National College of Ireland

Addressing Cloud Security Challenges using AI-Driven IoT Intrusion Detection Systems with UQ-IDS Dataset

MSc Research Project
Cybersecurity

Sabareesan Mohandass
Student ID: X22215786

School of Computing
National College of Ireland

Supervisor: Michael Prior

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Sabareesan Mohandass
Student ID:	X22215786
Programme:	Cybersecurity **Year:** 2023-2024
Module:	MSc Research Project
Lecturer:	Michael Prior
Submission Due Date:	12/08/2024
Project Title:	Addressing Cloud Security Challenges using AI-Driven IoT Intrusion Detection Systems with UQ-IDS Dataset
Word Count:	6717 **Page Count:** 22

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: Sabareesan

Date: 12/08/2024

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):	

Addressing Cloud Security Challenges using AI-Driven IoT Intrusion Detection Systems with UQ-IDS Dataset

Sabareesan Mohandass
X22215786

Abstract

Cloud computing and the Internet of Things (IoT) have expanded the attack surface and led to the introduction of new cybersecurity challenges, necessitating improved security measures to protect against the increased risk. However, traditional Intrusion Detection Systems (IDS) have been unable to keep up with use of evolving threats. Issues with traditional IDSs include high false-positive rates and poor ability to detect new types of attacks by utilizing sophisticated techniques. To overcome these challenges in this research, we propose a Conv-LSTM hybrid model that takes the strengths of Convolutional Neural Networks (CNN) in identifying patterns and the strengths of Long Short-Term Memory (LSTM) networks in processing sequential data. By using a hybrid architectural approach to the problem, we can improve both the accuracy of detection and reduce false positives. This research also includes an implementation of a web application that can be used in real time to present alerts to administrators through a friendly web interface. The novelty aspect of this research is the implementation of hybrid model Conv-LSTM, which is the most accurate model for detecting the anomalies from the system as compared to CNN and LSTM. Also, the implementation of web application in the cloud environment, offers a realistic and industry valid framework for a scalable and efficient cybersecurity solution for the modern network infrastructure.

1 Introduction

With the increasing popularity of cloud services in recent times, the importance of cyber security has now taken on a new level of urgency. While cloud services provide the convenience of less need for physical services and flexible operations compared to traditional IT solutions, the numerous opportunities for cyber-attacks have become a new reality. The reality is that the move to cloud services is no small thing. The recent figures have shown that approximately 69% of businesses today use cloud services (Tatineni, 2023), and cloud services such as AWS, Microsoft, Google, and others have become the backbone of operations. As the data and resources often take part in the cloud across distributed networks, it's now easier for hackers to exploit these vulnerabilities. Adding IoT devices to the mix can exacerbate this issue. For example, many companies deploying IoT continue to try to get ahead of the new cybersecurity norms. Companies must take a proactive approach to cybersecurity to protect themselves from unauthorized users accessing the data or resources available through the cloud.

Cybersecurity experts continue to work hard to develop strategies for preventing such attacks as DDoS (Distributed Denial of Service) and prevent hackers for exploiting potential weaknesses in cloud services. The fact that cloud services and IoT devices have experienced rapid growth, the threat of being compromised is as high as it has ever been and the need for high quality cyber security strategies is paramount. In the 21st century, preventing cyber-attacks is not an option but a necessity. Companies need to be ensuring that they have the latest tools to combat cyber-attacks that are growing in sophistication such as Intrusion Detection Systems and monitoring services. Companies as they leverage cloud services more frequently must make and take the necessary steps to ensure their data or resources are secure.

Amid the risks and uncertainties raised by the simultaneous use of cloud services in both private and public sectors, researchers have presented the need to address these challenges by introducing effective threat detection methods to identify the intrusion. An intrusion detection system (IDS) system is a common approach by experts that helps in tackling cyber security issues more distinctly. However, it is evident that some cloud security attacks such as "denial-of-service" (DoS) attacks, "cross-site scripting" attacks, "routing information attacks" and "distributed denial-of-service" (DDoS) attacks are some foremost challenges that require detection and thwarting to identifying the network attacks (Bakro et al., 2023). Although the IDS system is effective in identifying most cyber security attacks, the escalation of the attack configuration to advanced levels has introduced significant concerns. Nevertheless, Bakro et al., (2023) explained that it is integral to introduce a well-proposed IDS system that can effectively detect the intrusion of novel attacks.

With the complexities observed with network attacks when using cloud computing technologies, incident responses are a central concern with a firm's defence strategy. As previously discussed, network attacks are continuously evolving due to which industrial experts and developers are facing significant challenges to mitigate future risks. Amid these uncertainties, the development and integration of new solutions are both imperative and helpful through which organisation can detect, comprehend as well as mitigate the threat. Over the years, many detection methods have been introduced by experts that are indeed helpful with existing attacks. However, cloud security threats in recent times are continuously escalating with advanced capabilities, corresponding to which existing methods often fail to introduce countermeasures against the novel attack. It is, therefore, becoming increasingly imperative to introduce advanced detection techniques that can bolster firms' network security. As a matter of fact, numerous studies have been conducted that critically described the significance of optimal settings as well as consequences regarding intrusion detection in cloud computing and IoT environments. Among several integrated methods that have been introduced in recent times such as machine learning-based IDS detection, network intrusion detection system (NIDS), and others, a current advancement to artificial intelligence (AI) infused intrusion detection has gained significant priority in detecting threats in cloud security.

As firms are increasingly expanding their applications and data within the cloud system, there is a spontaneous need for threat detection in cloud security to ensure efficient response to particular incidents. According to certain evidence, AI integration in cloud infrastructure is a potential solution that addresses potential cybersecurity issues. A wide knowledge of AI informs that the algorithmic process facilitates an accurate and rapid intrusion/incident detection response where specific datasets are used for intrusion detection within the computer networks. Originally, some common datasets that have gained priority are KDD-CUP_99, NSL-KDD, and ISCX. Some modern intrusion detection methods such as deep learning-based intrusion detection systems are using these datasets to detect intrusion in IoT and fog networks. While understanding this, some studies have revealed the importance of artificial intelligence in successful intrusion detection by presenting suitable information on the solution it provides, and the dataset usually used. In this regard, the UQ-IDS dataset has gained significant attention.

1.1 Research Objectives

To improve and enhance the IoT security, we will achieve the following research objectives:

- To develop and implement a hybrid deep learning model (Conv-LSTM) that combines the strengths of CNN and LSTM for real-time intrusion detection in IoT networks.
- To evaluate the performance of CNN, LSTM, and Conv-LSTM models on the UQ IoT IDS dataset, using metrics such as accuracy, precision, recall, and F1-score.
- To design and deploy a web application that utilizes the Conv-LSTM model for real-time attack detection and alerting, ensuring a user-friendly interface for administrators and users.

1.2 Research Question

In this work, we aim to address the following research question:

- How can the integration of a hybrid Conv-LSTM deep learning model within a real-time web application, deployed in a cloud environment, enhance cybersecurity by improving the detection of intrusions in IoT networks compared to traditional approaches?

2 Related Work

The second chapter of the study provides an emphasis on the information from the literature that has summarised the importance of network intrusion detection systems (NIDS) and other methods in detecting network intrusion or cyber security attacks. In this emphasis, information has been contextualised on different datasets that are often used in the detection process and also explores the significance these datasets hold in detecting novel attacks in cloud security. Accordingly, a literature gap has been established, which distinctly provides a direction for future research scope in the area.

2.1 Empirical Analysis of Intrusion Detection Techniques and Emerging Cybersecurity Challenges

In the above data table, evidence from different studies has been summarised based on which, the significance of each study and their contribution to the current research has been determined. Considerably, in this section, an empirical discussion is performed to extensively explore the information and produce insights based on which, the gap can be identified. Integrated automatic intrusion detection has become an interesting area of discussion because of the need to detect the rising cybersecurity threats in computer networks and applications. In this regard, Guezzaz et al. (2022) explained that malicious and novel attacks are ongoing dilemmas faced by users due to their ability to infect wired as well as wireless networks. In another study presented by Kayode Saheed et al. (2022), a discussion of network threats in the IoT environment has been discussed which shows that the proliferation of the network application in terms of extensive use has been posing privacy threats with the continuous emergence of novel attacks. From the study perspective, it has been established that companies globally are increasingly investing and making efforts to improve malicious attack detection. In this regard, intelligent procedures are explored by measuring accuracy and other parameters as well as comparing them to identify the best method of intelligent identification of attacks.

In the below data table, evidence from different studies has been summarised based on which, the significance of each study and their contribution to the current research has been determined. Considerably, in this section, an empirical discussion is performed to extensively explore the information and produce insights based on which, the gap can be identified. Integrated automatic intrusion detection has become an interesting area of discussion because of the need to detect the rising cybersecurity threats in computer networks and applications. In this regard, Guezzaz et al. (2022) explained that malicious and novel attacks are ongoing dilemmas faced by users due to their ability to infect wired as well as wireless networks. In another study presented by Kayode Saheed et al. (2022), a discussion of network threats in the IoT environment has been discussed which shows that the proliferation of the network application in terms of extensive use has been posing privacy threats with the continuous emergence of novel attacks. From the study perspective, it has been established that companies globally are increasingly investing and making efforts to improve malicious attack detection. In this regard, intelligent procedures are explored by measuring accuracy and other parameters as well as comparing them to identify the best method of intelligent identification of attacks.

2.2 Intrusion Detection system using Machine Learning Methods

Nizamudeen (2023) explained that the intelligent classification of intrusion detection methods has gained wide attention due to the introduction of improved network systems and the continuous prevalence of malicious attacks. With the assessment of the study, it has been observed that the introduction of “Intelligent Intrusion Detection Framework” (IIDF) has gained priority in the detection of novel attacks in the network and applications where data from different datasets are used to pre-process data, select important features and classification (Nizamudeen 2023). Indicating the study objectives, a DL-based intrusion detection method is

introduced - 2D-ACNN which has been identified as a binary classifier that has detected both normal and abnormal network traffic with an accuracy of 97.24% and a false-positive alarm rate of 2.5% respectively. In another study presented by Douiba et al. (2023), the author discussed the importance of IoT as an improved network infrastructure; however, its popularity comes with undeniable security threats. The study introduces various ML and DL-based intrusion detection methods, the detection accuracy of which is investigated using benchmarked datasets - NSL-KDD, IoT-23, and BoT-IoT datasets. As per the experimental result, the algorithm-based IDS methods have shown a nearly 99.99% detection accuracy rate with minimum computation time.

Network Intrusion Detection Systems (NIDS) have gained significant attention due to their improved defense mechanisms in protecting computer networks from diverse and sophisticated attacks (Layeghy et al., 2024). While understanding this, the study detected another issue with supervised algorithms intrusion detection where existing datasets such as KDD99 have certain limitations due to which an optimal result failed to be obtained (Layeghy et al., 2024). Therefore, the study introduces specific NIDS datasets that are of high quality and ideally labelled network traffic as benign and malicious. Another study presented by Lata & Singh (2022) has presented the fundamental concept of intrusion detection in cloud services, which is considered to be another essential and remarkable network infrastructure. Nevertheless, malicious users' interference in network security creates vulnerability in the system with their increasing fraudulent activities. The study, therefore, extensively focused on new intrusion detection methods and widely explored three concerns - cloud security vulnerability, feature selection, and analysis of IDS techniques. Based on this approach, specific insights on issues and future research scope are obtained. Olabanji et al. (2024) explained that detecting cyber security threats in cloud computing and IoT environments is increasingly essential due to the increasing vulnerability users are facing when using the network system. In this regard, the study discussed the contribution of artificial intelligence and various algorithms in malicious attack detection in the network system. It has been observed that an AI-driven intrusion detection system is an advanced approach, which provides a hybrid security infrastructure with enhanced predictive capabilities that have been observed with improved accuracy in threat detection.

Cybersecurity is an emerging topic in the contemporary IT research paradigm due to the rising network and system vulnerabilities. Talukder et al. (2024) explained that machine-learning-based intrusion detection through behaviour analysis has gained importance due to the detection accuracy examined amidst the dynamism of cyber threats. Accordingly, the study demonstrates the importance of certain datasets - UNSW-NB15, CIC-IDS-2017, and CIC-IDS-2018. As per the observation of the focused experiment, it has been observed that ML models such as decision trees, random forests, and ensemble classifiers where random forest and ensemble classifiers provide 99.59% and 99.95% detection accuracy rate with the UNSW-NB15 dataset. On the contrary, each model attains an accuracy level of 99.99% with the CIC-IDS-2017 dataset and 99.94% with the CIC-IDS-2018 dataset respectively. Focusing on

another study by Zarpelão et al., (2017), a priority to the IoT paradigm is initially given extended to which network security issues are addressed. As per the understanding of the study findings, it has been observed that traditional IDS methods are ineffective in detecting novel cyber threats. Potential implications for the validation of new IDS methods are elicited with scope for new research directions where IDS schemes need to be explored further.

2.3 Advancements in Intrusion Detection Systems for Cloud Computing

A narrow-down focus on the growth trend observed in cloud computing services in recent years has demonstrated both opportunities and concerns in its application (Archana et al., 2021). In this regard, Al-Ghuwairi et al., (2023) explained that with the overgrowing concern for cloud security challenges, the significance of "Network Intrusion Detection Systems" (NIDS) has come to light. However, an ongoing issue with false-positive alarm rate remains a concern, which mainly because of the use of existing datasets. Concerningly, Al-Ghuwairi et al., (2023) introduced an improved feature selection method along with an intrusion detection model that can address the issue of misleading with time-series anomalies as well as attacks. The experimental result explored in the study shows that the performance of both feature selection and the "Facebook Prophet" prediction model shows efficiency with improved performance. In another study presented by Bharati & Tamane (2020), the authors investigated the importance of advanced nIDS method driven by ML and DL methods to detect cyber-attacks in cloud computing. In this approach, the CSE-CIC-IDS-2018 dataset is used, based on which a supervised ML model - random forest shows an accuracy level of 99%.

Accordingly, the information presented by Long et al. (2024) explains that cloud infrastructure needs a robust defence system that can secure network-accessible resources. In this regard, the study introduced a transformer-based NIDS method that provides an accuracy level of 93% compared to the CNN-LSTM model, thus underpinning the effectiveness of the intrusion detection method in cloud security enhancement. A compound knowledge achieved from the distinct review of the empirical evidence has explained the novelty of cloud computing technology in the current network paradigm. However, it is imperative to introduce a robust detection mechanism for novel attacks that are most concerning in contemporary network systems. Attou, Guezzaz, et al. (2023) explained that detecting anomalies in network traffic requires an improved IDS system to ensure proper prediction. Since existing models have become inefficient in detecting novel attacks, improved models are introduced. For instance, the above study introduced an RF classifier whose accuracy level is measured through parameters using two datasets - BoT-IoT and NSL-KDD. As per the experimental observation, the accuracy level detection shows an estimation of 98.3% for the BoT-IoT dataset and 99.99% for the NSL-KDD dataset respectively.

Table 1: Summary of Literature Review table

Author name and Year	Journal name	Summative Findings
(Kayode Saheed et al., 2022)	"A machine learning-based intrusion detection for detecting internet of things network attacks."	The study introduced a supervised ML-driven IDS system that detects IoT attacks with a potential accuracy of 99.99%. The IDS system introduced has enabled a restriction of information leakage by using a minimum-maximum normalisation process to enhance feature scaling.
(Zarpelão et al., 2017)	"A survey of intrusion detection in Internet of Things."	As per the study findings, the focus has been underpinned by IoT security challenges faced in recent decades and the rising importance of IDS systems. Survey-based information on intrusion detection is obtained which is indicated through different attributes - detection methods, placement strategy of IDS, possible security threats, and validation strategies.
(Attou et al., 2023)	"Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing."	The successive findings produce necessary evidence for the cloud security measures required due to inherent threats identified with technological advances. The study provides information on ML and DL-based IDS systems and illustrates their detection performance using "Bot-IoT" and "NSL-KDD" datasets.
(Douiba et al., 2023)	"Anomaly detection model based on gradient boosting and decision tree for IoT environments security."	The study summarizes the importance of IoT as an intelligent distribution of networks that provide an interface to the private and public sectors without any human intervention. Apart from underpinning the importance of IoT, the findings further summarised the security concerns observed in the IoT environment. In this regard, various algorithms-based IDS systems are explored while their performance is evaluated using features from different datasets - "NSL-KDD", "BoT-IoT", and "IoT-23".
(Olabanji et al., 2024)	"AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection."	The study summarizes a comparative effectiveness between AI-driven intrusion detection based on user-behavior analysis and conventional security measures for cloud systems. The established findings provide an analysis of necessary hybrid security strategies necessary in a cloud computing environment. Besides, it provides suitable insights regarding the effectiveness of AI-driven cloud security measures.

2.4 Literature Gap

Our literature review has helped to identify multiple deficiencies in modern Intrusion Detection Systems (IDS). Many modern IDS models, including those based on machine learning and deep learning, have struggled with high false-positive rates and have found it difficult to detect novel cyber-attacks, especially in cloud computing and IoT environments. Additionally, numerous IDS systems are not user-friendly, and are not real-time, which is required by modern distribution systems with large numbers of users. As a response, in this research we propose a modern IDS that is capable of integrating the power of Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to increase detection accuracy and decrease false positives. We were also able to develop a modern, real-time web application that is able to help bridge the gap of ease of use and the challenge of creating or using real-time IDS. The web application we developed is able to alert an administrator in real-time of an intrusion, and prevent a possible security concern.

3 Research Methodology

Maintaining a high-level security is very important to confirm save and trustful communication between several organizations. The research is taken by gathering the raw data form the various sources, preprocessing the data by indicating the large number of values that are unique in the target, which results in multiclass classification and to handle the large amount of data, the large number labels need large number of resources. Other than that, our methodology consists of several set of steps which will help to build an optimal intrusion detection system for detecting anomalies in the real time. The methodology diagram of the research as shown in Figure 1.

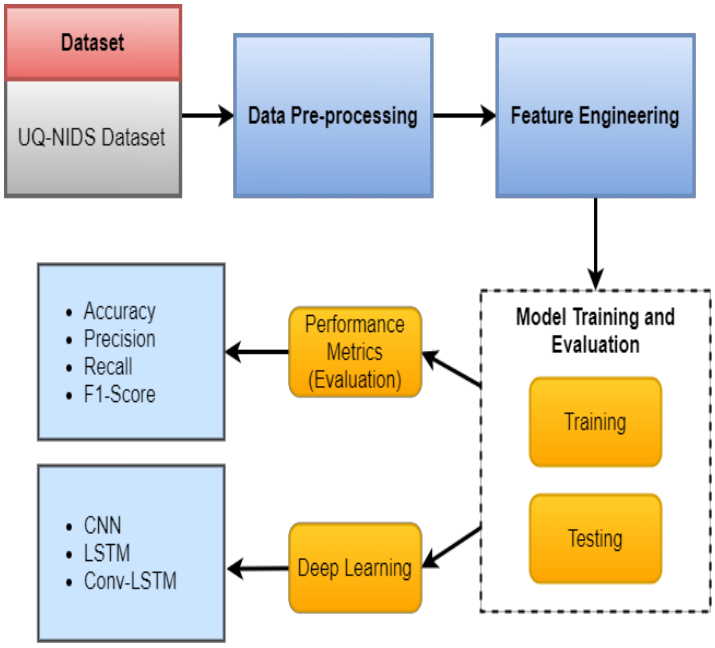

Figure 1: Methodology for Developing Intrusion Detection System

3.1 Dataset Description

In this research the data is gathered from NF-UQ-NIDS dataset, which is provided by the university of Queensland Sarhan, M. & Layeghy, S. (2023). This dataset consists of several small files and contains the flow from multiple networks. The categories of the attack are modified by combining all the parent categories. There are various attacks such as DoS Attacks-Hulk, DoS attacks slow HTTPTest, etc. DDOS attack-LOIC-UDP, DDOS attack-HOIC etc., is renamed to DDoS. Various attacks are combined as brute-force category such as FTP-BruteForce, SSH-BruteForce, Brute Force-Web. And last the SQL Injection attacks have been added to the category of injection attacks. There are 11,994,893 records in the data out which 9,208,048 (76.77%) are class of benign flows and 763285 are of DDos class, Reconnaissance having count of 482946, Injection have the count of 468575 and DoS class with a count of 348962, Brute Force class with a count of 291955, Password with count 156299 and there are many other class such as XSS, Infilteration, Exploits, Scanning, Fuzzers, Backdoor, Bot, Generic, Analysis, Theft, Shellcode, MITM, Worms, Ransomware.

3.2 Data Pre-processing

Data Preprocessing is a crucial part in the phase of model development. In data preprocessing step the data is cleaned i.e., removing null values from the data, fixing the outliers, filling missing values with other methods such as mean, median mode etc., transforming the data, and integration of data in order to make the data ready for further evaluation. With the help of data preprocessing, the quality of data is improved for better classification data and to improve the performance of the model. In the research, the attack column indicating a large number of unique values in the target, which gives the result as multiclass classification, but to handle this large number of labels needs large data which need a large number of resources. So, the attack column is categorized based on the type of attach classes such as DDoS, DoS, Reconnaissance, scanning, mitm are categories as Network Attacks, similarly some classes are categorized as Exploitation Attacks, some are Benign and other which are left as categorized as Unknown. All the data are merged to form a final dataset for further evaluation. Categorical features are converted to categorical features. Data such as IP is converted into decimals. Null values are checked and there are no null values present in the data.

3.3 Exploratory Data Analysis

Exploratory data analysis also plays an important role in uncovering the facts and insights from the data. These insights can be very helpful in examining many questions and pattern which is present in the data visually. The data analysis is carried out by plotting a histogram shown in Figure 2. shows a histogram plot to find the distribution between IPV4_SRC_ADDR with respect to Attack_Category. On the IPV4_SRC_ADDR the exploitation attack is much and there is less attack of benign. This indicates that exploitation attack should be prevented or controlled on IPV4_SRC_ADDR.

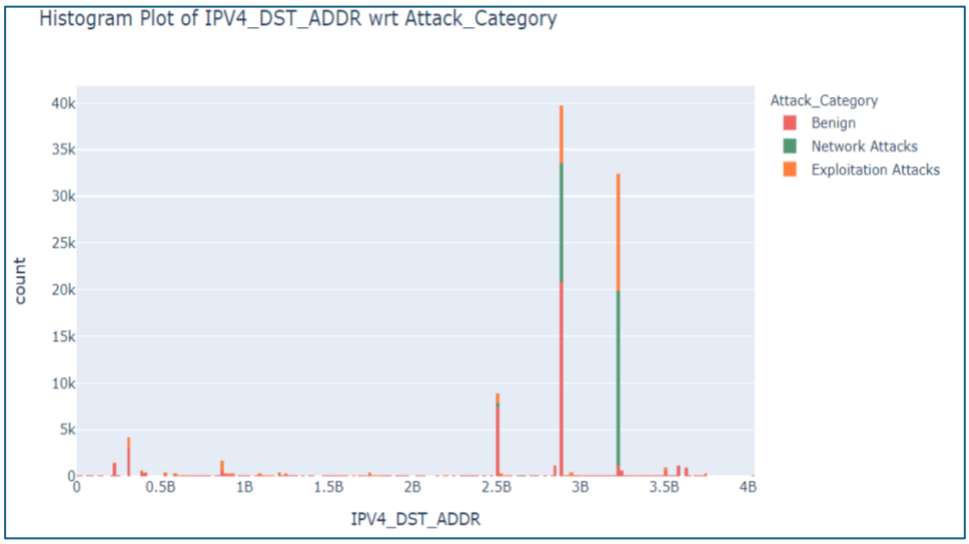

Figure 2: IPV4_DST_ADDR with respect to Attack

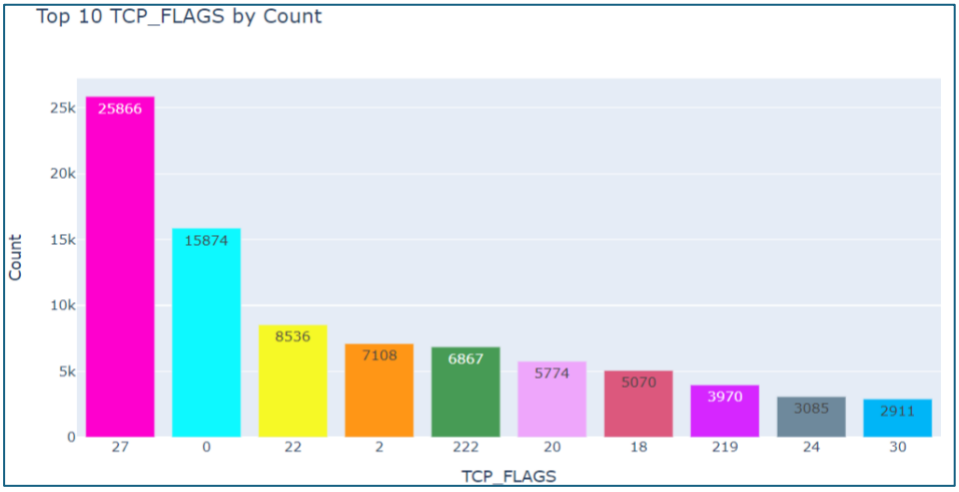

Figure 3: Top 10 TCP Flags

Figure 3, shows a bar chart for the top 10 TCP flags. TCP stands for Transmission Control Protocol which are control bits and used for managing the state and flow of communication between devices in the network. The top 10 TCP flags are given with the highest number of TCP flag of 27 type which is 25866 and the lower is 2991.

Figure 4: TCP flags with respect to attack categories.

Figure 4, shows a sun burst chart which gives the number of TCP flags with attack categories, the categories are 27, which consists of 27 network attacks, 27 benign, 27 exploitation attacks, and 30 TCP flags with attack categories as 30- Network attacks, 30 Benign, 24 Benign and 219 Benign. Similarly for 20, 18, 222 etc.

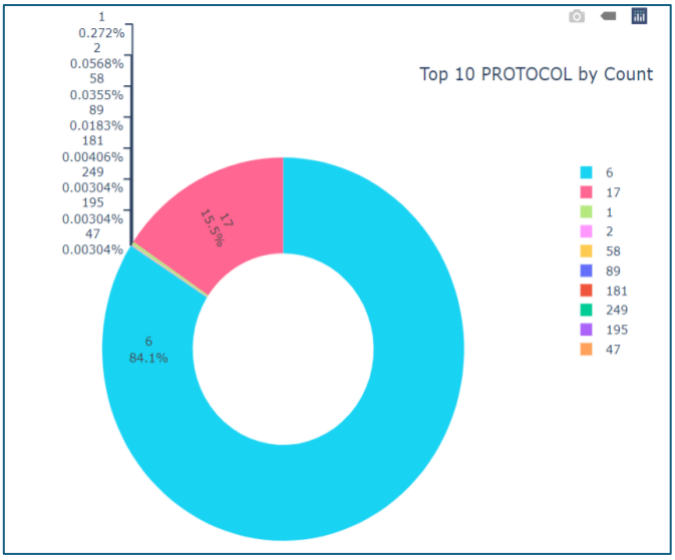

Figure 5: Distribution of Protocol

Figure 5, represents a donut chart which tells the distribution of protocols and the distribution of 6 protocol type is 84.1% and 15.5% are for protocol type 17 and other type of protocols are only in in the 0.2% to 0.006%.

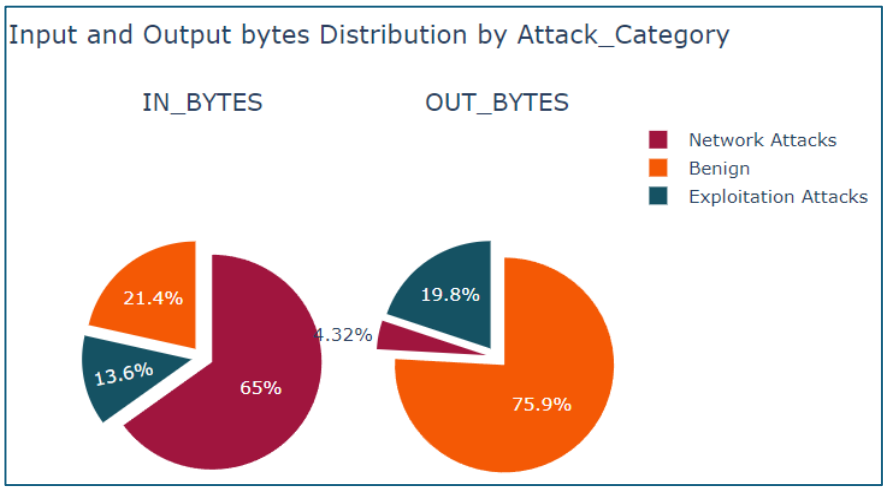

Figure 6: Input and Output bytes Distribution by Attack Category

Figure 6, represents two pie chart which gives the Input bytes by network attacks has the more distribution which is 65% and exploitation attacks with a less input of 13.6%. Talking about the output bytes, benign attack has more distribution with 75.9% and the there is less attack of network attacks.

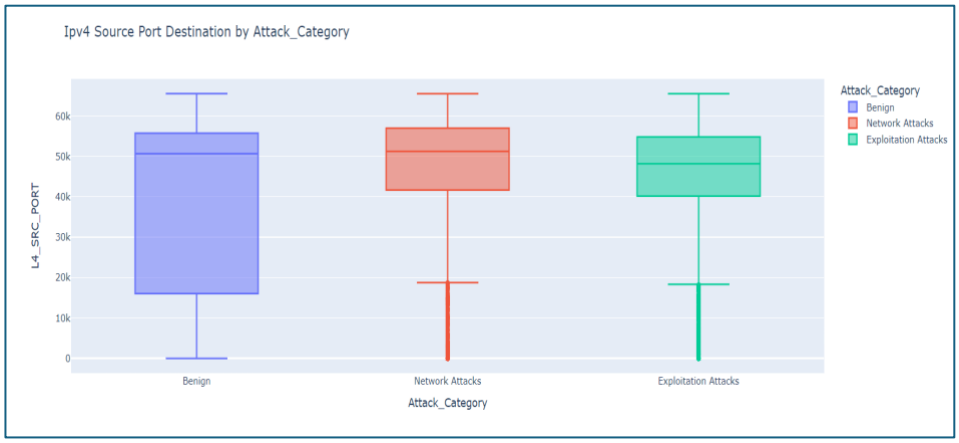

Figure 7: Box plot for IPv4 Source Port Destination by Attacks

Figure 7 shows a box plot with IPv4 source prost destination by attacks which shows the median for benign at 50k, Network attacks at 50k and exploitation attacks at 45k and this port, the network attack and exploitation attack contains a greater number of outliers that should be deleted or removed.

3.4 Feature Engineering

Feature Engineering plays an important role in the research study. Feature engineering consists of selecting the features and transforming the raw data into information which is relevant for machine learning models. With the help of feature engineering the performance of the algorithm such as accuracy can be increased. In this, first the data is label encoded means the categorical features are converted to numerical features, features such as IPV4_SRC_ADDR,

IPV4_DST_ADDR, L4_SRC_PORT, F4_DST_PORT and Attack_Category are label encoded. The target column is dropped from the data.

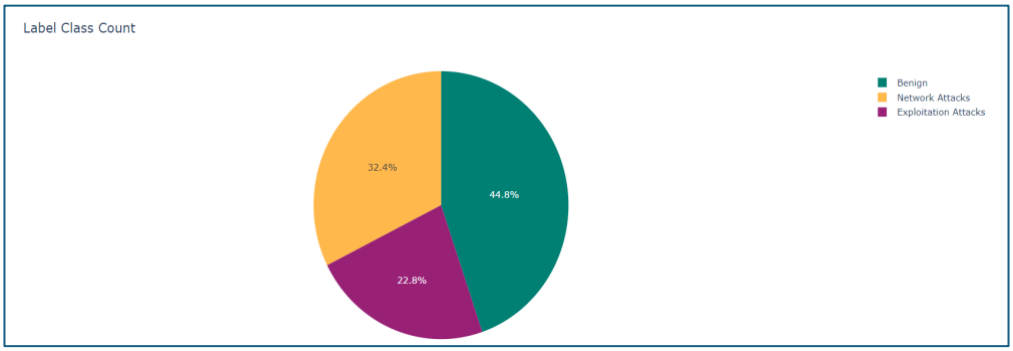

Figure 8: Label Count of each class

Figure 8, represent the distribution of the label count of each class, 44.8% labels are of benign class, 32.4% labels are of network attacks and 22.8% labels are of exploitation attacks class. The data contains a greater number of benign class and a smaller number of normal attack and exploitation attack which represents that data is unbalanced which can produce biased result in prediction. To address this, SMOTE (Synthetic Minority Over-sampling Technique) is applied on the data. SMOTE balances the data by generating synthetic samples of the minority class with the help of oversampling rather than under sampling the majority class. In this research the oversampling is performed on the data to balance it and the after applying SMOTE the dataset become balanced. Figure 9 represents a pie chart which gives distribution of balanced dataset.

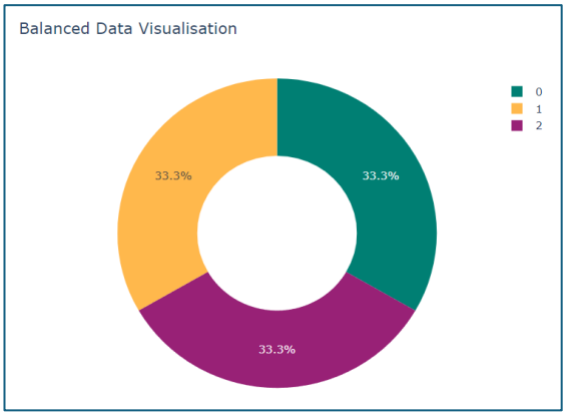

Figure 9: Balanced Data set after applying SMOTE

3.4.1 Feature Extraction

Feature extraction is the process of extracting the relevant features in machine learning. The features which play an important role in the performance of machine learning algorithm are extracted from the dataset. In the proposed method, first the dataset is split into training and testing set with a test size of 20%. For extracting the features, the Random Forest Classifier is

used and the important features are extracted. Figure 10 gives the feature importance and their scores.

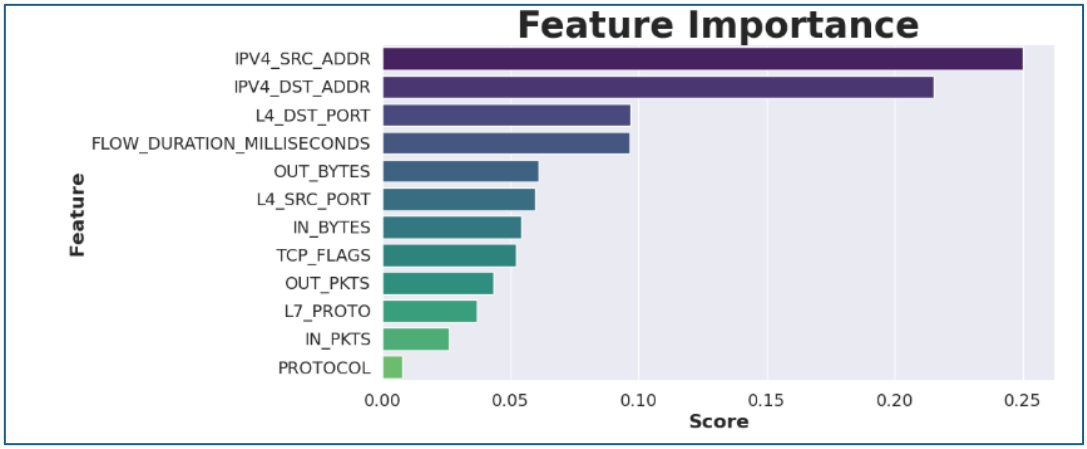

Figure 10: Feature importance with score.

The top 8 features with the highest scores such as IPV4_SRC_ADDR and IPV4_DST_ADDR etc., are selected for the training of algorithm and these features are selected and normalized with the help of MinMaxScaler.

3.5 Model Training

Model training is the very important part in making the predictions. After extracting the relevant features, 8 features are extracted. The features are then normalized with the help of min-max scaler. Then the dataset is split in to training and testing data with a test size of 20%. The training and testing data is reshaped into 2-Dimensional data and the argument max of the data test labels are taken. Three deep learning algorithms are employed on the data for the classification of attacks. The algorithms are: Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM) and Convolutional Long Short-Term Memory (Conv-LSTM). The training data is trained on these algorithms. The CNN model consists of 11 layers with an activation as relu and at output layer the activation function is 'softmax', the LSTM model consists of 9 layers with an activation function of relu and a batch normalization after 1 layer and a dropout of 0.4, 0.3 and 0.3 after third, fifth and seventh layer respectively. Conv-LSTM model contains 15 layers with batch normalization after first layers and with dropout of 0.4 with some layer. After implementing the model on the data, performance of the model is evaluated.

3.6 Model Evaluation

After training the data on algorithm, the last step is to evaluate the performance of the algorithm. Since, it is very important to evaluate the performance of the algorithm to determine how better the algorithm is performing on the data. Four performance metrics are used to evaluate the algorithm's performance. The performance metrics are accuracy (tells proportion of instances that are correctly classified and used when the classes are balanced), precision (tells proportion for positive prediction which are correct), recall (tells proportion of actual positives which are correctly identified and used when the rate of false negative is high), and

f1-score (harmonic mean of precision and recall). These metrics are evaluated by testing the test data on the algorithm and compared with the actual output of the test data. So, with the help of these metrics, it can be said that the algorithm is performing better on not for the intrusion detection.

4 Design Specification

We have already discussed data collection, pre-processing, feature engineering, model training, and model evaluation in the Methodology section. Now let's discuss about the follow-up steps that would be necessary for real-time deployment and operation of our IoT Intrusion Detection System (IDS). Our design begins with a router that manages network traffic between the internal and external network, the router passes the traffic to the firewall for initial security filtering, and the traffic arrives at our Intrusion Detection System (IDS). The IDS has a deep learning model that we have trained to classify the traffic packets into normal or potentially malicious packets. We have integrated this model in our IDS and are capable of classifying packets rates in real-time in the IDS. For real-time packet analysis, we also developed a web application that can detect an attack in real-time and displays alerts to administrators or users. The IDS classifies the network packets and if the IDS detects malicious activity the IDS will trigger an alert and detail the attack for an administrator or user to respond. Normal traffic will be passed by the IDS for the server to continue and provide the service to a legitimate user. The framework in this paper represents how the system would hypothetically operate as an IDS that could be used in real network environments. The aim of this framework is to give insights to the potential deployment and operation of the system as an IDS.

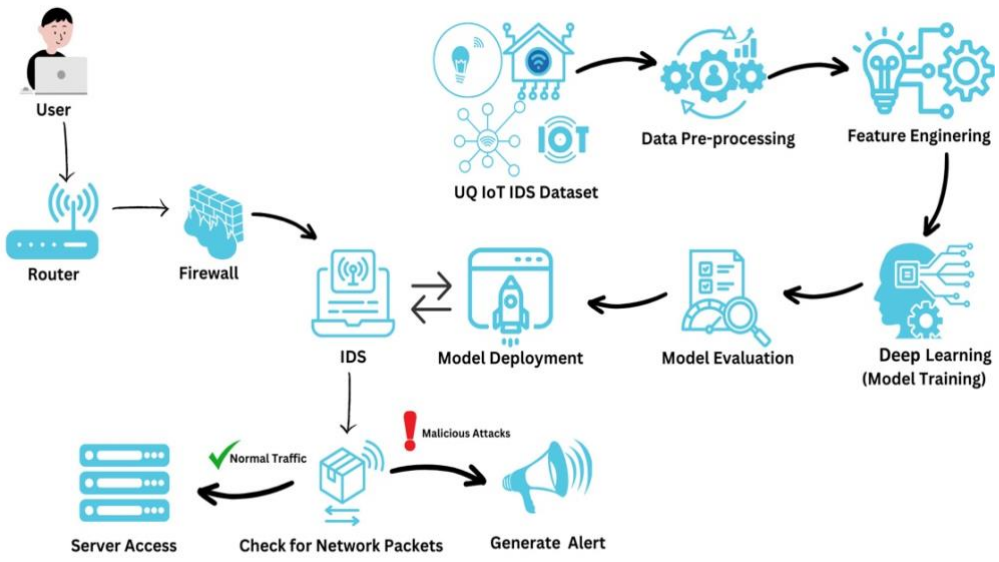

Figure 11: Design Framework for Real-Time Threat Detection and Alert System in Network System

5 Implementation

Our research project was implemented using Python, which is a versatile programming language particularly suited for tasks in data science and machine learning. We used some Python libraries for various stages of the project. NumPy was used for numerical computations so that we could handle large multi-dimensional arrays and perform important mathematical operations. Pandas was another tool we used, it was used for data pre-processing, cleaning, and so that the UQ IoT IDS dataset could be structured into a format that suited analysis better. In order to visualize data trends and how our models were performing, we used Plotly and Matplotlib, Plotly was used for creating interactive plots and Matplotlib was used for static visualizations, typically of a quality suitable for publication. Seaborn was also used to assist with data visualizations and enable us to make complex statistical graphics more informative and aesthetically pleasing. We used Scikit-learn (sklearn) to implement machine learning models, Scikit-learn includes a wide suite of algorithms and model-evaluation metrics, and also includes techniques for model selection and validation. For our deep learning models, the CNN, LSTM and the hybrid Conv-LSTM model, TensorFlow was used. Keras facilitated our model building and training process, by providing a high-level API. For the web application development, we used Flask which is a lightweight Python web framework, to build the backend to allow for real-time attack detection and alerting. The web pages were created using HTML, CSS, and JavaScript so that the web interface was responsive and user-friendly. We used AJAX to allow for a more interactive web page, so that it could work without refreshing completely.

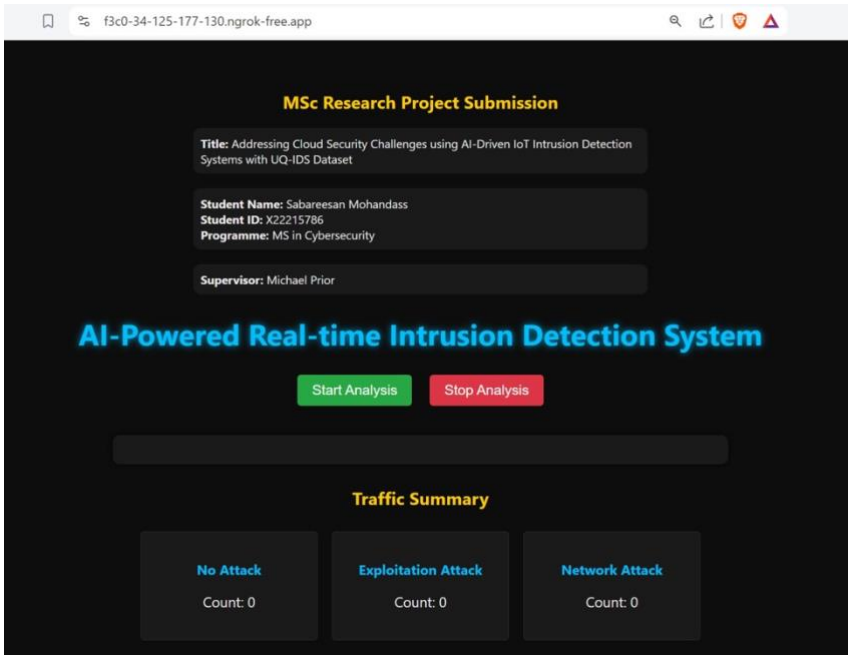

Figure 12: Web Application for Detecting Anomalies in Real time

In order to develop and train our models we used Google Colab which is an online Integrated Development Environment, and was used as it was efficient and provided the computational

resources that we needed. The web application was finally deployed in a cloud environment, as it would make the application scalable, accessible and performant in real-world scenarios. Taking each tool used, and considering the UQ IoT IDS dataset, meant that we could effectively implement and validate our IoT intrusion detection system. The screenshot of our web application is shown in Figure 12 and Figure 13.

Figure 13: Web application detecting anomalies and providing traffic summary

6 Evaluation

The research is carried out by implementing three unique algorithms. Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM) and Convolutional Long Short-Term Memory (Conv-LSTM Model). Since, the research problem is a classification problem with 3 classes as Benign attack, Normal attack, and Exploitation attack. Four key classification performance metrics are use namely – accuracy, precision, recall and F1-score are implemented to study the evaluation of each algorithm. The comparison and evaluation of these metrics are discussed.

6.1 Evaluation Based on Accuracy

Accuracy tells the proportion of instances that are classified correctly out the total instances. It is used when the classes are balanced. The higher the accuracy, the model is said to perform better. In the experiment, the evaluation of each model on the basis of accuracy provides a deeper insight on the performance of the model. The accuracy attained by CNN model is 81.64%, and the accuracy achieved by LSTM is lower that CNN which is 80.62%. However,

the ConvLSTM model attains a superior accuracy of 85.15%, which is better than the other two algorithms. Thus, the CovnLSTM model gives a better performance based on accuracy. This approach leverages the importance of features which is derived from the RandomForest classifier. Figure 14, show a bar char which gives a comparative analysis of the models on the basis of their accuracy.

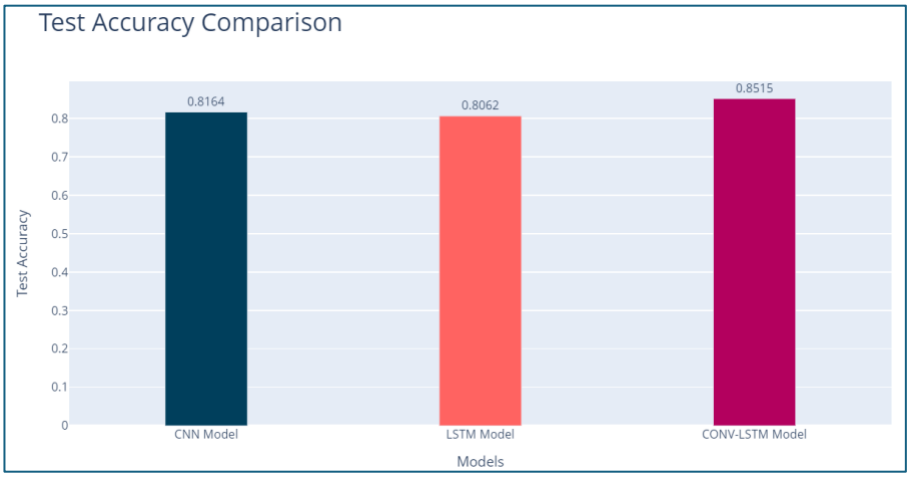

Figure 14: Comparative analysis of models based on accuracy

6.2 Evaluation Based on Precision

Precision tells the proportion of positive prediction which are actually correct and it is used when the rate of false positive is high. In the experiment the CNN model gives a precision of 83.62% which is slightly higher than the precision given by LSTM model which is 81.8%. The high precision attained by the ConvLSTM which is 86.89%, outperforming than other two algorithms. The ConvLSTM algorithm gives the superior performance based on the precision for positive predictions. Figure 15 represents a line chart which gives a comparative analysis for the algorithms on the basis of precision.

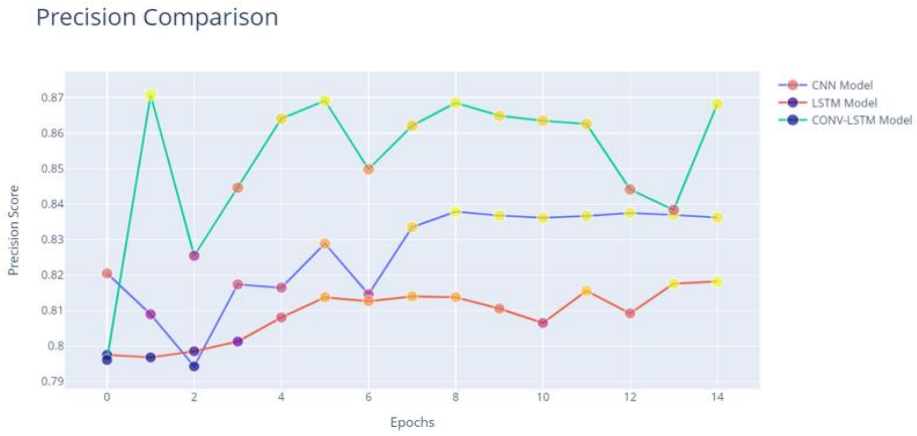

Figure 15: Comparative analysis of models based on precision

6.3 Evaluation Based on Recall

Recall or Sensitivity or True Positive Rate tells the proportion of actual positive that are identified correctly and recall is used when the rate of false positive is high. In the experiment, the recall metric is used to get the insights of the models' ability to get the instance which are positive. CNN model exhibits a recall of 83.39%, telling the effectiveness of true positives. LSTM model gives a recall of 80.69% which is less than CNN model. ConvLSTM model gives a recall of 86.76%, outperforming better than two algorithms. The high recall performance of the ConvLSTM models says that it is more efficient to capture the true positive instances, which makes it more reliable model in this approach for identifying the positive cases which is very crucial. Figure 16, shows a line chart which gives the comparison of recall for the three algorithms.

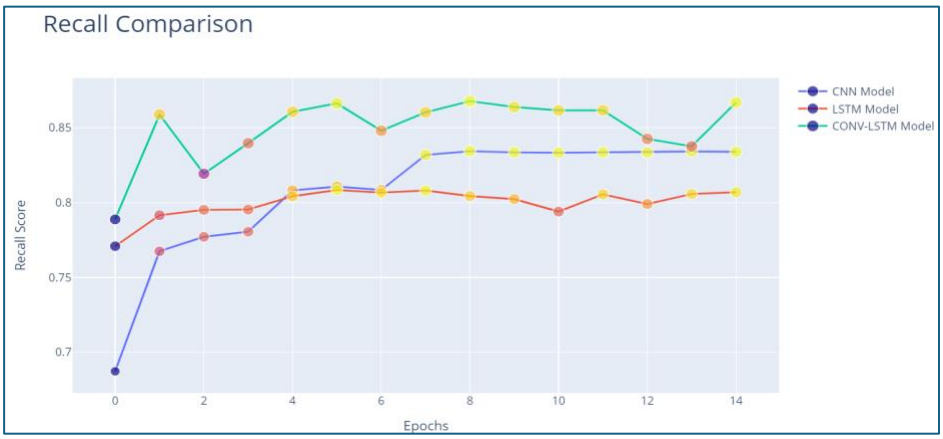

Figure 16: Comparison of recall for the algorithms

6.4 Evaluation Based on F1-Score

In this experiment, the F1-score, tells the harmonic mean of precision or recall which gives a single metric that balances both measures. The study is focusing on selection features which are important for evaluation and model training. The CNN model attains an F1-score of 77.86%, which tell that a balanced performance between recall and precision. The f1-score of CNN model is higher than LSTM model with an F1-Score of 74.46% which demonstrates that CNN model is better for balancing recall and precision. The ConvLSTM model outperforms both, having a high F1-Score of 81.73%. This performance of ConvLSTM tell an effectiveness in maintaining a high balance between precision and recall, which make it reliable among the three algorithms. Figure 17 represents a bar chart for the comparative analysis of F1-score for the algorithms, which illustrates the differences in the performance of the f1-score and highlight the performance of ConvLSTM model's ability to maintain the trade-off between precision and recall.

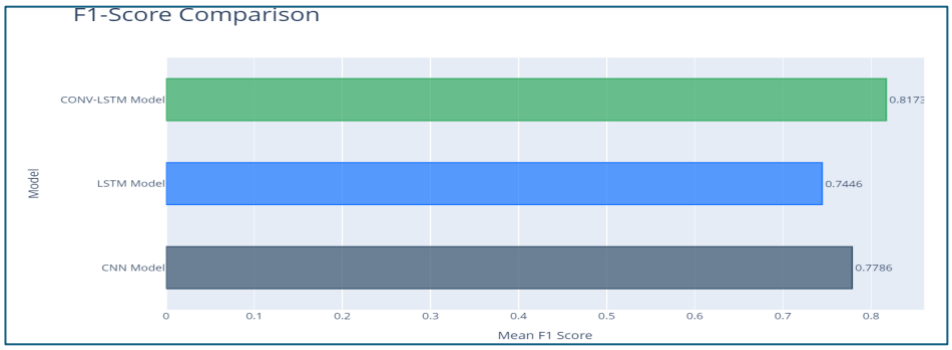

Figure 17: Comparison of F1-Score for the algorithms

6.5 Discussion

In the research, three unique algorithms for the intrusion detection system have been implemented which detects the 3 major classes benign attack, normal attack and exploitation attack. The three algorithms are Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM) and Convolution Long Short-Term Memory for classification of the attacks. The algorithms then evaluate with four key performance metrics: accuracy, precision, recall, and F1-score which provides a comprehensive comparison of the performance of the models. Among the algorithms which are trained on the UQ-IDS data, Conv-LSTM model outperformed better than CNN and LSTM which an accuracy of approximately 86% and other performance metrics such as precision, recall, and f1-score with a value of approximately 85.15% each respectively. This superior performance of Conv-LSTM can be attributed to the advanced architectural design by combining the power of convolutional layers and LSTM units which provides the model to capture spatial and temporal dependencies in the data effectively which leads to increase the capability to solve the classification problem. Other algorithms such as CNN and LSTM attains the accuracy of 81.64% and 80.62% respectively which is marginally lower than CNN. The result of this study by leveraging the importance of features which were selected for training the model says that Conv-LSTM is a reliable choice for solving this classification problem which represents the importance to consider the hybrid models for such classification task which are complex, and it also can improve the performance over traditional approaches.

7 Conclusion and Future Work

We have developed a novel hybrid Conv-LSTM model to address some of the existing challenges in IDSs, which enhance the detection of complex and novel cyberattacks, particularly in IoT and cloud computing environments. Our model brings together the strengths of Convolutional Neural Networks (CNN) with the advantages of Long Short-Term Memory (LSTM) networks. Our experimental evaluations revealed that the Conv-LSTM model outperforms CNN and LSTM, showing significantly higher accuracy, precision, recall, and F1-score, as above. Our performance evaluation results show that the combined Conv-LSTM model is a clear advancement over using CNN or LSTM alone in cyberattack detection. We have deployed this model in a real-time web application that not only provided similar

detection results, but also produced a user-friendly interface with instant alerts for administrators. The demonstration of effectiveness using a cloud-based platform confirms the scalability of the model and its practicality in securing modern networks. Our research remains a meaningful advance for the field of cybersecurity.

From here, there are several promising directions for future work. The hybrid model could be optimized further for efficiency and for handling large-scale, real-time data streams. One area to extend is to incorporate online learning techniques to ensure continual adjustment to new cyber threats and adaptability of the model. An additional extension incorporating new features into the web application, such as integrating advanced visualization tools or adding automated response mechanisms, could provide meaningful improvements. Finally, broad performance evaluations in various real-world environments and IoT platforms would provide more evidence on the suitability of the model under differing deployments, which will facilitate broader use and possibly even more advances in cybersecurity defences.

References

Al-Ghuwairi, A. R., Sharrab, Y., Al-Fraihat, D., AlElaimat, M., Alsarhan, A., & Algarni, A. (2023). Intrusion detection in cloud computing based on time series anomalies utilizing machine learning. Journal of Cloud Computing, 12(1), 1–17. https://doi.org/10.1186/S13677-023-00491-X/TABLES/3

Archana, C., Chaitra, H. P., Khushi, M., Pradhiksha Nandini, T., Sivaraman, E., & Honnavalli, P. (2021). Cloud-based network Intrusion detection system using deep learning. ACM International Conference Proceeding Series. https://doi.org/10.1145/3485557.3485562

Attou, H., Guezzaz, A., Benkirane, S., Azrour, M., & Farhaoui, Y. (2023). Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques. Big Data Mining and Analytics, 6(3), 311–320. https://doi.org/10.26599/BDMA.2022.9020038

Attou, H., Mohy-eddine, M., Guezzaz, A., Benkirane, S., Azrour, M., Alabdultif, A., & Almusallam, N. (2023). Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing. Applied Sciences 2023, Vol. 13, Page 9588, 13(17), 9588. https://doi.org/10.3390/APP13179588

Bakro, M., Kumar, R. R., Alabrah, A. A., Ashraf, Z., Bisoy, S. K., Parveen, N., Khawatmi, S., & Abdelsalam, A. (2023). Efficient Intrusion Detection System in the Cloud Using Fusion Feature Selection Approaches and an Ensemble Classifier. Electronics 2023, Vol. 12, Page 2427, 12(11), 2427. https://doi.org/10.3390/ELECTRONICS12112427

Bharati, M. P., & Tamane, S. (2020). NIDS-Network Intrusion Detection System Based on Deep and Machine Learning Frameworks with CICIDS2018 using Cloud Computing. Proceedings of the 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing, ICSIDEMPC 2020, 27–30. https://doi.org/10.1109/ICSIDEMPC49020.2020.9299584

Douiba, M., Benkirane, S., Guezzaz, A., & Azrour, M. (2023). Anomaly detection model based on gradient boosting and decision tree for IoT environments security. Journal of Reliable Intelligent Environments, 9(4), 421–432. https://doi.org/10.1007/S40860-022-00184-3

Guezzaz, A., Benkirane, S., & Azrour, M. (2022). A Novel Anomaly Network Intrusion Detection System for Internet of Things Security. EAI/Springer Innovations in Communication and Computing, 129–138. https://doi.org/10.1007/978-3-030-90083-0_10

Kayode Saheed, Y., Idris Abiodun, A., Misra, S., Kristiansen Holone, M., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal, 61(12), 9395–9409. https://doi.org/10.1016/J.AEJ.2022.02.063

Lata, S., & Singh, D. (2022). Intrusion detection system in cloud environment: Literature survey & future research directions. International Journal of Information Management Data Insights, 2(2), 100134. https://doi.org/10.1016/J.JJIMEI.2022.100134

Layeghy, S., Gallagher, M., & Portmann, M. (2024). Benchmarking the benchmark — Comparing synthetic and real-world Network IDS datasets. Journal of Information Security and Applications, 80, 103689. https://doi.org/10.1016/J.JISA.2023.103689

Long, Z., Yan, H., Shen, G., Zhang, X., He, H., & Cheng, L. (2024). A Transformer-based network intrusion detection approach for cloud security. Journal of Cloud Computing, 13(1), 1–11. https://doi.org/10.1186/S13677-023-00574-9/TABLES/4

Nizamudeen, S. M. T. (2023). Intelligent intrusion detection framework for multi-clouds – IoT environment using swarm-based deep learning classifier. Journal of Cloud Computing, 12(1), 1–14. https://doi.org/10.1186/S13677-023-00509-4/FIGURES/6

Olabanji, S. O., Marquis, Y., Adigwe, C. S., Ajayi, S. A., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection. SSRN Electronic Journal. https://doi.org/10.2139/SSRN.4709384

Sarhan, M. & Layeghy, S. (2023). NF-UQ-NIDS. The University of Queensland. Available at: https://espace.library.uq.edu.au/view/UQ:69b5a53

Talukder, M. A., Islam, M. M., Uddin, M. A., Hasan, K. F., Sharmin, S., Alyami, S. A., & Moni, M. A. (2024). Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. http://arxiv.org/abs/2401.12262

Tatineni, S. (2023). AI-Infused Threat Detection and Incident Response in Cloud Security. International Journal of Science and Research (IJSR), 12(11), 998–1004. https://doi.org/10.21275/SR231113063646

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25–37. https://doi.org/10.1016/j.jnca.2017.02.009