Iot Networks Intrusion Detection Using Machine Learning

Aqila Khatoon
AK1801406@qu.edu.qa

Department of Computer Science and Engineering
Qatar University
Doha, Qatar

Nirvana Aladal
NA1802829@qu.edu.qa

Department of Computer Science and Engineering
Qatar University
Doha, Qatar

Meriem Boussaa
MB1902903@qu.edu.qa

Department of Computer Science and Engineering
Qatar University
Doha, Qatar

***Abstract*— Intrusion detection is essential because of the growing number of Internet of Things (IoT) devices being used in various applications, which has raised the danger of security risks. In IoT networks, the usage of machine learning (ML) techniques for intrusion detection is on the rise. In this study, we investigate the efficacy of four popular machine learning (ML) methods for detecting intrusions in Internet of Things networks: Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Deep Learning, and Naïve Bayes. Using a dataset of network traffic data, we assess these algorithms' performance using a variety of performance criteria, such as accuracy, precision, recall, and F1-score. Our results demonstrate that all four algorithms are capable of reliably identifying intrusions in IoT networks, with deep learning showing the best accuracy and F1-score. The intrusion detection system's unique needs, such as the type of data being used and the available computing power, ultimately determine which method is used. Possibilities for improving the security of IoT installations are presented by the development of ML-based intrusion detection systems for IoT networks.**

Keywords*— *Machine Learning, Deep Learning, Intrusion Detection, SVM, KNN, Naïve Bayes

I. INTRODUCTION

The Internet of Things (IoT) is a network of linked objects working together to make decisions autonomously. The objects are devices that are utilized daily such as basic sensors and intricate industrial machines. The potential of employing advanced technologies in everyday life via the internet increased due to the emergence of numerous technologies such as wireless networking and automated proof of identity. Automated proof of identity, 5G networks and sensors are also included in the advanced technologies. Some of the interesting examples of internet of things usage are agricultural industries, manufacturing industries, healthcare devices, automation and transport and home automation. The drastic increase in the application of the internet of things requires strengthening the security precautions. There are security and privacy issues in IoT that arise from the consumption of energy and memory retention. The previous issues make it challenging to implement AES and RSA in IoT. Traditional security techniques such as cryptography and encryption that use the same key by many nodes result in increasing the vulnerability of the network if one of the nodes is hacked. Moreover, Machine learning based intrusion detection algorithms are incorporated in IoT systems nowadays as they reduced the energy usage.

A. Intrusion Detection System

To find malicious activity or security policy violations in network traffic, intrusion detection systems (IDS) are utilized. Unauthorized access to the IoT system, malware infections like viruses or torjans, and other attacks that interfere with the system's functionality are all examples of intrusions. Malware that results in denial of service affects the communication between the client and server. The detection rate is the major objective of intrusion detection systems. There are two forms of intrusion detection: host-based IDS, which monitors a single device, and network-based IDS, which keeps an eye on a network cloud. The implementation of machine learning-based approaches like Naive Bayes and SVM improves the rate of intrusion detection.

B. Machine Learning

Machine learning is a form of Artificial Intelligence (AI) that trains computers from experience rather than programming them. Machine learning algorithms are tested on large datasets which allow the visualization of different data patterns and making future predictions. Machine learning is widely used in this era and some applications of machine learning are fraud detection, automatic language translation and image and speech recognition. The process of Machine learning includes data gathering and preparation, training and testing the data and model deployment. Machine learning algorithms are classified into supervised, unsupervised and reinforcement learning. Initially, supervised learning is when the model is trained on a labelled dataset, KNN, Naïve Bayes and SVM are supervised learning algorithms. Unsupervised learning model is trained on an unlabeled dataset and the goal is to identify the data relationships and patterns such as clustering. Finally, reinforcement learning is when a model learns by trial and error and interacting with the environment.

II. BACKGROUND

Intrusion detection systems for IoT have been implemented using several machine learning algorithms

such as Naïve Bayes, K-Nearest Neighbours (KNN), support vector machines (SVM) and deep learning. The algorithms are deeply explained below.

A. *Naïve Bayes*

Naive Bayes is a probabilistic classification method that depends on the Bayes theorem, which calculates the probability of an event given the information or evidence that is currently available. Bayes networks are effective tools for making decisions and using logic in uncertain situations [7]. The process of calculating conditional probabilities is simplified by making the naive assumption that every attribute in the dataset is unique and equally significant. To detect and categorize network attacks for internet of things intrusion detection, the Naive Bayes machine learning algorithm analyzes the data set supplied by the network and predicts whether an anomalous packet flow will occur. The naive bayes method has numerous benefits, including being rapid and simple to develop and not requiring a sizable training dataset, which is helpful for IDS in contexts with limited resources. Naive Bayes' flaw is that it makes assumptions.

B. *Support Vector Machines*

SVM [8] has been extensively employed in the context of intrusion detection systems to categorize and identify network threats. In accordance with the values of the characteristics retrieved from the packets, SVM may categorize network packets as benign or malicious. SVM offers several benefits, such as the capacity to handle huge databases with high complexity and the flexibility to handle both nonlinear and linear data. SVMs can also manage skewed datasets, which makes them appropriate for systems to detect intrusions where harmful data is comparatively infrequent. SVM has some drawbacks, including the potential for high computational costs, especially when training big datasets.

C. *K-Nearest Neighbours*

KNN [9] can be used to categorize network traffic into legitimate or malicious in relation to intrusion detection in Internet of Things (IoT) networks based on the features retrieved from the network packets. KNN can be used to identify possible dangers in fresh traffic by first applying it to datasets of known benign and malicious traffic. KNN has the benefit of being a straightforward and simple algorithm, which makes it perfect for environments with little resources. KNN can be used for multi-class classification and binary classification and can handle both nonlinear and linear data. The fact that KNN can be sensitive to the distance measure employed and the K value chosen is one of its key disadvantages. The algorithm's performance can be considerably impacted by the distance metric that is selected.

D. *Deep Learning*

Neural networks are used in deep learning, a subset of machine learning, to extract complicated patterns and characteristics from data. By examining the enormous amounts of data produced by IoT devices, deep learning algorithms can be utilized in the IoT to detect and avoid network assaults. Deep learning architectures' self-taught and compression features are essential tools for identifying hidden patterns in training data that may be used to distinguish between attacks and legitimate traffic [10]. The use of deep learning has emerged as a promising method for intrusion detection considering the growing number of IoT devices and their potential vulnerability to cyber-attacks. To find anomalies and patterns in network traffic, deep learning algorithms can be trained on massive datasets of legitimate and malicious traffic. Deep Learning's capacity to automatically discover and retrieve features from the data, eliminating the requirement for manual feature engineering, is one of its key advantages. Large data sets for IoT intrusion detection can be difficult to gather and classify and training a Deep Learning model demands a lot of processing power.

III. ATTACK ALGORITHMS

As the variety of IoT devices expands so will the requirement for robust intrusion detection techniques. Machine learning algorithms have emerged as a potential way for determining attacks in IoT networks, with a broad range of approaches available for recognizing and preventing various sorts of assaults. In this context, this section addresses some of the most frequently encountered attack algorithms utilized in IoT network intrusion detection by applying machine learning.

A. *Distributed Denial of Service (DDoS)*

DDoS attacks are a more advanced type of DoS attacks in which numerous devices are utilized to initiate an attack[10]. The attacker in a DDoS assault directs a network of hacked devices (known as a botnet) to perform a coordinated attack on a target device or network. DDoS attacks can be detected using machine learning algorithms that analyze network traffic patterns and identify the coordinated behavior of numerous devices.

B. *Man-in-the-Middle (MitM)*

These attacks occur when an attacker intercepts communication between two IoT devices and modifies, steals, or injects new data. The attacker can listen in on the conversation, take important information, or modify the data to fool the devices. By analyzing communication patterns and recognizing any unforeseen modifications in the communication flow or data content, machine learning algorithms can detect MitM attacks.

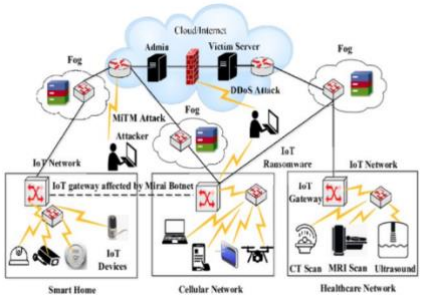

Figure 1: Security attacks on IoT devices

According to the findings of the previous figure, cyber assaults against IoT devices are on the increase and continue

to pose a substantial danger to the delivery of a wide variety of Internet services. The attacker captures communication between both parties and can change or alter the transmission in the MitM attack. In the DDoS attack, the attacker floods the network with traffic to overload and disrupt the normal communication. As a result, information security is a necessity that can monitor and secure the continuous flow of data over the Internet.

C. *Spoofing attacks*

A spoofing attack occurs when an attacker impersonates an authorized IoT device in order to acquire network access. This can be accomplished by stealing a valid device's identification or by inventing a false identity. Once the attacker has gained access, they can undertake illegal network activity. Machine learning techniques can detect spoofing attempts by monitoring the device's identification and behavior and finding any unusual changes.

D. *Replay attacks*

In a replay attack, the attacker collects valid communication between two IoT devices and repeats the same data to obtain unauthorized access. The attacker can use the recorded data to circumvent security measures and gain access to the network. Machine learning systems can detect replay attacks by examining communication patterns and recognizing any recurring patterns or data.

E. *SQL Injection attacks*

This type of attack takes advantage of flaws in web-based applications that use SQL databases by introducing malicious SQL code into user input areas. This can allow attackers to gain unauthorized access to sensitive data or execute arbitrary instructions on the database. By examining query patterns and spotting irregularities in the organization and syntax of arriving SQL queries, machine learning models may be taught to detect SQL injection attacks[11].

F. *Advanced Persistent Threat (APT) attacks*

An attacker makes a sustained and focused effort to obtain unauthorized access to a system. Multiple phases and strategies, including as malware distribution, spear-phishing, and social engineering, are frequently used in APT assaults[12]. APT assaults may be detected using machine learning models that analyze patterns of behavior and discover abnormalities in network traffic, user activity, and system records.

G. *Remote Code Execution (RCE) attacks*

This type of attack takes advantage of flaws in software applications to launch arbitrary code on a remote server. By examining code patterns and finding irregularities in the syntax and layout of incoming code, machine learning models may be taught to detect RCE attacks.

H. *Cross-Site Scripting (XSS) attacks*

These attacks inject malicious code into a website, enabling attackers to gain user credentials or conduct unauthorized actions on the website. Machine learning models may be taught to identify XSS attacks by examining the structure and syntax of the requests and answers.

I. *Buffer Overflow attacks*

This type of attack exploits weaknesses in software programs by overflowing a buffer with more information than it can manage, causing the system to malfunction or launch arbitrary code. Machine learning models may be taught to recognize buffer overflow attacks by studying code patterns and recognizing irregularities in the quantity and structure of incoming data.

J. *Clickjacking attacks*

These attacks fool users into tapping on a hidden button or url by overlaying it over another legitimate-looking interface component. Machine learning models may be taught to distinguish between clickjacking attacks by studying user interactions and acknowledging irregularities in the location and behavior of interface components.

K. *Cross-Site Request Forgery (CSRF) attacks*

These attacks trick users into executing unauthorized activities on a website by forging requests from an authorized user. Machine learning models may be taught to detect CSRF attacks by examining the layout and syntax of incoming queries and recognizing irregularities in the origin and destination of the request.

L. *Brute-force attacks*

These entail a systematic attempt to determine a user's password or other login information by attempting multiple combinations of letters or words. Machine learning models may be taught to detect brute-force assaults by examining patterns of unsuccessful login attempts and spotting irregularities in the number and sequence of login requests.

Machine learning algorithms can be trained to detect these types of attacks by analyzing the patterns of network traffic, identifying anomalies, and detecting deviations from normal behavior. It is important to note that these are just a few examples of the many different types of attack algorithms that can be used to target IoT networks. Additionally, the specific machine learning techniques used to detect these attacks may vary depending on the type of attack and the nature of the IoT network being monitored.

Figure 2 below shows an illustration of what might happen if we employed intrusion detection technologies. Because of the remote-control functionality, many IoT servers and IoT devices are immediately accessible to the public Internet, as seen in this diagram. Attackers will use the flaws to get access to the IoT servers. An IDS is essential for detecting and protecting IoT servers from attacks.

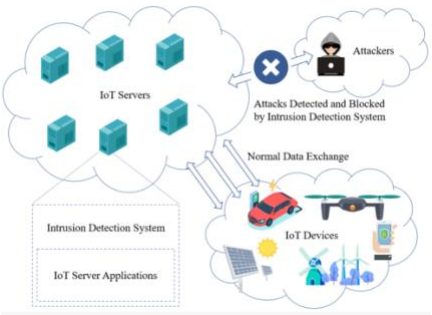

Figure 2. The Scenario of the IDS applied in the IoT network.

IV. EVALUATION METHODOLOGIES

The increased use of IoT devices in our daily lives has resulted in a rise in cybersecurity concerns. To identify and prevent these risks, intrusion detection systems (IDS) have been created; however, the efficiency of these systems must be evaluated using assessment procedures. There are several assessment approaches available for assessing the efficiency of intrusion detection systems in identifying certain attack tactics in IoT networks. In the following section, we will look at different assessment approaches and how they might be utilized to improve the performance of intrusion detection systems.

A. Dataset-based evaluation

*T*o implement this method, a labelled data set of the network's traffic is needed, where normal and anomalous traffic is recorded. This dataset is then split into a training and testing set, to use the training set to train the model, and the testing set to evaluate its performance. Using this method allows for an objective evaluation as it is trained for a wide range of synopses. However, many challenges can be faced while using this method, such as wrong labeling of data and the chance of facing a very different real-world attack that was not learned by the model. This concludes that the performance of the data set may not accurately reflect its real-world performance. Hence, it can't be relied on to get accuracy and approve the model.

B. Cross-validation:

The data set is first divided into K folds (typically k is between 5 - 10), so each fold can be used as training and testing set. This method yields a more accurate perfomance as of data have been used for training and testing. [13] used 5-fold cross validation to evalute different techniques implementing deep learning model. Results in graph… can be seen of the perfromance of the model in pridicting the attacks:

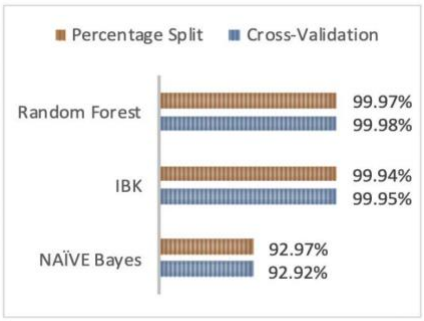

Figure 3. Comparison of Accuracy on KDDCup99 Dataset.

C. Receiver Operating Characteristic ROC curve analysis

This curve represents the trade-off between true positive rate and false positive rate in a classification method. In network intrusion detection the curve can evalute the performance of the model. From the ROC curve the model can be adjusted as such the commonly used to evalute the perfromance, and AUC of 1 is considered a perfect model, although on average most model have an AUC of 0.5. We can see ROC evalution used in the below table by [14] for evaluting different algorithms for intrusion detection. In this case the ROC is a very helful metric to select the best algortithm that would reduce the number of false positives and increase accuracy.

Table 1. ROC comparison of deep learning architectures.

Algorithm	*ROC*
RBF	*0.9741*
Ensemble	*0.9639*
KNN	*0.9532*
NB	*0.9481*
SVM	*0.8023*
KM	*0.6148*
FCM	*0.6148*

D. Precision, recall, and F1-score

This is the most common method used to evaluate the performance of a machine learning model. The precision of a deep learning model is detected by properly identifying malicious activity. It is defined in this context as the ratio of true positives (properly recognized malicious actions) to the total positive predictions provided by the model. Next, the model's recall is defined as the proportion of true positives to the total number of real malicious behaviours in the data. This statistic assesses the model's ability to detect all harmful activity in data. The harmonic mean of accuracy and recall is the F1-score. It gives a single figure that combines accuracy and recall, giving equal weight to each. It's very effective to compare the positive instances and the actual positive instances, as it shows where the model went wrong, and how successful the model was in doing the task. When the balance between accuracy and recall is critical, the F1 score can be beneficial. The F1 score is determined as follows:

F1-score = 2 * (Preciseness * Recall) / (Preciseness + Recall)

[15] have determined that the CNN architecture implemented to detect the attacks has shown 99.5% - 99.9% in F1-score, proving that the model used is ideal for detecting attacks on the network.

E. *Real-world testing*

Refers to the evaluation and assessment of a system, such as an intrusion detection system (IDS) for IoT networks, in a real-world environment. It involves deploying the system in a production environment and observing its performance under real-world conditions. During real-world testing, the IDS is exposed to live network traffic and continuously monitored to evaluate its ability to detect and respond to intrusions accurately and promptly. The performance of the system can be assessed based on various metrics, including detection accuracy, false positive and false negative rates, response time, and system stability. It is important to note that real-world testing should be conducted in a controlled manner, considering the potential risks associated with live attacks and the impact on the operational network. Careful planning, coordination, and risk mitigation strategies should be in place to ensure the safety and security of the network during testing.

V. RESULTS AND CONCLUSION

Intrusion detection systems for IoT have been implemented using several machine learning algorithms such as Naïve Bayes, K-Nearest Neighbors (KNN), support vector machines (SVM) and deep learning. To detect and categorize network attacks for internet of things intrusion detection, the Naive Bayes machine learning algorithm analyzes the data set supplied by the network and predicts whether an anomalous packet flow will occur. Machine learning algorithms can be trained to detect these types of attacks by analyzing the patterns of network traffic, identifying anomalies, and detecting deviations from normal behavior. The most critical part of implementing a machine learning model for attacks detection is to carefully evaluate the model, as the network is very data sensitive. Ensuring high percentage of accuracy and precision is necessary since the system is intolerable for faults.

REFRENCES

[1] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Nov. 2014, doi: https://doi.org/10.1109/iccad.2014.7001385.

[2] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020, doi: https://doi.org/10.1109/COMST.2020.2986444.

[3] J. J. P. Tsai and Z. Yu, *Intrusion Detection: A Machine Learning Approach*. World Scientific, 2011. Accessed: May 11, 2023. [Online]. Available: https://books.google.com.qa/books?hl=en&lr=&id=_Fa7CgAAQBAJ&oi=fnd&pg=PR7&dq=+Intrusion+Detection++A+Machine+Learning+Approach.+&ots=WPp2y33NI_&sig=pvCKgxjhuRhVV_xh7lijfAafiKY&redir_esc=y#v=onepage&q=Intrusion%20Detection%20%20A%20Machine%20Learning%20Approach.&f=false

[4] Evtimov *et al.*, "Robust Physical-World Attacks on Machine Learning Models." Accessed: May 11, 2023. [Online]. Available: https://s3.observador.pt/wp-content/uploads/2017/08/08133934/1707-08945.pdf

[5] M. Zhong, Y. Zhou, and G. Chen, "Sequential Model Based Intrusion Detection System for IoT Servers Using Deep Learning Methods," *Sensors*, vol. 21, no. 4, p. 1113, Feb. 2021, doi: https://doi.org/10.3390/s21041113.

[6] R. Chaudhary, G. S. Aujla, N. Kumar, and S. Zeadally, "Lattice based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions," *IEEE Internet of Things Journal*, pp. 1–1, 2018, doi: https://doi.org/10.1109/jiot.2018.2878707.

[7] Amor N., Benferhat S., Elouedi Z. Naive Bayes vs Decision Trees in Intrusion Detection Systems; Proceedings of the 2004 ACM symposium on Applied computing; Nicosia, Cyprus. 14–17 March 2004; pp. 420–424. [Google Scholar]

[8] Kaplantzis S., Shilton A., Nallasamy M., Sekercioglu Y. Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Support Vector Machines; Proceedings of the 3rd IEEE International Conference on Intelligent Sensors, Sensor Networks and Information; Melbourne, Australia. 3–6 December 2007; pp. 335–340. [Google Scholar]

[9] Sutharshan R., Leckie C., Palaniswami M., Bezdek J.C. Anomaly Detection in Wireless Sensor Networks. IEEE Wirel. Commun. 2008;**15**:34–40. [Google Scholar]

[10] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Distributed denial of service (ddos) resilience in cloud: Review and Conceptual Cloud Ddos Mitigation Framework," *Journal of Network and Computer Applications*, vol. 67, pp. 147–165, 2016. doi:10.1016/j.jnca.2016.01.001

[11] K. Ross, M. Moh, T.-S. Moh, and J. Yao, "Multi-source data analysis and evaluation of machine learning techniques for SQL Injection detection," *Proceedings of the ACMSE 2018 Conference*, 2018. doi:10.1145/3190645.3190670

[12] Chen, Zhiyan, et al. "Machine Learning-Enabled IoT Security: Open Issues and Challenges under Advanced Persistent Threats." ACM Computing Surveys, 19 Apr. 2022, https://doi.org/10.1145/3530812.

[13] Faker, O., & Dogdu, E. (2019). Intrusion detection using big data and Deep Learning Techniques. *Proceedings of the 2019 ACM Southeast Conference*. doi:10.1145/3299815.3314439

[14] M. Zaman and C. -H. Lung, "Evaluation of machine learning techniques for network intrusion detection," NOMS 2018 - 2018 IEEE/IFIP Network Operations and

Management Symposium, Taipei, Taiwan, 2018, pp. 1-5, doi: 10.1109/NOMS.2018.8406212.

[15] M. Baich, T. Hamim, N. Sael, and Y. Chemlal, "Machine learning for IOT based networks Intrusion Detection: A Comparative Study," *Procedia Computer Science*, vol. 215, pp. 742–751, 2022. doi:10.1016/j.procs.2022.12.076

APPENDIX

- Effort distribution of the student as shown below as example:

QUID: 201801406	STUDENT NAME: Aqila Khatoon	Effort given: 33.3%
QUID: 201802829	STUDENT NAME: Nirvana Aladal	Effort given:33.2%
QUID: 201902903	STUDENT NAME: Meriem Boussaa	Effort given:33.3%