (2018) . The dataset under consideration consists of data collected from various devices. The dataset is derived from communication traffic from several devices within an IoT network. It also holds benevolent traffic and traffic generated from sources such as Gafgyt (BASHLITE) and Mirai – both of which are marked separately as classes. The data it yielded contains numerous features obtained from statistical characteristics of network behaviour, such as mean value, variance, and standard deviation.

The classes included are:

- **Benign:** No significant traffic spikes or lows, no presence of unusual traffic patterns.
- **Gafgyt Attacks:** This framework also comprises of combo, junk, scan, TCP and UDP attacks' types.
- **Mirai Attacks:**Including the scenarios of ack, scan, syn, UDP and UDP plain.

The data for each class of the attacks are present separately in the dataset and is given in CSV files. After combining, the total number of samples in the dataset amounts to 169278 samples with 115 features for each attack type. A label column is added to the dataset based on the data collected from the file. There are a total of 11 classes present in the dataset making it a multi-class classification problem. To provide for reasonable class distribution while at the same time dealing with class imbalance, the authors adopted workable stratified sampling where all the 11 classes had equal representation while maintaining the statistical distribution of each. By combining these two datasets, a balance of sentiments that assures a good data set for training the machine learning models is obtained. Figure 2 below shows the final distribution of the attacks in the combined dataset.

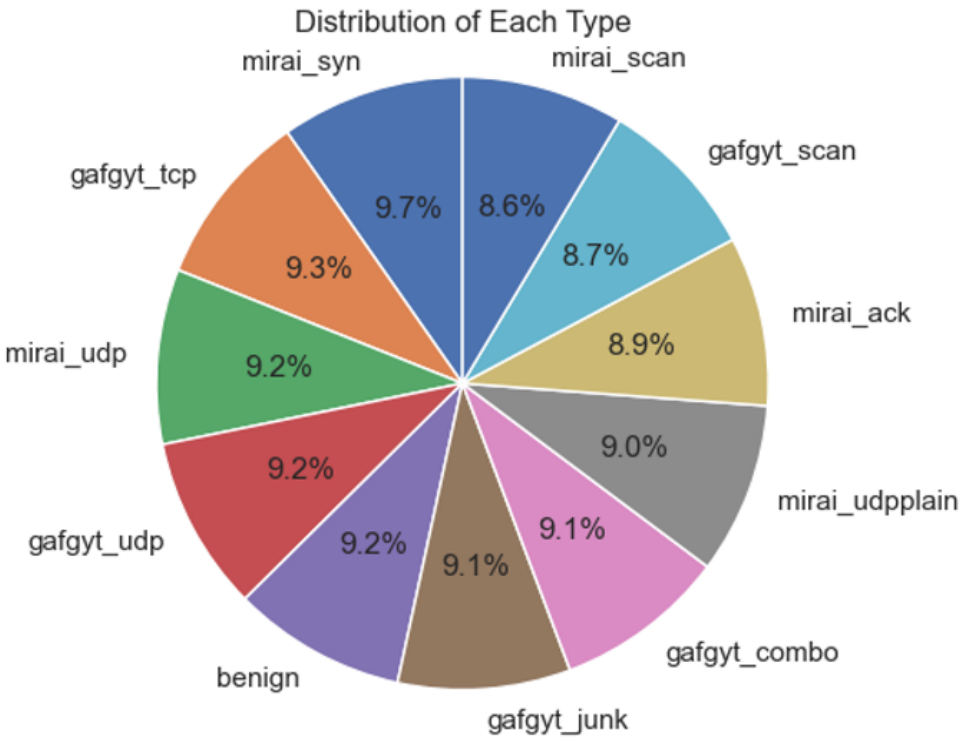

Figure 2: Distribution of Class Labels

3.2 Data Preprocessing

Data preprocessing is vital in analysing and modelling the data to come up with a meaningful result. The following steps were undertaken: The dataset underwent stratified down-sampling to ensure balanced representation of classes, with variable labels describing the type of traffic associated with each record. Missing values were addressed using mean imputation, where the missing values of a feature were replaced with its mean, preserving the original data distribution (Pedregosa et al.; 2011; Little and Rubin; 2002).Feature scaling was performed using Scikit-learn's StandardScaler to standardise features to zero mean and unit variance, which is particularly crucial for models like Support Vector Machines (SVM) that rely on the magnitude of features (Hastie et al.; 2009). Additionally, Principal Component Analysis (PCA) was applied for dimensionality reduction, preserving 95% of the variance and reducing computational complexity, especially for deep learning models.

3.3 Modelling

To provide a classification of network traffic, both the conventional machine learning methods, and deep learning frameworks were used, although each offering unique features. The study was designed to use both KNN, to obtain a synergistic benefit to produce the best solution that is accurate with IoT network traffic classification with greater reliability.

3.3.1 Traditional Machine Learning Models

The traditional approaches of machine learning were used for its simplicity, interpretability and computational time. Such models have been useful in the management of structured data and giving reference points for other more sophisticated models. The following algorithms were employed:

Random Forest: Random Forest is one of the most popular ensemble methods that builds a lot of decision trees to reduce variance and obtain better test accuracy and stronger regularization simultaneously. To achieve diversity among individual trees, the model subdivides feature space and data space randomly, assigning partial feature space and data to each tree in the model. The final reduction is achieved through a majority vote of trees, making it immune to noise and less prone to overfitting (Breiman; 2001). The algorithm is particularly beneficial when the feature interactions in the dataset are complex (Ho; 1995).

Gradient Boosting: :As a machine learning technique, Gradient Boosting iteratively develops a set of models, typically decision trees, by reducing the residuals of the preceding model. For each new tree, the errors of the previous tree are corrected, ultimately resulting in a highly accurate prediction model (Friedman; 2001). Its strength lies in tuning the weights of a developed model and the non-linearity of the function, making it suitable for classification problems with complex datasets (Chen and Guestrin; 2016).

Support Vector Machines (SVM): SVM focuses on identifying the hyperplane that best classifies classes in multidimensional space. Feature space transformations are applied to convert a dataset into a space where separation by a hyperplane becomes feasible. This approach is most appropriate when the separating hyperplane is distinct, making SVM a good choice for IoT network classification (Cortes and Vapnik; 1995).

K-Nearest Neighbours (KNN): KNN is a simple yet efficient method that determines the benchmark position of present data elements in the feature space. It is suitable for small datasets and useful in early data analysis but may require extensive computation for larger datasets (Cover and Hart; 1967).

Gaussian Naive Bayes (GNB):): GNB is a classifier that operates based on Bayes' theorem, assuming that features are independent. While this independence assumption may not always hold, GNB is computationally efficient and yields reasonable results for high-dimensional datasets. Its simplicity makes it a useful starting point or benchmark(Rish; 2001).

3.3.2 Deep Learning Models

Deep learning models were chosen for their ability to handle large, high-dimensional datasets and capture complex patterns that traditional models might miss. The study employed both sequential and graph-based architectures to address the unique characteristics of IoT network data.

Recurrent Neural Networks (RNN), LSTM, and GRU: These models process time-series data, retaining memory of earlier inputs, making them ideal for temporal dependencies, such as those representing specific attack behaviors in IoT network traffic. LSTM and GRU are particularly designed to overcome the vanishing gradient problem, enabling long-term dependency handling (Hochreiter and Schmidhuber; 1997; Cho et al.; 2014).

Graph Neural Networks (GNN): IoT network datasets often contain inherent relationships between features that can be modeled as graphs. GNNs enable relational reasoning, making them highly suitable for such tasks (Scarselli et al.; 2009).

Graph Convolutional Network (GCN):): GCNs aggregate information from neighboring nodes, capturing feature representations that consider both local and broader graph contexts. This approach enhances IoT network traffic classification by modeling dependencies between features (Kipf and Welling; 2017).

Graph Isomorphism Network (GIN): GINs incorporate multi-layer perceptrons (MLPs) in the GCN structure during aggregation, making them more expressive and capable of distinguishing graph structures. This capability is crucial for identifying variations in IoT network attack patterns (Xu et al.; 2019).

3.3.3 Model Training and Validation

All models were trained on 70% of the dataset and validated through 10-fold cross validation to make the proposed models more reliable and generalize. This validation technique partitions the data into 10 folds, which in each round uses nine folds for training and the tenth for testing, which reduces the chances of overemphasizing correctness. Mean values of accuracy, precision, recall, and F1-score of all the folds were used to assess the efficiency of each model. For this reason, this paper followed this approach of rigour to ensure that the training and testing sets did not influence the results.

3.4 Evaluation

Model evaluation was performed using the following metrics to assess performance comprehensively:

1. **Accuracy:** The proportion of correctly classified samples across all classes.
2. **Precision:**The ratio of true positives to predicted positives indicates model reliability in classifying a specific category.
3. **Recall (Sensitivity):** The ratio of true positives to all actual positives, reflecting the model's ability to identify a class.
4. **F1-Score:**The harmonic mean of precision and recall, providing a balanced performance metric.
5. **ROC-AUC:** The area under the Receiver Operating Characteristic curve, measuring the model's ability to distinguish between classes.

Confusion matrices were generated to provide insights into misclassification patterns. Deep learning models, particularly GNNs, consistently outperformed traditional machine learning models, with superior F1-scores and recall.

4 Design Specifications

IoT network traffic classification is challenging, and the chosen approaches must provide high accuracy and efficiency. This chapter discusses the design requirements and performance assessment measures of the machine learning as well as deep learning models adopted in the study. Two distinct approaches are employed to validate the models: with and without cross-validation. Cross-validation is a more stringent way of approaching the model validation as means of assessing its ability to generalise by using multiple partitions of the data for training and validation. The approach without cross-validation employed the train-test split to assess the skills within models and work with less computational resources at the cost of stability. The system architecture for the study is shown in Figure 3 below.

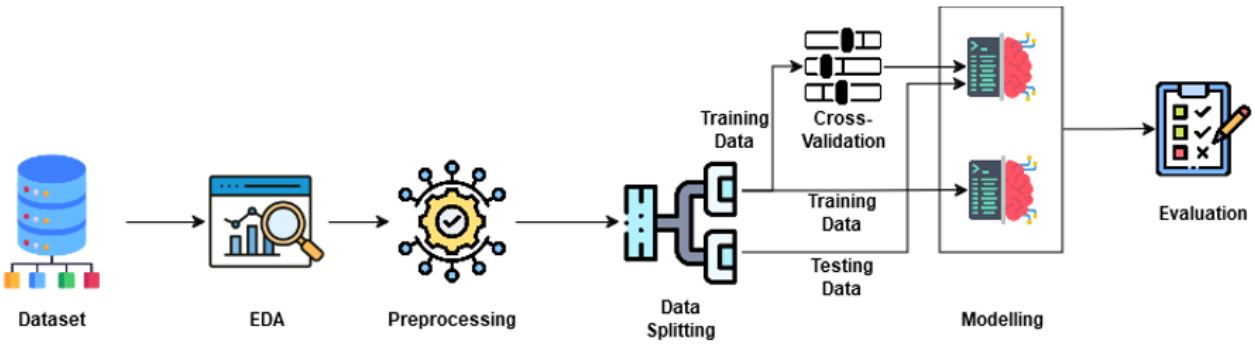

Figure 3: System Architecture

4.1 Modelling with Cross-Validation

The concept of cross validation and the process of applying the model using inputs from the former is used. Peculiarities of cross-validation is a rational concept for assessment of models and generalisation. of the obtained results. Cross-validation resembles k-fold validation where it splits K subgroups called folds and the rest K subgroups are used for training in the current implementation of the system. 1 folds when using the remaining 25% of data to validate the model. This process is repeated K times, i.e., find X nováK. This This approach drastically eliminates over fitting of models and which on average provides a decent biased assessment of the models. performance. However, prior to inputting the data into the cross-validation process, the data is first pre- processed. There are many operational variables within the data set and most of these variables have missing values exceeding 40 percent. which are replaced by statistical imputation this

like, for instance, the mean or median. Standardisation meth- ods are used on feature scaling so that the mean of the features becomes zero and 12 variance equal to one. Also, Principal Component Analysis (PCA) is applied to reducing the dimensionality by asking for 10 principal components form the data in an in an effort to cut down on computation time, while trying to provide as much information as will be useful. The features are also preprocessed by filtering correlated features after undergoing correlation treatment to bring feature selection into a more manageable and interpretable framework for analysis. used data is in the form of randomly selected dataset of snapped shots of samples divided into training and test set. The training dataset is partitioned into 10 various folds. Each fold is used one for the purpose of validation, the other folds are used for training of the model. This approach guarantees that all points of data are enter to training and validation, which takes therefrom, there is inconsistency in the estimation of performance.

4.2 Modelling without Cross-Validation

The manner in which the model is conducted without cross validation is generally easy to. as it only entials the division of data into two sections which are the training section and the testing section. Other methods like the leave one out method are less computationally intensive and thereby, although having stronger statistical properties in comparison to cross-validation, can provide the same level of high reliability in evaluation of the performance. The same pre-processing that has been discussed in cross-validation is applied. Regarding data preprocessing step, there are missing values in the features. Indeed, many of the features are standard. In the present study, PCA is applied to assist in the solution of the above problem. of the dimensionality, reduction, and feature selection are based on the correlation analysis. for further improvement of the range of features to be included in the final set. The training set is subtlety only the materials that were used for training the models. the test material comprises only the material for testing the models. Differently from the In the case of the cross-validation method, the dataset is not partitioned and repartitioned time and again. This approach is effective in the training phase since less time is consumed but it YMight not be very accurate. Lack of cross-validation reduces the computational burden, and hence should be avoided. in the first stages or if there are limitations in the calculations capabilities of the available analytical tools. However, it does not have the stability and utilization of the cross-validation technique. The is due to the fact that the assessment of the models is based on only one distinct division.

4.3 Outcome

The IDS integrates both traditional machine learning (ML) models, such as Random Forest, Gradient Boosting, k-Nearest Neighbour (KNN), Gaussian Naive Bayes (GNB), and Support Vector Machines (SVM), as well as advanced deep learning (DL) architectures, including Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), Graph Convolutional Networks (GCN), and Graph Isomorphism Networks (GIN). Among these, Random Forest and KNN demonstrated the highest accuracy at 96.30% and 96.77%, respectively, while LSTM and GCN excelled at recognising complex traffic patterns. The GIN model further outperformed GCN in handling specific network scenarios. This design ensures scalability, robustness, and adaptability to diverse IoT environments

5 Implementation

The impact of the prospective IoT network traffic classification system is discussed in this chapter. Implementation stage is the set-up of the computer hardware and software, arrangement of the development environment for this project, hooking up of the operations described above under data preparation, modeling, or evaluation among other things. Working on the system, the latest tools and technologies were employed to guarantee high accuracy, fast results, and possibility to expand the system's functionality. The objective of Intrusion Detection System (IDS) was to design and set up a well-structured pipeline analysis of IoT networks traffic. The first process was data pre-processing Data set from the UCI repository was pre-processed to handle missing values using mean imputation, scaling features using standardisation and feature selection using PCA. Feature selection was done by correlation analysis in order to select the best features for model building. For graph-based deep learning models, the author created graphs to represent relations within data.

5.1 System Configuration

The implementation utilised a robust hardware and software setup to ensure seamless execution of the computationally intensive tasks involved in the project. The system configuration is as follows:

- **Hardware Specifications:**
  - **RAM:** 8GB DDR4
  - **Storage:** 1TB HDD + 256GB SSD
  - **GPU:** AMD Radeon RX Vega 10 Graphics
  - **Processor:** AMD Ryzen 7
- **Operating System:** Windows 11 Home Single Language (64-bit)

The inclusion of a dedicated AMD Radeon RX Vega 10 Graphics significantly accelerated the training of deep learning models, particularly those using architectures such as LSTM, GRU, and Graph Neural Networks. The NVMe SSD enhanced data read/write speeds, optimising data preprocessing and model training tasks.

5.2 Development Configuration

The development environment was configured to facilitate efficient implementation of machine learning and deep learning workflows. Key tools and libraries included:

- **Programming Language:** Python 3.9
- **Integrated Development Environment (IDE):** Jupyter Notebook (via Anaconda distribution)
- **Libraries:**
  - **Data Handling and Analysis:** NumPy, Pandas

- **Visualisation:** Matplotlib, Seaborn
- **Machine Learning:** Scikit-learn
- **Deep Learning:** TensorFlow, PyTorch
- **Graph Neural Networks:** PyTorch Geometric

These tools provided a seamless framework for implementing the various phases of the project, including data preprocessing, visualisation, feature engineering, model development, and evaluation.

5.3 Model Training and Configuration

A small amount of data cleaning was performed on the input data, addressing missing values with mean imputation, scaling features with Scikit-learn's `StandardScaler`, and performing feature extraction using PCA while retaining 95% of the variance. The Intrusion Detection System (IDS) was developed using both conventional machine learning and deep learning approaches. Traditional models such as Random Forest, KNN, Gradient Boosting, Gaussian Naïve Bayes, and Support Vector Machines were trained with default settings and slight tuning. For Random Forest, `n_estimators` was set to 100, and Gradient Boosting utilized a `learning_rate` of 0.1. KNN used `n_neighbors` set to 5, and SVM applied a radial basis function (RBF) kernel with `C=1.0`.

Deep learning models, including LSTM, GRU, Graph Convolutional Networks (GCNs), and Graph Isomorphism Networks (GINs), were implemented to capture temporal and relational patterns in IoT network traffic. The LSTM and GRU models were configured with 128 hidden units and a batch size of 32. The GCN and GIN models used two graph convolution layers with a hidden layer size of 64 and a learning rate of 0.01. Dropout regularization with a rate of 0.5 was applied to prevent overfitting.

To evaluate the stability and generalizability of the models, a 10-fold cross-validation process was employed, splitting the data into ten sets. Each iteration trained on nine folds and validated on the remaining fold, ensuring that data was used for both training and validation without redundancy. These configurations provided a robust architecture for the IDS, addressing the specific requirements of IoT network security.

6 Evaluation

This chapter provides a detailed assessment of the IoT network traffic classification system, examining model performance under cross-validation and standard training conditions. It highlights the most significant results, analyses their relevance to the research objectives, and discusses their implications in both academic and practical contexts.

6.1 Experiment 1: Modelling with Cross-Validation

This section provides the results obtained for the modelling with 10-Fold Cross Validation. The results obtained for the modelling with cross-validation is consolidated in Table 2 below.

Table 2: Results for Modelling with Cross-Validation

Model	Accuracy	Precision	Recall	F1 Score	ROC AUC
Gradient Boosting	0.9267	0.9314	0.9267	0.9264	0.9960
KNN	0.9677	0.9681	0.9677	0.9678	0.9966
Gaussian Naive Bayes (GNB)	0.5845	0.5843	0.5845	0.5399	0.9676
Random Forest	0.9630	0.9663	0.9630	0.9628	0.9977
SVM	0.8103	0.7756	0.8103	0.7773	0.9833
LSTM	0.8846	0.8523	0.8846	0.8537	N/A
RNN	0.8709	0.8278	0.8709	0.8397	N/A
GRU	0.8882	0.8475	0.8882	0.8575	N/A
GCN	0.7587	0.7197	0.7587	0.7263	0.9844
GIN	0.7912	0.7560	0.7912	0.7591	0.9751

6.1.1 Results Analysis

The Gradient Boosting Model (GBM) achieved an accuracy of 92.67%, a precision of 93.14%, and a recall of 92.67%, demonstrating strong overall performance. Its ROC AUC of 0.9960 indicates excellent discriminatory capability. Class-wise, GBM consistently performed well, with precision and recall near or above 90% for most categories. However, the model struggled with *mirai_udp* and *gafgyt_scan*, as shown by their lower recall of 81% and 80%, respectively.

The KNN model exhibited outstanding performance with an accuracy of 96.77%, precision of 96.81%, and recall of 96.77%. Its ROC AUC of 0.9966 further supports its strong predictive capabilities. KNN performed exceptionally well across all classes, with precision and recall nearing or reaching 100% for benign and critical malicious categories.

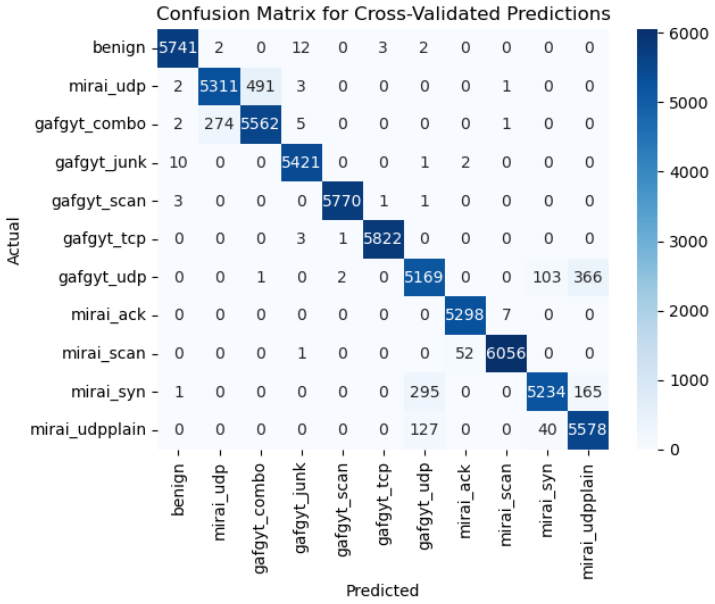

Figure 4: Confusion Matrix for KNN Model

The Gaussian Naive Bayes (GNB) model achieved a relatively lower accuracy of 58.45%, with precision and recall at 58.43% and 58.45%, respectively. While the ROC

AUC of 0.9676 suggests the model has some discriminatory power, it struggled to effectively classify several categories, particularly *gafgyt_scan* and *mirai_syn*, where recall was 58.45%.

The Random Forest model delivered exceptional results, with an accuracy of 96.30%, precision of 96.63%, and a recall of 96.30%. Its ROC AUC of 0.9977 demonstrates near-perfect classification ability.

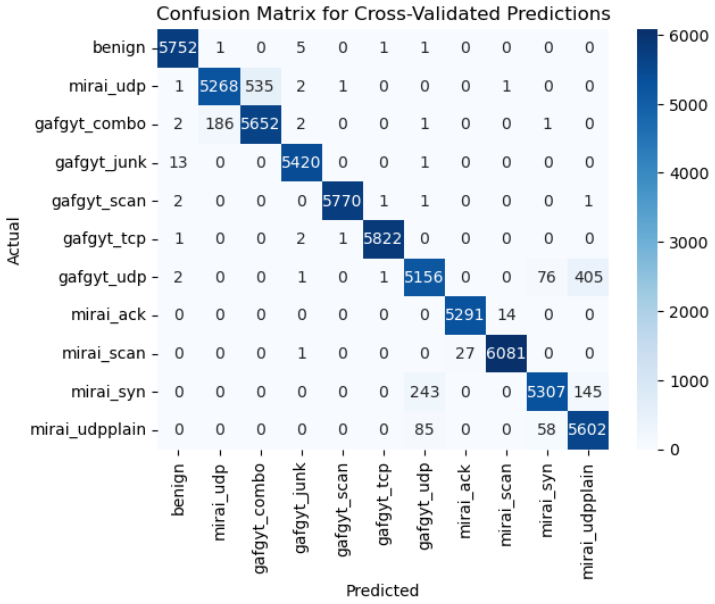

Figure 5: Confusion Matrix for Random Forest Model

The LSTM model demonstrated robust performance, achieving an accuracy of 88.46%, a precision of 85.23%, and a recall of 88.46%. The ROC AUC further highlighted its capacity for classification tasks. The model excelled in recognising benign and malicious traffic like *mirai_ack* and *gafgyt_combo*.

The GRU model outperformed standard RNNs, achieving an accuracy of 88.82%, a precision of 84.75%, and a recall of 88.82%. Its ROC AUC highlights strong classification performance

The GCN model showed moderate results, achieving an accuracy of 75.87%, a precision of 71.97%, and a recall of 75.87%. Its ROC AUC of 0.9844 indicates good discriminatory capability, but the confusion matrix highlights significant challenges in classifying traffic types like *gafgyt_scan* and *gafgyt_tcp*, which were frequently mislabelled.While GCNs excel in leveraging graph-structured data, further optimisation in graph construction could improve their performance on this dataset.

The GIN model achieved slightly better results than GCN, with an accuracy of 79.12%, a precision of 75.60%, and a recall of 79.12%. The ROC AUC of 0.9751 indicates good classification potential. Similar to GCN, GIN performed well for benign and specific malicious traffic types like *gafgyt_combo* and *mirai_ack*. However, it struggled with *gafgyt_tcp* and *mirai_scan*, suggesting that further optimisation is required to exploit GIN's full potential.

6.2 Experiment 2: Modelling without Cross-Validation

The evaluations without cross-validation also gave better performance measures for most of the models than with cross-validation as the latter includes validation splits which might again discourage the models from performing their very best on the training data set. This approach allowed to assess the full potential of each algorithm: it performed well for intricate pattern and imbalanced class distributions.

The results obtained for the 10 models implemented in the study without cross-validation are consolidated in Table 3 below.

Table 3: Results for Modelling without Cross-Validation

Model	**Accuracy**	**Precision**	**Recall**	**F1 Score**	**ROC AUC**
Gradient Boosting	0.9379	0.9424	0.9379	0.9376	0.9968
KNN	0.9819	0.9821	0.9819	0.9820	0.9998
Gaussian Naive Bayes (GNB)	0.5830	0.5859	0.5830	0.5385	N/A
Random Forest	0.9813	0.9845	0.9813	0.9811	0.9977
SVM	0.8127	0.8704	0.8127	0.7799	0.9836
LSTM	0.8910	0.9376	0.8910	0.8603	0.9968
RNN	0.8772	0.9088	0.8772	0.8464	0.9961
GRU	0.3638	0.2946	0.3638	0.2839	0.9745
GCN	0.7632	0.7253	0.7632	0.7309	0.9890
GIN	0.7900	0.7600	0.7900	0.7578	0.9755

6.2.1 Results Analysis

The Gradient Boosting Model (GBM) showed a slightly higher efficiency, with an accuracy of 0.9379 and an ROC AUC of 0.9968, which also proved the model's good Class Discrimination

Without cross-validation, KNN achieved an even higher accuracy of 98.19%, with uniformly strong class-wise performance. Precision and recall for all classes were above 90%, with many achieving near-perfect scores. The confusion matrix confirms minimal classification errors, reinforcing the model's reliability for differentiating between benign and malicious traffic in this experiment.

GNB showed consistent performance with a slightly lower accuracy of 58.30% compared to Experiment 1. Misclassifications among malicious classes (*gafgyt_combo*, *mirai_udpplain*) remained prevalent, as evidenced by the confusion matrix. The model's reliance on Gaussian assumptions is likely unsuitable for the complex, multimodal distribution of the data.

The Random Forest model achieved a near-perfect accuracy of 98.13% and a ROC AUC of 0.9977, showcasing its strength in handling high-dimensional datasets. Class-wise metrics reveal precision and recall close to 100% for most categories, particularly for benign, *mirai_ack*, and *gafgyt_junk*.

The Support Vector Machine (SVM) model showed moderate performance with an accuracy of 81.27% and a ROC AUC of 0.9836. While it excelled in recognising benign and some malicious classes like *gafgyt_combo* and *mirai_ack*, its precision and recall dropped significantly for *gafgyt_scan* and *mirai_udp*.

The Long Short-Term Memory (LSTM) model delivered strong results, achieving an accuracy of 89.10% and a ROC AUC of 0.9968. It excelled in recognising benign and

certain malicious classes, such as *mirai_ack* and *gafgyt_junk*, with precision and recall approaching 100%.

The Recurrent Neural Network (RNN) achieved an accuracy of 87.72% and a ROC AUC of 0.9961. Similar to LSTM, the RNN model performed well for benign and certain malicious categories, , such as *mirai_ack* and *gafgyt_combo*.

The Graph Isomorphism Network (GIN) performed slightly better than GCN, achieving an accuracy of 79.12% and a ROC AUC of 0.9755. Class-wise metrics indicate robust performance for benign, *mirai_ack*, and *gafgyt_junk*, with precision and recall close to 100%.

6.3 Discussion

The results show that there is great discrepancy in the accuracy achieved out of all algorithms and modelling situation. Random forest and KNN were found to be accurate with fair precision or recall depending on the metric used, suggesting the models ability to deal with the inherent complexity in the dataset. These models also had impressive resistance to violation of class imbalance as a result a keeper performance in almost all categories.

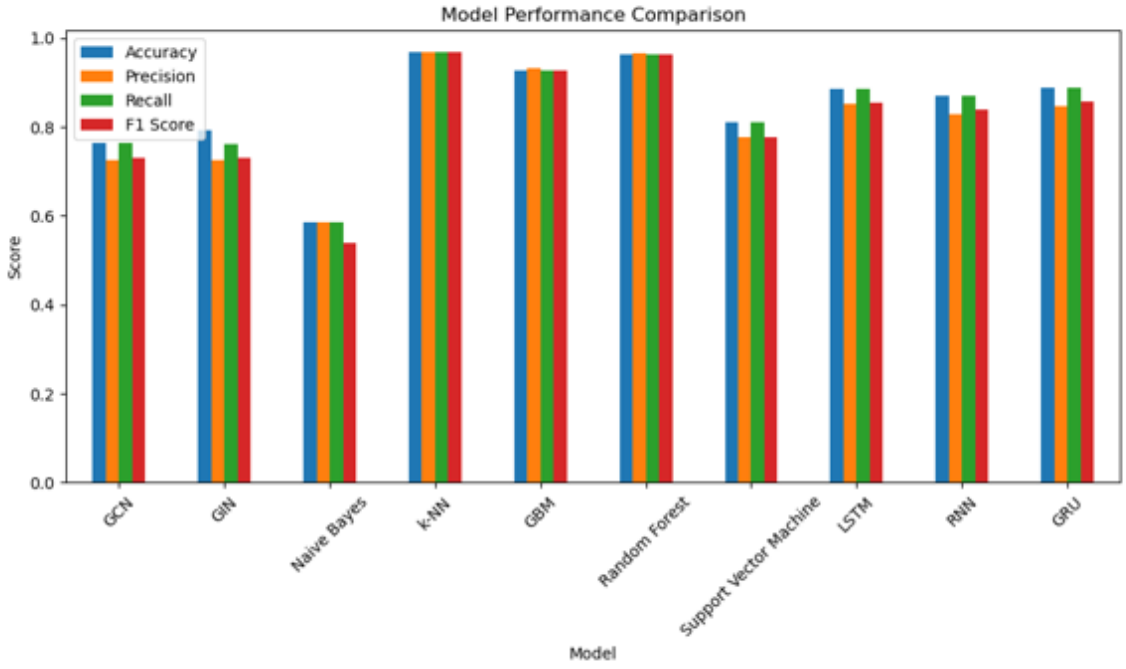

Figure 6: Model Performances with Cross-Validation

On the other hand, such models as GNB and GRU showed some severe drawbacks Response and Recommendation The obtained results suggest that the analyzed models show moderate performance, while models such as GNB and GRU present significant drawbacks. The use of a generative approach in GNB meant that it had to deal with complex higher dimensions of feature space and some classification was off the mark. Likewise, because of a failure to model the dependencies within the sequences, GRU presented notably low recall for several of the categories. These results accentuate the

need for choosing appropriate algorithms according to the properties of a given set of data and the problem solving task at hand.

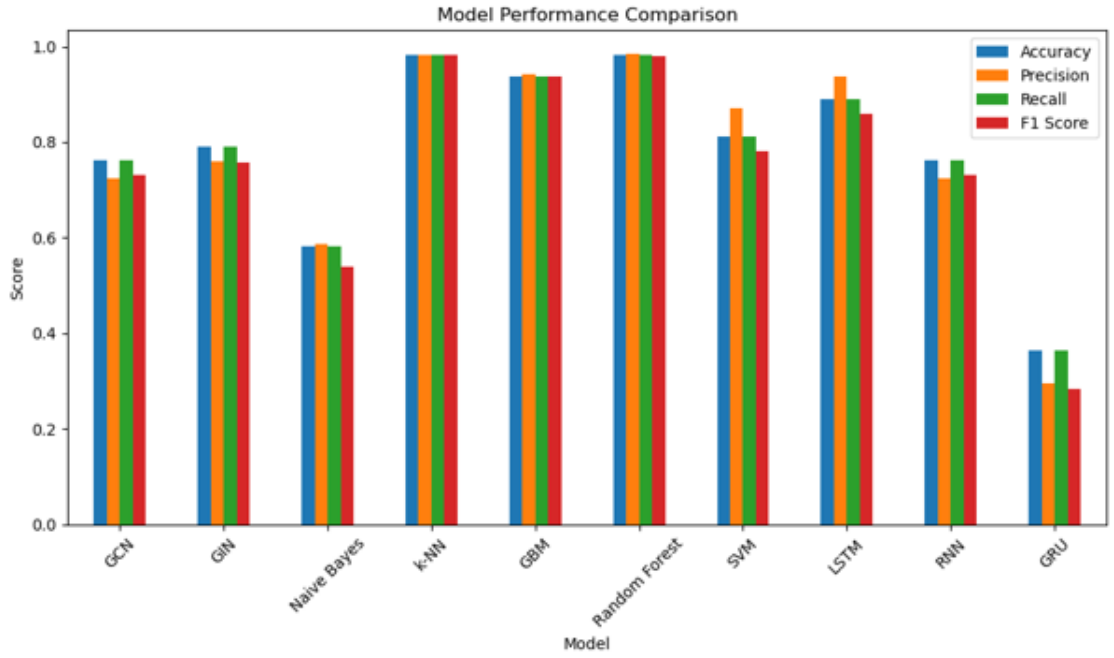

Figure 7: Model Performances without Cross-Validation

Therefore, in cross validation and non cross validation scenario , the performance of the models has shown better non cross validation environment may be due to less over head involved in cross-validation. But this may imply overly complex models are being trained; a problem of overfitting. From the ROC AUC results, most models show high levels of performance for the models' ability to assign different classes with high accuracy, Gafgyt Scan and Gafgyt TCP are constantly misclassified and may need feature separation analysis and alternative data set bias.

7 Conclusion and Future Work

7.1 Conclusion

Hundreds of industries benefit from enhanced interconnectedness and automation because of IoT device popularity and fast adoption. The rapid development of networking systems has created major security dangers which require specific Intrusion Detection Systems (IDSs) for IoT infrastructures. The research developed an anomaly-based intrusion detection system (IDS) that combined traditional machine learning methods alongside Graph Neural Networks (GNNs) as an advanced deep learning technique. The study provides several key insights:

The outcome of modeling with KNN and Random Forest exceeded other models by achieving top results for accuracy and precision and recall and F1 scores while handling traffic class imbalances to find anomalous data points in most network classes. These analytical tools delivered dependable output findings while maintaining interpretability for various IoT systems. The Gradient Boosting Machine (GBM) demonstrated overall

successful performance yet struggled to identify certain traffic types particularly Mirai UDP and Gafgyt Scan. The Gaussian Naive Bayes (GNB) model had the worst performance levels because of its basic Gaussian distribution assumption which triggered higher misclassification rates in particular traffic categories.

Research on recurrent architectures demonstrated that Long Short-Term Memory earned better accuracy scores and recall statistics for managing temporal relationships than Gated Recurrent Unit. The relational patterns within IoT network data became feasible through Graph Neural Networks including Graph Convolutional Networks (GCNs) and Graph Isomorphism Networks (GINs). The traffic classification results showed GIN performing better than GCN for complex network scenarios while maintaining its capacity to recognize intricate patterns. The models showed difficulty in precise detection of traffic types including Gafgyt TCP and Mirai Scan.

The models performed slightly better using non-cross-validation designs because they eliminated data splitting and reduced computational loads. Model generalisability received more realistic evaluation through cross-validation while maintaining computational efficiency. System requirements must determine which validation method works best for each deployment situation. The results of this study highlight the value of choosing models which correspond to the peculiar needs of IoT anomaly detection software systems. Traditional models consisting of KNN and Random Forest remain straightforward to run yet GNNs continue to prove essential in processing intricate IoT traffic complexity. Fundamental IDSs for IoT networks take shape through hybrid approaches which integrate traditional anomaly detection methods along with deep learning algorithms to create resilient adaptive systems.

7.2 Future Work

Despite the promising results achieved in this study, several limitations and opportunities for future research remain. These include:

1. **Enhanced Graph Neural Networks:**
    - The robustness of the GNN-based models still pose challenges because the theoretical instantiation of a graph neural network is O(n2) and in real-world application, graphs are often very large.. To this end, subsequent studies could analyze the strategies for constructing a more efficient graph, or sample data using GraphSAGE or hierarchical GNNs.
2. **Incorporating Real-Time Capabilities:**
    - Real-time intrusion detection is essential for IoP networks security as they revealed.. The future studies should aim at enhancing the proposed IDS to fit actual-time environments using less resource-intensive deep learning systems or methods based on accelerator hardware.
3. **Addressing Class Imbalances:**
    - The observed misclassifications in underrepresented traffic types suggest the need for advanced techniques to handle class imbalances. Techniques such as synthetic oversampling, cost-sensitive learning, or generative adversarial networks (GANs) for data augmentation could improve classification performance.

References

Ahmad, W., Rasool, A., Javed, A., Baker, T. and Jalil, Z. (2021). Cyber security in iot-based cloud computing: A comprehensive survey, *Electronics* **11**(1): 16.

Alajlan, R., Alhumam, N. and Frikha, M. (2023). Cybersecurity for blockchain-based iot systems: a review, *Applied Sciences* **13**(13): 7432.

Alsoufi, M., Razak, S., Siraj, M., Nafea, I., Ghaleb, F., Saeed, F. and Nasser, M. (2021). Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review, *Applied Sciences* **11**(18): 8383.

Alsoufi, M., Siraj, M., Ghaleb, F., Al-Razgan, M., Al-Asaly, M., Alfakih, T. and Saeed, F. (2024). Anomaly-based intrusion detection model using deep learning for iot networks, *Computer Modeling in Engineering & Sciences* **141**(1): 823–845.

Altaf, T., Wang, X., Ni, W., Yu, G., Liu, R. and Braun, R. (2023). A new concatenated multigraph neural network for iot intrusion detection, *Internet of Things* **22**: 100818.

Bernabe, J. and Skarmeta, A. (2022). Introducing the challenges in cybersecurity and privacy: The european research landscape, *Challenges in Cybersecurity and Privacy-the European Research Landscape*, River Publishers, pp. 1–21.

Breiman, L. (2001). Random forests, *Machine Learning* **45**(1): 5–32.

Chen, T. and Guestrin, C. (2016). Xgboost: A scalable tree boosting system, *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, ACM, pp. 785–794.

Cho, K., van Merriënboer, B., Gulcehre, C., Bahdanau, D., Bougares, F., Schwenk, H. and Bengio, Y. (2014). Learning phrase representations using rnn encoder-decoder for statistical machine translation, *arXiv preprint* **arXiv:1406.1078**.
URL: *https://arxiv.org/abs/1406.1078*

Choo, K., Gai, K., Chiaraviglio, L. and Yang, Q. (2021). A multidisciplinary approach to internet of things (iot) cybersecurity and risk management, *Computers & Security* **102**: 102136.

Chopra, A. (2020). Paradigm shift and challenges in iot security, *Journal of Physics: Conference Series*, Vol. 1432, IOP Publishing, p. 012083.

Cortes, C. and Vapnik, V. (1995). Support-vector networks, *Machine Learning* **20**(3): 273–297.

Cover, T. and Hart, P. (1967). Nearest neighbor pattern classification, *IEEE Transactions on Information Theory* **13**(1): 21–27.

Farooq, M., Khan, M. and Khan, R. (2023). Implementation of network security for intrusion detection & prevention system in iot networks: Challenges & approach, *Int. J. Advanced Networking and Applications* **15**(05): 6109–6113.

Friedman, J. H. (2001). Greedy function approximation: A gradient boosting machine, *Annals of Statistics* **29**(5): 1189–1232.

Hastie, T., Tibshirani, R. and Friedman, J. (2009). *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*, 2nd edn, Springer, New York, NY, USA.

Ho, T. K. (1995). Random decision forests, *Proceedings of the 3rd International Conference on Document Analysis and Recognition*, IEEE, pp. 278–282.

Hochreiter, S. and Schmidhuber, J. (1997). Long short-term memory, *Neural Computation* **9**(8): 1735–1780.

Inayat, U., Zia, M., Mahmood, S., Khalid, H. and Benbouzid, M. (2022). Learning-based methods for cyber attacks detection in iot systems: A survey on methods, analysis, and future prospects, *Electronics* **11**(9): 1502.

Industrial IoT - market size worldwide 2020-2030 (2024).
URL: *https://www.statista.com/statistics/611004/global-industrial-internet-of-things-market-size/*

Kipf, T. N. and Welling, M. (2017). Semi-supervised classification with graph convolutional networks, *arXiv preprint arXiv:1609.02907* .

Lee, I. (2020). Internet of things (iot) cybersecurity: Literature review and iot cyber risk management, *Future Internet* **12**(9): 157.

Li, Y., Xie, S., Wan, Z., Lv, H., Song, H. and Lv, Z. (2023). Graph-powered learning methods in the internet of things: A survey, *Machine Learning with Applications* **11**: 100441.

Little, R. J. and Rubin, D. B. (2002). *Statistical Analysis with Missing Data*, 2nd edn, Wiley-Interscience, Hoboken, NJ, USA.

Lo, W., Layeghy, S., Sarhan, M., Gallagher, M. and Portmann, M. (2022). E-graphsage: A graph neural network based intrusion detection system for iot, *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, IEEE, pp. 1–9.

Marshal, R., Gobinath, K. and Rao, V. (2021). Proactive measures to mitigate cyber security challenges in iot based smart healthcare networks, *2021 IEEE International IoT, Electronics and Mechatronics Conference (IEMTRONICS)*, IEEE, pp. 1–4.

Mendhurwar, S. and Mishra, R. (2021). Integration of social and iot technologies: architectural framework for digital transformation and cyber security challenges, *Enterprise Information Systems* **15**(4): 565–584.

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, E. and Duchesnay, (2011). Scikit-learn: Machine learning in python, *Journal of Machine Learning Research* **12**: 2825–2830.

Raimundo, R. and Rosário, A. (2022). Cybersecurity in the internet of things in industrial management, *Applied Sciences* **12**(3): 1598.

Rane, J., Mallick, S., Kaya, O. and Rane, N. (2024). Automated machine learning (automl) in industry 4.0, 5.0, and society 5.0: Applications, opportunities, challenges, and future directions, *Future Research Opportunities for Artificial Intelligence in Industry 4.0 and 5.0* **5**: 2.

Rish, I. (2001). An empirical study of the naive bayes classifier, *IJCAI Workshop on Empirical Methods in AI*, pp. 41–46.

Scarselli, F., Gori, M., Tsoi, A. C., Hagenbuchner, M. and Monfardini, G. (2009). The graph neural network model, *IEEE Transactions on Neural Networks* **20**(1): 61–80.

UCI Machine Learning Repository (2018).
URL: *https://archive.ics.uci.edu/dataset/442/detection+of+iot+botnet+attacks+n+baiot*

Ullah, I. and Mahmoud, Q. (2021). Design and development of a deep learning-based model for anomaly detection in iot networks, *IEEE Access* **9**: 103906–103926.

What is IoT Security? (n.d.).
URL: *https://www.paloaltonetworks.in/cyberpedia/what-is-iot-security*

Wu, Y., Dai, H. and Tang, H. (2021). Graph neural networks for anomaly detection in industrial internet of things, *IEEE Internet of Things Journal* **9**(12): 9214–9231.

Xu, K., Hu, W., Leskovec, J. and Jegelka, S. (2019). How powerful are graph neural networks?, *arXiv preprint arXiv:1810.00826* .

Yaseen, A. (2023). The role of machine learning in network anomaly detection for cybersecurity, *Sage Science Review of Applied Machine Learning* **6**(8): 16–34.