International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 16, No.1 (Aug-24)

https://dx.doi.org/10.12785/ijcds/160148

Machine Learning-Based Security Mechanism to Detect and Prevent Cyber-Attack in IoT Networks

Abdullah Alomiri[1], Shailendra Mishra[2] and Mohammed AlShehri[3]

[1,2,3]*Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Majmaah, Saudi Arabia*

Received 28 Apr. 2023, Revised 3 Apr. 2024, Accepted 27 Apr. 2024, Published 1 Aug. 2024

Abstract: The increasing prevalence of Internet of Things (IoT) systems has brought about significant security concerns. Cyber-attacks, including denial-of-service attacks, malware infections, and phishing attempts, pose serious threats to the integrity and functionality of IoT networks. To ensure comprehensive protection, it is essential to develop machine learning-based security measures that employ robust models and integrate multiple security mechanisms. In this study, a Ridge Classifier is utilized as a powerful model to detect anomalies in IoT systems. By leveraging this approach, the proposed security system can accurately identify and predict cyber-attacks in real-time, utilizing secure and up-to-date information from the network. The integration of machine learning techniques enhances the system's ability to detect and mitigate threats effectively. Experimental results demonstrate the high accuracy of the proposed system in detecting and mitigating network threats in IoT systems, achieving a remarkable accuracy rate of 97 percent. This level of accuracy not only improves the security and resilience of government and business networks but also ensures the protection of valuable data from malicious threats. The development of machine learning-based security measures, such as the system presented in this study, is crucial for addressing the security challenges faced by IoT systems. By accurately detecting and predicting cyber-attacks, these measures play a pivotal role in safeguarding the integrity, confidentiality, and availability of IoT networks. Furthermore, the integration of robust models and the incorporation of multiple security measures provide a comprehensive defense against a wide range of threats. In conclusion, the implementation of machine learning-based security measures, particularly utilizing the Ridge Classifier model, offers significant benefits in protecting IoT systems. By effectively detecting and mitigating network threats with high accuracy, these measures contribute to improving the security and resilience of government and business networks. Moreover, the protection of data from malicious threats ensures the integrity and confidentiality of IoT systems, fostering trust and reliability in the rapidly expanding IoT landscape.

Keywords: Cyber Attacks, Network Threats, Network Security, Security Countermeasure.

I. Introduction

The growth of the Internet of Things (IoT) has brought significant changes in the way devices interact and communicate with each other, enabling the development of smart homes, cities, and industries. However, as the number of connected devices increases, the risk of network threats also grows, and traditional security measures may not be sufficient to protect IoT devices. To address these security challenges, machine learning (ML) has emerged as a promising solution. Today, digital transformation is moving fast to digitize our lives to make it easy and available anytime from everywhere. Technology made our lives easy with our families and businesses, everything can be published easily on the internet, and everyone can reach it from anywhere, that's contributed to an increase in the electronic services that serve clients, businesses, socials, and more. Computer networks are the main gate to connect systems, services, and people from anywhere together with less than a second, services can be integrated for better services for the end user experience [1]. Due to the criticality of electronic services today and how it's impacted human life. Cybercriminals take advantage of the importance of electric services today to impact people's lives and try to steal or damage computer networks, web services, and applications that are published on the internet for their intentions. Cybercriminals are individuals or groups of people with different levels of expertise who try to hack or gain unauthorized access to protected networks [2]. This study discusses the recent development of cyber-attacks on network levels and the most important cyber security controls that detect and prevent cyber-attacks. In addition, recent cyber-attacks happened and impacted the targeted victims.

A. Background

IoT refers to a network of interconnected devices, sensors, and software that facilitate communication between

E-mail address: 431104745@s.mu.edu.sa, s.mishra@mu.edu.sa, ma.alshehri@mu.edu.sa

physical objects and digital systems. The widespread adoption of IoT is due to its potential to create smart homes, cities, and industries. However, the increasing number of connected devices also raises concerns about the security of these networks. IoT networks are vulnerable to various network threats, including malware, ransomware, and DDoS attacks. Traditional security measures, such as firewalls and encryption, are no longer sufficient to protect IoT devices from these evolving threats. Hence, there is a need for more advanced security measures to safeguard IoT networks [3]. Machine learning has become an important solution to address the security challenges in IoT networks. ML is a subset of artificial intelligence (AI) that involves training machines to learn from data without explicit programming. ML techniques can detect anomalies, identify patterns, and predict potential security threats in IoT networks. By analyzing large amounts of data from various sources, including network traffic, sensor data, and user behavior, ML algorithms can detect suspicious activity and prevent security breaches. The background section aims to provide a comprehensive overview of the development of network threats and security measures in IoT using ML. The section starts by discussing the rapid growth of IoT networks and the associated security challenges. It then examines the various types of network threats and the shortcomings of conventional security measures. Finally, the section highlights the potential of ML techniques in addressing the security challenges in IoT networks. Network attacks are the gateway to gain inside the corporate networks and protecting the boundary of the networks with advanced network countermeasures is mandatory to keep the network secure from external threats. Threat actors are trying to find a vulnerable service or public facing machine to send their malicious and exploit the vulnerability of the system. Services and computer systems are expositions to new threats that are known and unknown by the development team. Building a comprehensive network security measure against different types of attacks will prevent and protect even the vulnerable system from threats and reduce the associated risk. Cyber defense controls can in preventive, corrective, or detective controls, and all of them are used to achieve a high level of security posture. External threat actors can launch an easy attack and cause a huge impact such as a denial of services (DDoS) attack and that's one the hardest attacks to prevent as it targets stateful devices such as network firewalls, load blancher, applications, and so on [4]. In cyberspace, security controls must be aligned with the recent cyber threats and attacks to have the capability of detecting known and unknown attacks. Implementing integrated cyber security controls that will contribute to fully synchronized cyber defense solutions. Protecting the networks can detect outbound threats or internal threats such as infiltrating sensitive data outside the organization. Placing the security controls must cover whole the traffic whether north south or east west flow. Today, visibility to the threats is part of the detection, most of the attacks are encrypted traffic, and applying decryption controls is a prerequisite to give the chance for the security controls to inspect the packets that travel in the network. The growth of IoT networks has been exponential in recent years. IoT networks have the potential to create new business models and improve efficiency in various industries [5]. However, the increasing number of connected devices also raises concerns about the security of these networks. IoT devices are vulnerable to various network threats, including malware, ransomware, and DDoS attacks. The increase in the number of IoT devices has also led to the development of new types of network threats. Malware is a common type of network threat that can infect IoT devices and cause damage to their functionality. Malware can be spread through email, social media, or even through the download of malicious applications. Once an IoT device is infected with malware, the attacker can gain unauthorized access to the device's data, or even control the device remotely [6]. Ransomware is another significant network threat in IoT networks. Ransomware attacks on IoT devices can cause significant disruptions to businesses and individuals, leading to data loss, system downtime, and financial loss. DDoS attacks are another significant threat to IoT networks. DDoS attacks involve overwhelming a target network or device with a large volume of traffic, causing it to crash or become unresponsive. DDoS attacks on IoT devices can be particularly damaging, as they can disrupt critical infrastructure, including healthcare systems, transportation systems, and industrial control systems. The purpose of this study is to investigate network threats and security measures in IoT using machine learning. The study aims to identify different types of network threats that can affect IoT systems and evaluate the effectiveness of machine learning-based security measures in detecting and mitigating these threats. The study also aims to provide recommendations for improving machine learning-based security measures in IoT systems, which is crucial as these systems become more prevalent and crucial to various industries. The main contribution of this research is to develop effective machine learning-based security measures for the Internet of Things (IoT) environment, intending to mitigate network threats and improve overall network security. Specifically, the research aims to:

- Investigate the current state of network threats and security measures in the IoT environment and identify potential gaps and limitations in existing approaches.
- Explore the potential applications of machine learning algorithms in IoT security and evaluate their effectiveness in detecting and responding to network threats.

- Develop novel machine learning-based techniques for identifying and mitigating network threats in the IoT environment and evaluate their effectiveness in real-world scenarios.
- Investigate the impact of machine learning-based security measures on the overall security and performance of IoT networks and develop strategies for optimizing these measures for maximum effectiveness.

Provide recommendations for the design and implementation of machine learning-based security measures in IoT environments, to improve network security and reduce the risks associated with network threats. To accomplish the paper's objectives, the paper is divided into six sections. Section 1 provides an introduction to the research topic, Section 2 provides a literature review that explores the different types of network threats, traditional security measures, and the potential of machine learning in addressing security challenges in IoT networks. Section 3 explains the research methodology and the data collection process. Section 4 presents the data analysis and the findings of the study, including the performance evaluation of the machine learning algorithms for detecting network threats in IoT networks. Section 5 offers a discussion of the results, implications, and limitations of the study. Finally, Section 6 provides the conclusion, recommendations, and future research directions based on the findings of the study.

B. Problem Evolution

The development of network threats in IoT has evolved over time, driven by the increasing number of connected devices and the sophistication of attackers. Initially, network threats in IoT were limited to simple attacks such as port scanning and eavesdropping. However, as the number of IoT devices increased, attackers began developing more sophisticated attacks such as malware, ransomware, and DDoS attacks [9].

Malware is a type of network threat that can infect IoT devices and cause damage to their functionality. Malware attacks on IoT devices can result in data theft, financial loss, and privacy breaches. Ransomware attacks have become more prevalent in recent years, encrypting data on IoT devices and demanding payment for its release. In addition, botnets and DDoS attacks have become significant threats in IoT, with attackers using IoT devices to launch attacks on other networks.

Traditional security measures such as firewalls and antivirus software have limited effectiveness in protecting IoT devices from these sophisticated attacks. These measures are often designed to protect traditional computing devices such as laptops and desktops and may not be suitable for IoT devices. In addition, IoT devices are often designed with low computational power, limiting their ability to handle complex security tasks.

II. LITERATURE REVIEWS

Many researchers took the chance and broke down the experience of network threats and vulnerabilities with extensive studies and experiments. The most important thing that we know is no one technology can prevent all the threats, or one control can reduce the risk. All is about implementing the policies, procedures, and processes, with proper implementation. The authors highlight the limitations of traditional signature-based and rule-based methods in detecting unknown or sophisticated attacks in IoT systems. The proposed approach consists of four different deep learning models, namely CNN, LSTM, Autoencoder, and Denoising Autoencoder [7]. In addition, modeling a potential cyber-attack can save time, money, and other resources for an organization. By employing cyber-attack modeling techniques, organizations can better understand potential cyber-attacks and implement measures to mitigate them, thereby safeguarding their network and data [8]. Therefore, it is essential to develop a comprehensive understanding of cyber threats and devise effective strategies to protect against them. The cyber security controls are primarily designed to detect and protect assets based on signature-based approaches that identify previously known attacks that have occurred in different organizations and were identified by security researchers. In [9] "Defending against insider threats with network security's eighth layer," he points out that the threat landscape associated with insider threats can be broadly classified into two categories. The first category includes people within the organization who aim to attack it for unlawful purposes. These individuals are typically dissatisfied employees who attempt to cause harm or steal sensitive data. The second category includes untrained employees who are susceptible to cyber threats, and this type of employee can be found in almost every organization. Therefore, it is crucial to implement effective security measures to address both types of insider threats and protect organizational assets from potential harm. Both two types of insider threats are internal risks for each organization, unhappy workers are very difficult to detect and know their intentions and some of them have a high privilege of access to the critical systems which is a very high risk to the organization and they should build a strong polices to maintain and monitor the activity of these users. The second part is the employee with a low level of awareness of cyber threats and attacks, they are usually targeted by social engineering or any type of phishing attack. According to the European Union Agency for Cybersecurity Threat Landscape report in 2022, 60 percent of organizations affected by Ransomware may have paid

ransom demands, and the largest Denial of Service (DDoS) attack ever was launched in Europe in July 2022 [10]. Furthermore, Akami's DDoS protection provider was announced by author Craig Sparling.The largest DDoS attack launched against a European customer against Prolexic's platform was discovered and stopped by Akamai, with attack traffic peaking at 853.7 Gbps and 659.6 Mpps over 14 hours. In terms of the number of IP addresses targeted, it was the most significant worldwide horizontal attack mitigated on Prolexic's platform. The author provides an overall summary of the attack and how the bad actor leveraged a highly sophisticated DDoS attack. Critical infrastructure is susceptible to sophisticated and highly targeted cyber attacks, usually targeted on different levels such as the availability of the service or breaching the networks and the security systems. In addition, the Cyber security team should perform external testing against the exposed service from different types of attacks such as DDoS, phishing, web service testing, and more. The concern is to put the security perimeter to the real test and be ready for such attacks. While rule-based detection engines are a strong foundation for security businesses, cyber threat hunting is a crucial skill to have to detect undisclosed advanced threats. In contrast to rule-based detection approaches, hunting identifies and investigates risks proactively [11]. Cyber threat hunting is a proactive eye into the entire network to keep focused on the networks and endpoint to hunt malicious, suspicious, or any risky activity that has detection by existing tools. A network Intrusion Detection system is one of the important security controls that can detect and sniff the traffic to perform signature-based analysis and capture malicious traffic [12]. In [13], authors suggested an approach to incorporate spatial and temporal learning via public datasets NSL-KDD and UNSW-NB15 for training and testing. With a low False Positive Rate and a high detection rate, the proposed model combines the advantages of a Convolutional Neural Network with that of a Bi-directional LSTM. Meanwhile, the Network Intrusion Prevention system is an inline security control that is designed to detect and prevent network threats. An IDS only needs a limited amount of data to detect an attack quickly. Feature selection is essential for selecting the most accurate features. Using UNSW-NB15 and CICDoS2019 attack datasets, the authors of the paper [14] propose an ensemble classifier-based wrapper-based approach to feature selection. IGRF-RFE is a hybrid method for selecting features for network anomalies in multi-class networks, based on IG and random forest (RF). MLP's multi-classification accuracy has increased from 82.25 percent to 84.24 percent because of IGRF-RFE, which reduced the number of features from 42 to 23 [15]. Overall, both NIDS and NIPS are detective and preventive security measures that work on signature-based to predefined security attacks that are known previously.

A. Research Gap

Despite the many recent developments in network security measures, there are still significant gaps in research that need to be addressed. Here are some potential research gaps:

- Developing effective security measures for IoT devices: As the number of IoT devices continues to increase, it is becoming increasingly important to develop effective security measures for these devices.
- Improving threat intelligence: Threat intelligence is critical to identifying potential threats and mitigating risks. However, there is still a need to improve the accuracy and effectiveness of threat intelligence.
- Enhancing cloud-based security measures: Cloud-based threats are becoming more common, and there is a need to enhance security measures for cloud-based infrastructure and applications.
- Addressing the human factor: Insider threats continue to pose a significant risk to network security, and there is a need to address the human factor in network security.
- Developing new approaches to network security: As network threats continue to evolve, there is a need to develop new approaches to network security that can effectively detect and respond to these threats.

Recent developments in network threats and security measures have highlighted the need for ongoing research to address potential gaps in network security. By identifying these gaps and developing new solutions, it is possible to improve network security and mitigate the risks associated with network threats. This paper uses Developing effective security measures for IoT devices using ML. The rapid growth of the Internet of Things (IoT) has created a wide range of new vulnerabilities and attack vectors in network security. IoT devices often lack proper security mechanisms, and many are deployed in critical infrastructure environments, making them an attractive target for cybercriminals. As a result, it is crucial to develop effective security measures for IoT devices to mitigate the risks associated with network threats. One potential solution to this problem is to use machine learning (ML) algorithms to detect and respond to security threats in real-time. ML algorithms can analyze large amounts of data from IoT devices to identify patterns and anomalies that may indicate a potential security threat. Once a threat is detected, the ML algorithm can take appropriate action to mitigate the risk, such as blocking network traffic or alerting security personnel. ML algorithms can also be used to develop predictive models that can anticipate potential security threats before they occur. By analyzing historical data on network activity and security incidents, ML algorithms can identify patterns

and trends that may indicate a future security threat. This information can then be used to develop proactive security measures that can prevent or mitigate the risk of a security breach. Another potential use of ML in IoT security is to improve authentication and access control mechanisms. ML algorithms can be used to analyze user behavior and identify patterns that may indicate unauthorized access or suspicious activity. This information can then be used to enhance authentication and access control mechanisms to prevent unauthorized access to IoT devices and networks. However, several challenges must be addressed when using ML in IoT security. For example, ML algorithms require large amounts of data to train effectively, and many IoT devices may not have the processing power or storage capacity to support these algorithms. Additionally, ML algorithms may produce false positives or false negatives, which can create additional security risks if not properly addressed. IoT devices using ML is a promising approach to mitigating the risks associated with network threats. By leveraging the power of ML algorithms, it is possible to detect and respond to security threats in real-time, develop proactive security measures, and improve authentication and access control mechanisms. However, further research is needed to address the challenges associated with implementing ML in IoT security and to develop effective solutions that can be deployed at scale. One possible research gap related to the UNSW-NB15 dataset and the development of network threats and security measures in IoT using ML is the lack of research on the effectiveness of different ML algorithms for detecting network threats and anomalies in IoT traffic. While some studies have used the UNSW-NB15 dataset to develop and evaluate machine learning models for network intrusion detection and anomaly detection, there is still a need for further research to compare the effectiveness of different ML algorithms for this task. Another research gap could be the lack of research on the generalizability of ML models developed using the UNSW-NB15 dataset to different IoT environments and scenarios. As IoT devices and networks can vary in terms of their characteristics, it is important to determine whether ML models developed using the UNSW-NB15 dataset can be effectively applied to different IoT environments and scenarios.

B. Research Objectives

The objective of this research is to develop effective machine learning-based security measures for the Internet of Things (IoT) environment, with the aim of mitigating network threats and improving overall network security. Specifically, the research aims to:

- Investigate the current state of network threats and security measures in the IoT environment and identify potential gaps and limitations in existing approaches.
- Explore the potential applications of machine learning algorithms in IoT security and evaluate their effectiveness in detecting and responding to network threats.
- Develop novel machine learning-based techniques for identifying and mitigating network threats in the IoT environment and evaluate their effectiveness in real-world scenarios.
- Investigate the impact of machine learning-based security measures on the overall security and performance of IoT networks, and develop strategies for optimizing these measures for maximum effectiveness.
- Provide recommendations for the design and implementation of machine learning-based security measures in IoT environments, with the aim of improving network security and reducing the risks associated with network threats.

III. Proposed Framework

This study will employ a mixed-methods research design, including both qualitative and quantitative data collection and analysis. Data will be collected from various sources, including research papers, reports, and publicly available datasets, and will include network traffic data, expert opinions, and user experiences with machine learning-based security solutions. The data will be analyzed using both qualitative and quantitative methods, such as content analysis, statistical analysis, and machine learning algorithms, to identify patterns, trends, and correlations in the data.

A. Framework components

1) Dataset (UNSW-NB15): A collection of data that serves as the basis for analysis and modeling.
2) Tool (Jupyter Notebook and Python): Software used to perform data manipulation, analysis, and modeling tasks.
3) Data Preprocessing: The process of cleaning and transforming raw data to make it suitable for analysis.

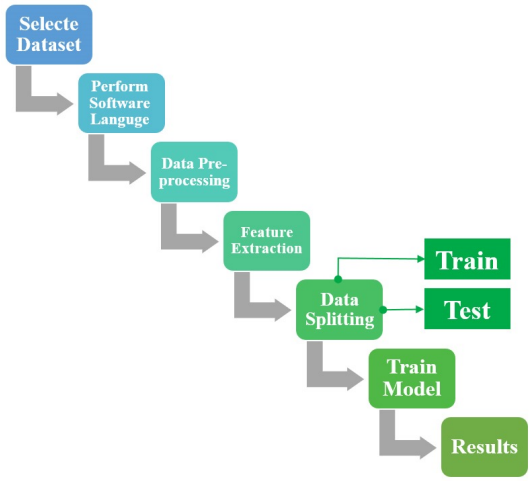

Figure 1. Research Framework

4) Feature Extraction: The process of selecting relevant features from the dataset to use in the model.

5) Data Splitting (Test and Train): The division of the dataset into two subsets (test and train) to evaluate the performance of the model.

6) Train Model: The process of training a machine learning model on the training data to learn patterns and make predictions.

7) Output: The result of running the trained model on the test data.

8) Visualization: Matplotlib to visualize the results of the analysis.

B. System Design

The system design for developing network threats and security measures in IoT using ML is shown in Fig 2.

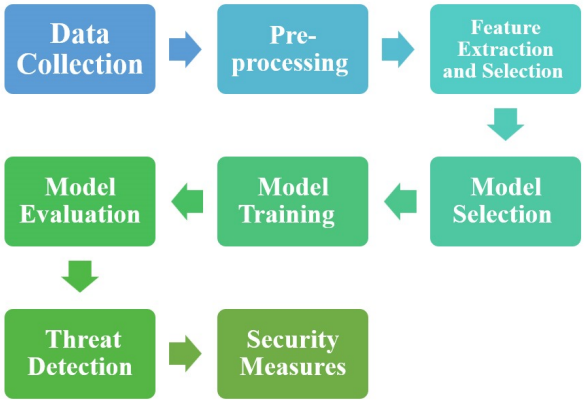

Figure 2. System design

In the following discussion, each step will be discussed in detail:

1) Data Collection: Data is collected from various sources, including IoT devices, network logs, sensor data, and other relevant sources. This data provides information about network behavior, device activity, and potential threats.

2) Preprocessing: The collected data is preprocessed to clean and transform it into a suitable format for further analysis. This may involve removing noise, handling missing values, normalizing data, and performing other necessary data preparation steps.

3) Feature Extraction and Selection: Relevant features are extracted from the preprocessed data. These features capture important characteristics and patterns related to network threats. Feature selection techniques are then applied to choose the most informative and discriminative features.

4) Model Selection: Different machine learning models are evaluated and compared to select the most appropriate model for threat detection. This may include supervised learning algorithms like decision trees, random forests, or neural networks, as well as unsupervised learning methods like clustering or anomaly detection.

5) Model Training: The selected machine learning model is trained using a labeled dataset. The dataset consists of labeled instances, indicating whether they represent normal behavior or potential threats. The model learns from this data to identify patterns and make predictions.

6) Model Evaluation: The trained model is evaluated using a separate validation dataset. Performance metrics such as accuracy, precision, recall, and F1-score are calculated to assess the model's effectiveness in detecting threats.

7) Threat Detection: The trained model is deployed to detect potential threats in real-time or near real-time. It analyzes incoming data from IoT devices and network logs, comparing it to learned patterns and identifying any suspicious or malicious activities.

8) Security Measures: Upon detecting a threat, appropriate security measures are implemented to mitigate the risk. This may involve activating intrusion detection systems, isolating affected devices or networks, blocking malicious traffic, or triggering alerts for further investigation.

IV. Experimental Setup and Implementation

For this research, utilized various tools and technologies to build our system. We primarily used Python, which is a major programming language, in its 64-bit version 3.6. We employed Python for the majority of our data extraction, preprocessing, and preparation tasks required to compile our import data. Additionally, we used Python for visualization tasks, such as constructing graphs, for which we used the Matplotlib library. Python and Jupyter are popular tools for machine learning and data analysis, and they can be utilized in the Development of Network Threats and Security Measures in IoT using ML. In addition, several technologies can be employed to facilitate the implementation of ML algorithms in the IoT network environment. This article will discuss some of the relevant tools and technologies that can be used in this domain.

A. Experiment analysis

1) Dataset
The study used the UNSW-NB15 (ADFA, 2015) dataset, which is a collection of network traffic data in the form of a network packet capture (pcap) CSV file. The dataset is categorized as normal or attack-oriented, with separate categories for routine activity and harmful assaults. It consists of 257,673 records, each with 49 attributes and a class label, including nine categories of traffic, numerous attacks, and a broad range of genuine normal activities. However, in this research, we focused only on the binary classification of the dataset. The dataset includes 45 attributes that assist in accurately categorizing the targets.

TABLE I. Datasets Files

CSV Files	Description
UNSW_NB15_features.csv	49 Features with the class label
UNSW_NB15GT.csv	The name of the ground truth table
UNSW_NB15LIST EVENTS.csv	Name of the event list
UNSW_NB15train/test.csv	Divid the data into 20% 80% for traning and testing

2) EDA
Exploratory data analysis (EDA) is a technique commonly used in data science to explore and analyze datasets. It involves summarizing the main properties of the data using visualizations and other statistical methods. EDA helps in identifying patterns, trends, and anomalies in the data, which can be useful in developing network threats and security measures in IoT using ML [16]. In the context of developing security measures for IoT networks, EDA can be used to identify potential threats and vulnerabilities. By analyzing the data, data scientists can determine which features are most relevant for detecting and preventing attacks. For example, they may look for patterns of network traffic that are indicative of malicious activity or unusual patterns of behavior in connected devices. EDA can also be used to evaluate the effectiveness of different security measures. By analyzing the data before and after implementing a security measure, data scientists can determine whether the measure has effectively mitigated the threat or whether further improvements are needed. Overall, EDA plays a critical role in developing network threat and security measures in IoT using ML by providing insights into the data and helping data scientists make informed decisions about how to address security challenges.

3) Data Preprocessing
Data preprocessing is a crucial step in the development of network threats and security measures in IoT using ML. It involves transforming and cleaning the data to ensure that it is ready for analysis and modeling [17].

4) Data Cleaning
Data cleaning is an essential process in data preprocessing, which involves identifying and handling inaccurate, missing, or irrelevant data points, as well as correcting any errors or inconsistencies in the data. It is a critical step in ensuring that the data used for analysis is accurate and reliable.

5) Data Transformation
Upon analyzing the characteristics of each feature, we determined that standardization and normalization were necessary for the data. Normalization guarantees that there are no duplicated data points and that all data is stored in a single location while ensuring that any dependencies between data points are logical. This step is crucial in ensuring the accuracy and reliability of the data for subsequent analysis and model development [18].

6) Data Reduction
Large datasets can be costly to acquire, slow to process, and challenging to maintain effectively. To address this issue, data reduction techniques are used to provide a simplified representation of the information contained within a dataset. Before proceeding to the data visualization stage, we eliminated outliers from the dataset to obtain a better understanding of how the properties were represented. Although we included all samples of the selected 49 characteristics in the final training,

removing outliers was necessary to ensure that the data was accurate and reliable. By eliminating outliers, we obtained a clearer visualization of the data, which aided in the subsequent analysis and model development stages.

B. Data Visualization

1) Univariate Analysis

In the study, the attacks vs normal samples in the dataset of UNSWNB15train/test.csv were visualized using subplots with the Python seaborn package. Specifically, Figure 4 shows a plot that allows us to compare attacks vs normal [19]. The plot is divided into two subplots, one for the training set and the other for the testing set.In each subplot, the number of samples is displayed on the y-axis, while the type of sample (attack or normal) is displayed on the x-axis. This visualization provides a useful overview of the class distribution in the dataset, which can be helpful when selecting appropriate machine-learning algorithms and evaluating the model performance.

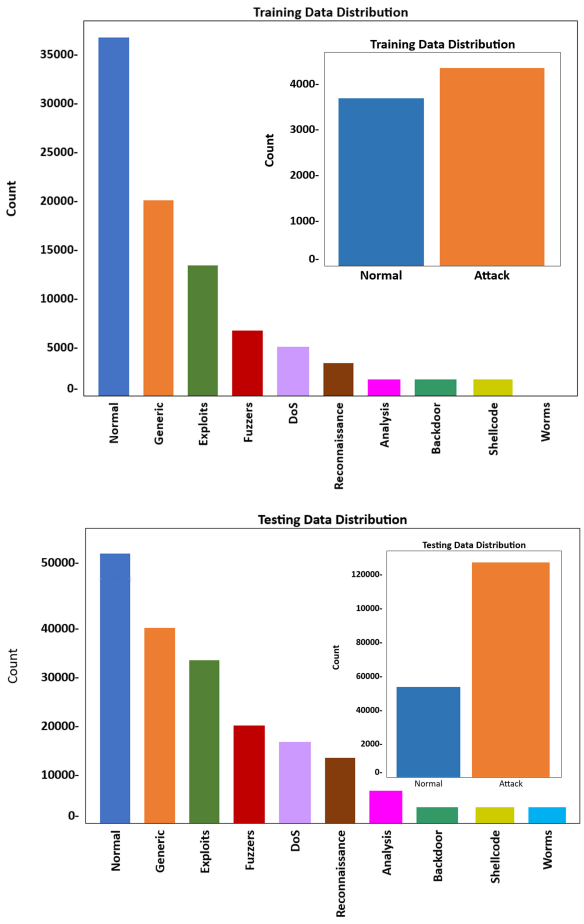

Figure 3. Attack graph analysis: Normal vs Attack

Bivariate Analysis Bivariate analysis is a useful technique to analyze UNSW NB15 testing-testing.csv data, which allows us to compare multiple variables simultaneously. To perform this analysis, we used a heatmap plot generated using the seaborn package in Python. Figure 5 shows the heatmap plot for both the testing and training datasets. The plot shows the correlation between different variables, which helps us to identify any relationships or patterns between them [20]. This can help identify any variables that may be redundant or irrelevant in our analysis, as well as identify potential variables of interest for further exploration.

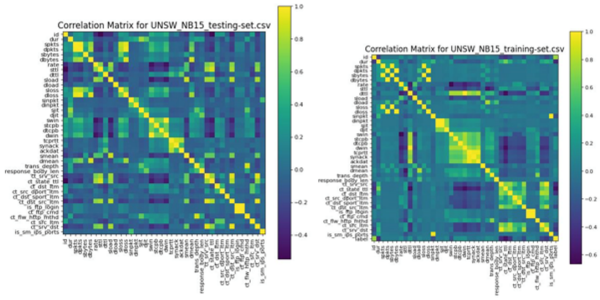

Figure 4. Testing and training confusion matrix

In Figure 4, scatterplots are used to visualize the relationship between two numerical variables in the UNSWNB15training/testing.csv dataset. The position of each point on the plot indicates the values of the two variables for that sample. By examining the scatterplot, we can infer the correlation between the two variables. If the points cluster closely around a line, it suggests a strong positive or negative correlation between the two variables. If the points are more spread out and do not follow a clear pattern, it suggests a weaker or no correlation between the two variables. The scatterplot in Figure 5 helps in identifying the patterns or relationships between two variables in the dataset. By examining the scatterplot, we can gain insights into which variables may be important in predicting the class labels and identifying anomalies.

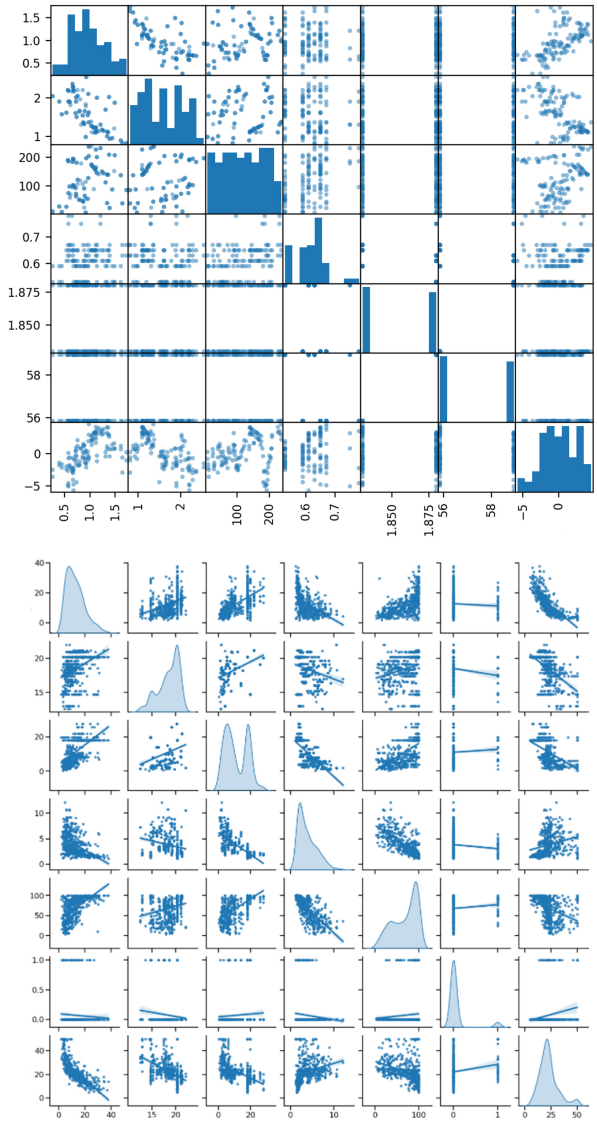

Figure 5. Scatter Density plot

2) Data Splitting
To split the UNSW NB15 dataset into training and testing sets, the sklearn model evaluation package was utilized in this study. The dataset was split into a 70/30 ratio, with 70 percent of the data allocated for training and 30 percent of the data for testing. This allowed for the development of a model that could accurately predict outcomes and generalize well to new, unseen data. Moreover, the model evaluation package was employed to evaluate the model's performance on the testing set using metrics such as accuracy, precision, recall, and F1 score. These metrics provided valuable insights into the model's performance, enabling further optimization and enhancement of the model.

3) Feature engineering
In this input, the characteristics and properties of UNSW-NB15 are represented as structured columns. However, all algorithms require data characteristics with specific qualities to function properly. Therefore, feature engineering is performed to create an input dataset that meets the requirements of ML models. As a result, we start by converting all categorized features into similar numerical labels.

4) Data Normalization
Normalization is a crucial step in the data preparation process that ensures all quantitative columns in a UNSWNB-15 dataset are adjusted to a similar scale, especially when the attributes in the data have varying ranges Fig 6. To address this issue, we used the MinMaxScaler method, which transformed the dataset into a range of (0,1) as follows:

$$X = \frac{x - xmin}{xmax - xmin}$$

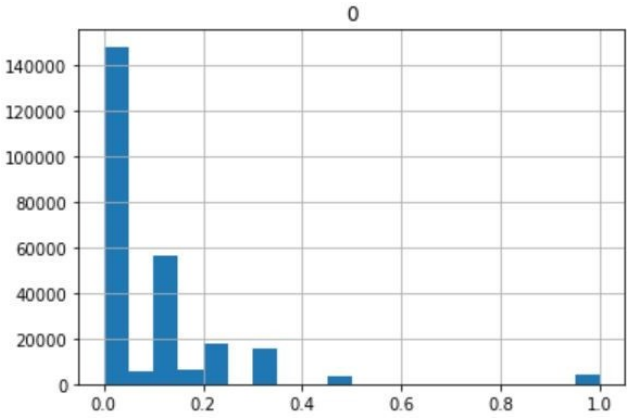

Figure 6. After normalization

C. Machine learning model

The evolution of human civilization has led to the development of numerous technologies that make our lives easier, such as travel, industry, and computing. Machine learning is a subfield of computer science that helps to train computers to manage large datasets more efficiently. It involves the use of various mathematical and programming techniques to find solutions to complex problems.
Anomaly detection systems based on machine learning involve the creation of powerful new models to detect abnormal network traffic using learning algorithms that can flag potential intrusion attempts. Machine learning algorithms enable the creation of a mathematical model based on sample data, which allows computers to make decisions without

being explicitly programmed.

1) Linear Regression
Linear regression is a statistical approach to modeling the relationship between a dependent variable (target) and one or more independent variables (predictors) by fitting a linear equation to the data. It assumes that the relationship between the dependent and independent variables is linear, meaning that a change in one variable is associated with a proportional change in the other variable. In the context of machine learning, linear regression is used for regression tasks, where the goal is to predict a continuous value. The algorithm finds the best-fit line to the data by minimizing the sum of the squared errors between the predicted and actual values. Once the model is trained, it can be used to make predictions on new data. Linear regression has several advantages, including its simplicity and interpretability. It is also computationally efficient and can handle large datasets with a large number of features. However, it has some limitations, such as its assumption of linearity, which may not hold in all cases. It may also be prone to overfitting, which occurs when the model fits the training data too closely and performs poorly on new data.

2) Ridge Classifier
Ridge Classifier is a binary classification algorithm that performs classification by adding a penalty term to the coefficients in the linear equation. This penalty term shrinks the coefficients towards zero and makes the model less complex, reducing the likelihood of overfitting. It is a regularized version of the standard linear classifier that is commonly used when there is a high degree of collinearity among the input features. The Ridge Classifier algorithm optimizes a modified objective function that consists of the sum of squared errors of the training data and a penalty term that is proportional to the square of the magnitude of the coefficients. The penalty term is multiplied by a hyperparameter alpha, which controls the strength of regularization. A higher value of alpha results in stronger regularization and a simpler model. During training, the Ridge Classifier algorithm adjusts the coefficients of the linear equation by minimizing the objective function. The resulting coefficients determine the decision boundary between the two classes, and new data points can be classified by evaluating the linear equation with the learned coefficients. Ridge Classifier has several advantages, such as its ability to handle high dimensional data and its robustness to noise and outliers. However, it also has some limitations, such as its sensitivity to the choice of hyperparameters and its tendency to produce biased estimates if the input features are not properly scaled.

3) Ensemble learning
A machine learning technique called ensemble learning combines different models to increase the reliability and accuracy of predictions. By training several individual models and combining their predictions, the final output is achieved, often through a weighted average that takes into account the performance of each model. There are various ensemble learning techniques, such as bagging, boosting, and stacking Fig 7.

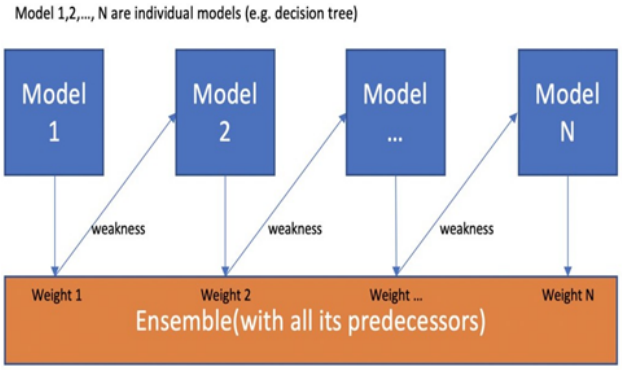

Figure 7. Ensemble (Boosting)

To avoid overfitting and increase model stability, bagging entails training several models on various subsets of the training data. Boosting sequentially trains several models, each of which corrects the flaws in the previous model to increase the model's total accuracy. The process of stacking entails training numerous models and feeding the outputs of those models as inputs into a higher-level model, which then combines the outputs to produce the final product.

$$H = (x) = pi\,if = \sum_{k=0}^{n} \binom{n}{x} x^k a^{n-k} \ldots\ldots eq(2)$$

Ensemble learning can significantly enhance the performance of machine learning models. However, it may be computationally expensive and require a large amount of data to train individual models. Therefore, careful consideration of the tradeoffs between model accuracy and computational resources is important when utilizing ensemble learning techniques.

4) SGD
Machine learning frequently employs the optimization process known as Stochastic Gradient Descent (SGD). It is a variation of gradient descent, which is employed in learning algorithms to reduce the cost function.

In SGD, instead of computing the gradients of the cost function using the entire dataset, the gradients are calculated for a small subset of the data at each iteration. This is more computationally efficient and allows for faster convergence to the optimal solution.

$$min\left\{\frac{1}{N} \in l(w^t xn, yn)\right\} where\ f(w)\ Linear\ ...(3)$$

$$min\left\{\frac{1}{N} \in l(h^w xn, yn)\right\} where\ f(w)\ General\ ...(4)$$

SGD is particularly useful for large scale problems, where the number of examples in the dataset can be in the millions or billions. It can also be used for online learning, where the model is updated continuously as new data arrives. One potential disadvantage of SGD is that it can be sensitive to the learning rate, which determines the step size of each iteration. To address this issue, various techniques such as learning rate schedules and adaptive learning rates have been developed to help SGD converge more efficiently.

D. Model Evaluation

Model evaluation, a crucial step in machine learning, helps assess how well a trained model performs when used with new, untested data. In this process, the model is first trained on a training dataset and then evaluated on a test set, which is an additional, unidentified dataset. To evaluate the model's performance, various metrics are used depending on the type of problem being solved, such as classification or regression. For classification problems, commonly used metrics include accuracy, precision, recall, and F1 score (Table II). These metrics are derived from a confusion matrix showing the true positives, true negatives, false positives, and false negatives predicted by the model. Precision evaluates how frequently the model accurately detects positive predictions, whereas accuracy measures how frequently the model makes the right forecast. The frequency with which the model correctly recognizes true positives is measured by recall, while the harmonic mean of accuracy and recall is the F1 score. These measures are employed to assess the performance of various models and to compare them. Positive vs negative predicted values (Table II)

TABLE II. Positive vs negative values

	Predicted Negative	Predicted Positive
Actual Negative	True Negative (TN)	False Positive (FP)
Actual Positive	False Negative (FN)	True Positive (TP)

Based on the values from the confusion matrix, we assess the optimal neural network model for each class to further assess anomaly detection effectiveness. [20]. The model evaluation of all algorithms is calculated using the above Performance Metrics (Table III).

TABLE III. Performance Metrics

Performance metrics	Formulas
Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$
Precision	$\frac{TP}{TP+FP}$
Recall	$\frac{TP}{TP+FN}$
F1 Score	$2 * \frac{Precision*Recall}{Precision+Recall}$
Throughput	$\frac{\sum ReceivedPackets*PacketSize}{SimulationTime}$

TABLE IV. All Machine Learning Model result

Model	Accuracy	Precision	Recall	F1 score
Linear Regression	94%	95%	99%	97%
Ridget Classifier	97%	98.3%	98.5%	98.4%
SGD Classifier	96.6%	99.9%	98.4%	98.7%
Ensemble Learning	96.5%	98.45%	98.5%	98.4%

Table IV. Shows all evaluated machine learning model result. The result depicts that the accuracy of the Rigdet classifier is better than other classifiers in terms of Accuracy. Result Analysis ROC (Receiver Operating Characteristic) curves are a graphical representation of the performance of a binary classifier, which shows the tradeoff between its sensitivity and specificity for different classification thresholds. When comparing ROC curves, the AUC-ROC value can be used to determine which classifier is performing better. The higher the AUC-ROC value, the better the classifier's performance.

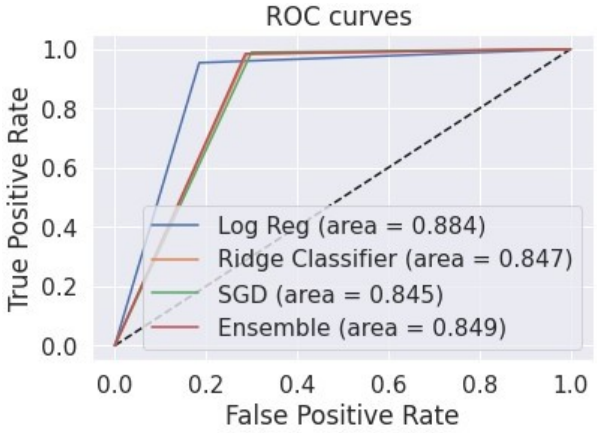

Figure 8. Positive vs negative values

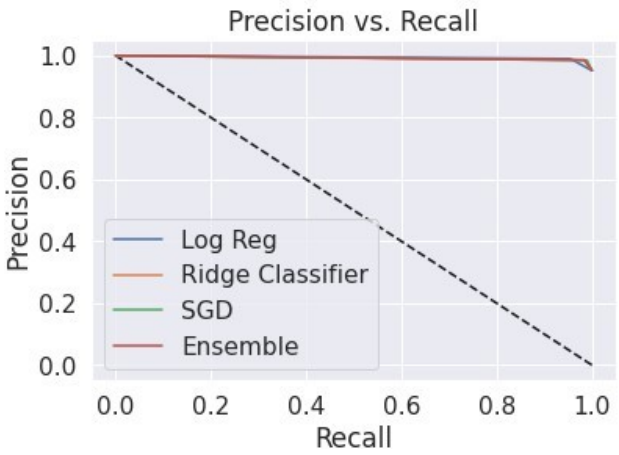

Figure 9. Precision vs, recall all algorithms

Based on the confusion matrices, ROC curves, and Precision and Recall charts shows in Figure 9, and 10 the overall performance of classification is quite good, with most of the predictions falling on the diagonal. However, there are a few classes where the misclassification rate is higher. For example, all three methods incorrectly identified DoS packets as vulnerabilities, and the same was observed for backdoor and analysis classes. The reason for this misclassification is the data imbalance, which we attempted to address. However, due to the significant variation in the number of samples available for each class, we still need to address this issue for classes with fewer examples. This problem can lead to over fitting, which affects the classification accuracy of certain classes.

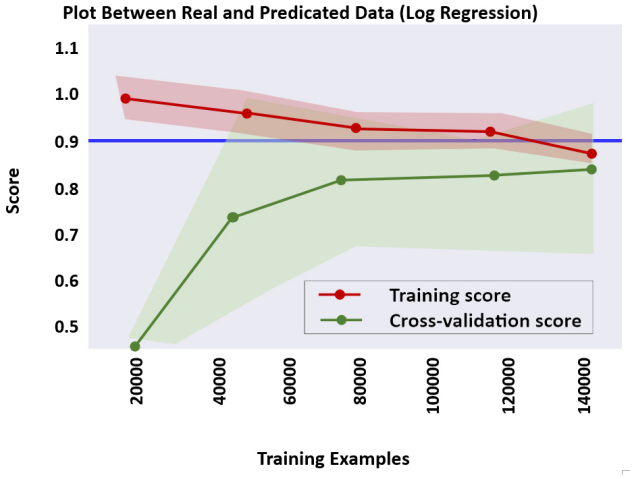

Figure 10. Real and predicted (SGD)

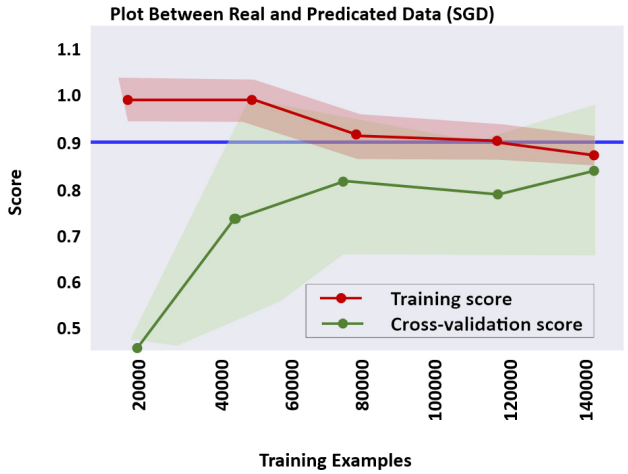

Figure 11. Real & Predicted (Log Regression)

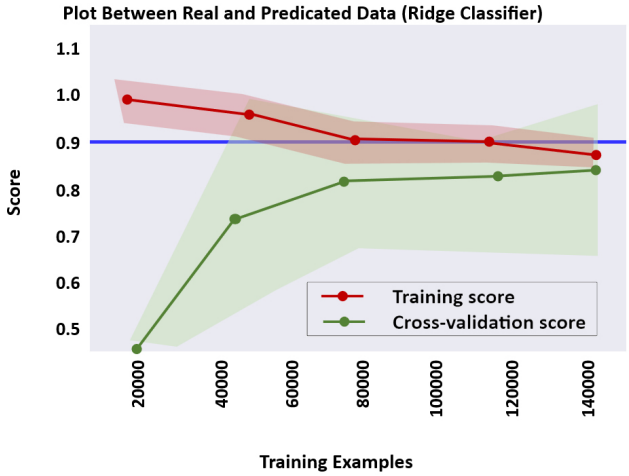

Figure 12. Real vs predicted (Ridge classifier)

Another way to compare ROC curves is to visually examine the curve shape. A steeper ROC curve indicates better performance, as it means that the classifier can achieve high true positive rates (sensitivity) while keeping a low false positive rate (1-specificity) across a wide range of classification thresholds. It is important to note that ROC curves and AUC-ROC values should be interpreted in the context of the specific problem being solved and the costs associated with false positives and false negatives. In some cases, a classifier with a lower AUC-ROC value may be more appropriate, depending on the specific needs and constraints of the application. Here plotting real and predicted data of log regression, SGD and Ridge classifier is shown in (Fig 10, 11 and, 12) means that we are visualizing the actual values and the values that our machine-learning model has predicted. By plotting both the real and predicted data on a

graph, we can easily compare and contrast the two sets of values.

V. Discussions

The results of the study suggest that the proposed features can effectively differentiate between legitimate and malicious activities using data from IoT sensors from the UNSW-NB15 dataset. This implies that machine learning (ML) methods can be employed to develop network threats and security measures in IoT. The Custom Tab Transformer system, which is based on network flow identifiers and characteristics, can be used to track suspicious attack activities. The Ridge classifier model outperformed both classification models, achieving a greater detection rate, accuracy, and a lower false positive rate (FPR). This suggests that the Ridge classifier is more effective at detecting attacks and minimizing the risk of false alarms. The results of the study also demonstrated that ML methods using flow IDs can efficiently and effectively detect assaults and their trails. The metrics obtained from the ML models trained on the UNSW-NB15 dataset show that the proposed approach can be used to develop effective security measures for IoT devices. Overall, these findings provide valuable insights into the use of ML methods for developing network security measures in IoT and highlight the potential of flow IDs for detecting and preventing malicious activities.

VI. Limitations of the Study

This research was limited to the UNSW-NB15 dataset, which is a publicly available dataset with a relatively small number of samples compared to real-world scenarios. Therefore, the performance of the proposed ML algorithms may vary when applied to larger and more diverse datasets. Secondly, the study focused on network traffic data from IoT sensors and did not take into account other sources of data, such as system logs, user behavior, and contextual information, which may improve the accuracy of the anomaly detection models. Thirdly, the study used a fixed set of features extracted from the network traffic data, which may not capture all possible characteristics of the network behavior. The use of more advanced feature extraction techniques may improve the accuracy of the proposed models.

VII. Conclusion and Future Work

This paper aims to explore the development of network threats and security measures in IoT using machine learning. The UNSW-NB15 dataset was used to evaluate the performance of various machine learning algorithms such as linear regression, ridge classifier and ensemble learning. The accuracy findings demonstrated that these models can effectively distinguish between normal and malicious activities in an IoT network. The dataset is large, which makes Proposed algorithm was statistically measured and compared with existing literature. Proposed work with existing work. For validation purpose (Table V)

TABLE V. All Machine Learning Model result

Citation	Methods	Accuracy
[12]	CNN, BAT-MC, BAT	97%
Proposed work	Linear regression, Ridge classifier, SGD and Ensemble learning	97%
[13]	XGBOOST CLASSIFIER, Random forest	90
[14]	MLP	82.4%

It is suitable for training and evaluating machine learning models. The UNSW-NB15 dataset is also freely available for research purposes, making it accessible to researchers and practitioners in the field. Finally, the dataset has a specific focus on anomaly detection, which is a critical area of cybersecurity. Amongst the models tested, the ridge classifier and ensemble learning demonstrated the best performance, with the ridge classifier achieving an accuracy of 97%. This highlights the importance of selecting the appropriate machine learning algorithm for anomaly detection in IoT networks. Furthermore, this paper also utilized exploratory data analysis techniques to gain insights into the distribution and skewness of the data, which aided in better visualizing the data and determining which attribute is more crucial than others. The results obtained can inform the development of effective security measures for IoT networks, thus contributing to the ongoing efforts to ensure the security and privacy of IoT devices and networks. In the future, it would be useful to investigate the performance of the ML models on larger and more diverse datasets. It would be worthwhile to investigate the use of more advanced ML techniques such as deep learning and reinforcement learning. It may be useful to explore the development of more automated approaches to network threat detection and mitigation. This could involve the use of intelligent agents or other AI-based approaches to continuously monitor and respond to threats in real time. It may be worthwhile to investigate the integration of blockchain technology with IoT networks as a means of enhancing security and privacy. This could involve the use of smart contracts to automate threat detection and mitigation, or the use of blockchain-based identity management systems to better secure IoT devices and networks.

References

[1] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," *IEEE communications surveys & tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[2] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for iot security based on learning tech-

niques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019.

[3] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, "Towards developing network forensic mechanism for botnet activities in the iot based on machine learning techniques," pp. 30–44, 2018.

[4] S. H. Chauhdary, M. S. Alkatheiri, M. A. Alqarni, and S. Saleem, "An efficient evolutionary deep learning-based attack prediction in supply chain management systems," *Computers and Electrical Engineering*, vol. 109, p. 108768, 2023.

[5] V. A. Kanthuru, S. Rajasegarar, P. Rathore, R. R. M. Doss, L. Pan, B. Ray, M. Chowdhury, C. Srimathi, and M. S. Durai, "Cyber attack detection in iot networks with small samples: Implementation and analysis," in *International Conference on Advanced Data Mining and Applications*. Springer, 2022, pp. 118–130.

[6] F. Khan, R. Alturki, M. A. Rahman, S. Mastorakis, I. Razzak, and S. T. Shah, "Trustworthy and reliable deep-learning-based cyberattack detection in industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 1030–1038, 2022.

[7] R. A. Elsayed, R. A. Hamada, M. I. Abdalla, and S. A. Elsaid, "Securing iot and sdn systems using deep-learning based automatic intrusion detection," *Ain Shams Engineering Journal*, vol. 14, no. 10, p. 102211, 2023.

[8] P. Chapman, "Defending against insider threats with network security's eighth layer," *Computer Fraud & Security*, vol. 2021, no. 3, pp. 8–13, 2021.

[9] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-based methods for cyber attacks detection in iot systems: A survey on methods, analysis, and future prospects," *Electronics*, vol. 11, no. 9, p. 1502, 2022.

[10] A. Raza, S. Memon, M. A. Nizamani, and M. H. Shah, "Machine learning-based security solutions for critical cyber-physical systems," in *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE, 2022, pp. 1–6.

[11] A. Jahangeer, S. U. Bazai, S. Aslam, S. Marjan, M. Anas, and S. H. Hashemi, "A review on the security of iot networks: From network layer's perspective," *IEEE Access*, 2023.

[12] D. Nookala Venu, A. Kumar, and M. A. S. Rao, "Botnet attacks detection in internet of things using machine learning," *NeuroQuantology*, vol. 20, no. 4, pp. 743–754, 2022.

[13] I. U. Khan, N. Aslam, R. AlShedayed, D. AlFrayan, R. AlEssa, N. A. AlShuail, and A. Al Safwan, "A proactive attack detection for heating, ventilation, and air conditioning (hvac) system using explainable extreme gradient boosting model (xgboost)," *Sensors*, vol. 22, no. 23, p. 9235, 2022.

[14] Y. Yin, J. Jang-Jaccard, W. Xu, A. Singh, J. Zhu, F. Sabrina, and J. Kwak, "Igrf-rfe: a hybrid feature selection method for mlp-based network intrusion detection on unsw-nb15 dataset," *Journal of Big Data*, vol. 10, no. 1, pp. 1–26, 2023.

[15] M. Anwer, S. M. Khan, M. U. Farooq *et al.*, "Attack detection in iot using machine learning," *Engineering, Technology & Applied Science Research*, vol. 11, no. 3, pp. 7273–7278, 2021.

[16] T. R. Gadekallu, M. Manoj, N. Kumar, S. Hakak, S. Bhattacharya *et al.*, "Blockchain-based attack detection on machine learning algorithms for iot-based e-health applications," *IEEE Internet of Things Magazine*, vol. 4, no. 3, pp. 30–33, 2021.

[17] O. Habibi, M. Chemmakha, and M. Lazaar, "Imbalanced tabular data modelization using ctgan and machine learning to improve iot botnet attacks detection," *Engineering Applications of Artificial Intelligence*, vol. 118, p. 105669, 2023.

[18] M. E. Shipe, S. A. Deppen, F. Farjah, and E. L. Grogan, "Developing prediction models for clinical use using logistic regression: an overview," *Journal of thoracic disease*, vol. 11, no. Suppl 4, p. S574, 2019.

[19] V. A. Kanthuru, S. Rajasegarar, P. Rathore, R. R. M. Doss, L. Pan, B. Ray, M. Chowdhury, C. Srimathi, and M. S. Durai, "Cyber attack detection in iot networks with small samples: Implementation and analysis," in *International Conference on Advanced Data Mining and Applications*. Springer, 2022, pp. 118–130.

[20] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Machine learning-based iot-botnet attack detection with sequential architecture," *Sensors*, vol. 20, no. 16, p. 4372, 2020.

Abdullah Alomiri, Master student in Cyber Security & Digital Forensics ,IT Deptt. Majmaah University, Saudi Arabia. His research interests include cloud security, cybersecurity, the IoT, semantic web, cloud and edge computing, and smart city and mathematical modeling of physical and biological problems in general and mathematical analysis.

Shailendra Mishra, Shailendra Mishra (Senior Member, IEEE) received the Master of Engineering (M.E.) and Ph.D. degrees in computer science and engineering from the Motilal Nehru National Institute of Technology (MNNIT), India, in 2000 and 2007, respectively. He is currently working as Professor with the Department of Computer Engineering, College of Computer and Information Science, Majmaah University, Majmaah, Saudi Arabia. He has published and presented more than 90 research articles in international journals and international conferences. His current research interests include cloud and cyber security, SDN, the IoT security, communication systems, computer networks with performance evaluation, and design of multiple access protocol for mobile communication networks. He is a Senior Member of ACM, and a Life Member of the Institution of Engineers India (IEI), the Indian Society of Technical Education (ISTE), and ACEEE

Mohammed AlShehri, Mohammed Alshehri (Member, IEEE) received the B.S. degree from King Saud University, in 2001, the M.S. degree in computer and communication engineering from the Queensland University of Technology (QUT), Australia, in 2007, and the Ph.D. degree in information technology from Griffith University, Australia, in 2013. From 2002 to 2009, he was with the Ministry of Defense, Saudi Arabia, as an IT Manager, where he was a Consultant, from 2013 to 2015. He has been with Majmaah University, Saudi Arabia, since 2015, where he is currently Professor and Vice Rector ,Majmaah Universty. His research interests include span both computer science and information technology and applications to robotics in the field of education, cloud computing, artificial intelligence, and data science.