ACADEMIA International Journal for Social Sciences
Volume 4, Issue 4, 2025 ISSN-L (Online): 3006-6638

Assessing Cyber Threat Resilience in IoT Networks through Machine Learning–Based DDoS Detection

Engr. Mahad Rehman Tariq
mahadrjofficial@gmail.com
BSc. Electrical Engineering (Computer Systems), Department of Electrical Engineering, NFC Institute of Engineering and Technology, Multan, Pakistan

Engr. Manal Azhar
manalazhar31@gmail.com
BSc. Electrical Engineering (Computer Systems), Department of Electrical Engineering, NFC Institute of Engineering and Technology, Multan, Pakistan

Engr. Muhammad Nabeel
nabeelrajpoot1514@gmail.com
BSc. Electrical Engineering (Computer Systems), Department of Electrical Engineering, NFC Institute of Engineering and Technology, Multan, Pakistan

Engr. Hamza Mukhtar
hamzasail329@gmail.com
BSc. Electrical Engineering (Computer Systems), Department of Electrical Engineering, NFC Institute of Engineering and Technology, Multan, Pakistan

Engr. Hafiz Zeeshan Ahmad
zeeshebhai48@gmail.com
BSc. Electrical Engineering (Computer Systems), Department of Electrical Engineering, NFC Institute of Engineering and Technology, Multan, Pakistan

Syeda Fizza Bukhari
fizzanaqvi184@gmail.com
BS Computer Science, Department of Computer Science, Virtual University of Pakistan
Corresponding Author: * Engr. Mahad Rehman Tariq mahadrjofficial@gmail.com

Received: 13-10-2025 **Revised:** 09-11-2025 **Accepted:** 05-12-2025 **Published:** 26-12-2025

ABSTRACT

The fast increase in Internet of Things (IoT) networks has made them susceptible to DDoS attacks, which are capable of disrupting its communication and reducing system availability. The work explores machine learning- based DDoS attack detection and compares the performance of Support Vector Classifier (SVC), K-Nearest Neighbors (KNN), Naive Bayes, Random Forest, and an Ensemble approach. Experimental evidence demonstrates that SVC and Random Forest performed highly in balanced classification and lower reliability was obtained with Naive Bayes though computationally inexpensive. Ensemble model was able to outperform all the individual classifiers, and was more robust with a combination of individual classifier strengths. These results underscore Ensemble learning as a better and dependable method of mitigating DDoS attacks in IoT systems.

Keywords: *Machine Learning, DDos, IoT Networks, Cyber Threats*

INTRODUCTION

The increasing integration of Internet of Things (IoT) devices into environments that are residential, industrial, and public has introduced convenience along with a new era in connectivity. However, IoT networks have been exposed to a variety of cybersecurity threats through this rapid adoption. One of the most critical challenges is Distributed Denial of Service (DDoS) attacks, which are among the most common types of attacks. IoT systems are overwhelmed by these attacks using excessive traffic, causing service degradation or network failure. To avoid such attacks, it is important to ensure that the mechanisms are reliable and dependable in terms of IoT deployments. This problem can be solved in the project entitled "Detection of DDoS Attacks in IoT Devices using Machine Learning. It aims to offer an effective platform in order to monitor suspicious traffic to IoT settings. Due to its great precision in detecting and raising red flags about possible DDoS attacks, the project incorporates real time packet capturing and machine learning-driven analysis. Wireshark, which is a popular packet sniffing tool, was used in this work to trace and capture network traffic of IoT devices. Preprocessed captured data were used to train a variety of machine learning algorithms. The classifiers chosen to use in the task are Naive Bayes, Support Vector Classifier (SVC), Random Forest, and K-Nearest Neighbors (KNN). All the selections were determined by the ability to detect network intrusions and its applicability in IoT space. The distinctive strength of each algorithm on the detection process allows the achievement of a robust adaptive solution.

Naive Bayes is a simple, probability-based algorithm, which confers it with simplicity which is why it is suitable in the analysis of high-dimensional network traffic. It operates under the assumption that every feature is independent and approximating the probability of traffic being malicious or safe. It is very handy especially in the real-time aspect with the IoT systems based on its speed and efficiency.

Support Vector Classifier (SVC) aims at identifying the optimal boundary between two classes hence effective in the separation of normal and malicious traffic. Its power is that it allows forming a distinct distinction between categories, which is also helpful to process the intricate traffic patterns in IoT settings.

One of the ensemble techniques is the Random Forest that constructs several decision trees and sums up their results in order to increase the classification accuracy. It is extremely resilient to overfitting and can even tell which characteristics have the greatest impact on the recognition of DDoS attacks, providing information about potential risks that are not obvious in the network traffic.

K-Nearest Neighbors (KNN) operates by contrasting a data point with its nearest neighbours and distance is used to identify abnormal behaviour. It is a non-parametric, simple strategy that is likely to work well in cases where data about attacks are in recognizable patterns or clusters.

The algorithms were evaluated and contrasted on the basis of their speed, precision and adaptability to various attacks in an IoT network. It was desired to leverage the distinctive capabilities of both methods to create a powerful and scalable DDoS detection system that will be able to work with the constraints of IoT infrastructure.

The reason as to why we selected this project is due to the increasing cases of DDoS attacks that specifically target the IoT devices which in most cases have limitations in processing power as well as memory. Common cybersecurity offerings are often too resource-heavy and are not ideally suited to real-time security in these limited settings. This has created a gaping hole in the existing state of security - one that requires smarter and lighter, and more adaptive security. To solve this, we will integrate machine learning with real time traffic, and we will provide a lightweight but efficient solution to early detection and mitigation of DDoS attacks in the IoT networks. Such a hybrid design is not only more accurate and

responsive in detecting, but also resource-efficient, which is why it is best suited to IoT usage. We intend to protect the IoT ecosystems without compromising their performance and efficiency- a crucial fact in an environment where devices have limited memory, processing units, and power.

The rest of this report is organized as follows: Security threats in IoT are discussed in Section 2. Formation of IoT Botnets and Their Role in DDoS Attacks is discussed in Section 3. Methodology is detailed in Section 4. Algorithms and Equations are covered in Section 5. In Section 6, Results and comparisons are discussed. Finally, Section 7 concludes the report and suggests future directions.

Security Threats in IOT Environments

Internet of Things (IoT) devices have radically changed the way we live, work, and engage with technology but at the same time has presented a real security threat. Since they are commonly intended to be low-weight and inexpensive, these devices tend to have little processing ability and insignificant in-built protection. This exposes them to be an easy prey of cybercriminals.

Starting with Distributed Denial of Service (DDoS) attacks, which overwhelm network with traffic, to unauthorized access and passive listening to unencrypted data, the list of potential threats is long and continues to grow. Most IoT devices continue to use weak or default passwords, old software or send sensitive data without encryption. Such neglect exposes and opens both individual data and important system functionality to cyberattacks.

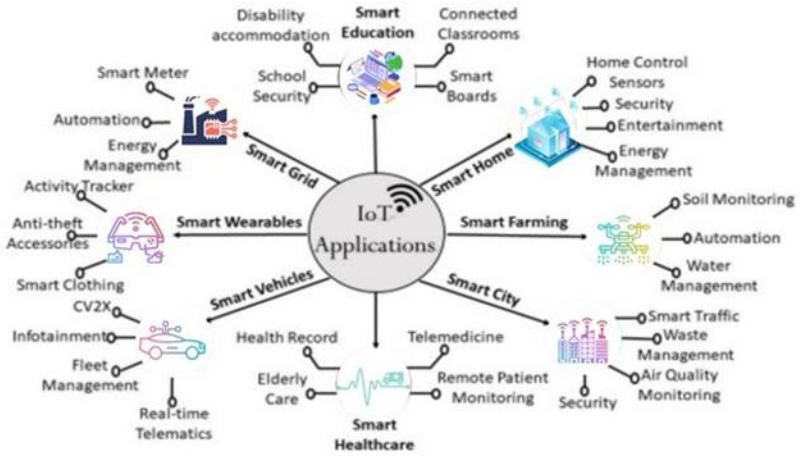

Figure 1: IOT Devices

Types of Attacks on IoT Devices

IoT devices are gaining popularity in our everyday life, and their convenience acquired a grave disadvantage: they are extremely prone to cyberattacks. Be- cause they are frequently highly distributed, have a low processing power, and are configured with minimal security, they are an easy target by hackers. A Distributed Denial of Service (DDoS) attack is among the most common types of threat: attackers employ a network of infected systems to overwhelm a server or a computer system with traffic, which slows it down.

Other threats are less evident, yet equally threatening. Man-in-the-Middle (MitM) attacks are those that hackers intercept and alter information that is being transferred between devices without raising any concern. The other key issue is eavesdropping, which is particularly prevalent when no encryption is

used, so delicate data can be easily intercepted. Attacks can also be made to use software vulnerabilities to inject malware codes or hijack firmware to have access to both the device and the data.

The other trick is replay, where the hackers intercept legitimate pieces of data transmitted, and retransmit them to cause a device to act in the wrong way. And not only digital attacks, physical attacks into devices without tamper protection can provide attackers with immediate access to stored information or system controls.

All these increasing threats leave one thing undisputed, IoT systems require more than simple protection. These prone networks need a robust multi-layered security strategy that would guard against the constantly changing cyber threats.

Challenges of IoT Security Threats

With the IoT gadgets becoming more and more integrated in our homes, industries, and even smart cities, security risks are increasing at an equal pace. They are frequently made small and efficient which implies that they have constrained processing power and memory. Due to that, they cannot easily manage the types of more powerful systems which use traditional, resource intensive security solutions.

The other significant problem is that regular updates of the firms are not done on many IoT devices. This exposes them to established weak areas over extended durations of time- basically providing hackers with more time and room to attack. To add to that, there is even no common standard of securing the IoT devices and, considering that there are already billions of devices all over the world, the scale of an issue is enormous.

The result? An enormous space of attack points that cybercriminals are keen to take advantage of. Since DDoS attacks that cause a service to crash have become a staple, so have spoofing and data breaches that steal personal or sensitive data, IoT networks have become the focus of the modern threat environment.

Machine Learning-Based Solution for IoT Security Challenges

To help address the increasing security risks in the IoT setting, our project is more intelligent and adaptive as it employs machine learning (ML) as an efficient mech- anism to identify DDoS attacks. Conventional cybersecurity tools do not tend to fit well with IoT devices- they are far too resource-consuming and require complex encryption or detection mechanisms often out of reach of most IoT devices, since they have limited processing capabilities.

Our solution is targeted at lightweight ML algorithms that are fast and effective and can analyze network traffic in a real-time with the least effect on system performance. With the help of the popular packet sniffing tool Wireshark, we gather live network traffic of the IoT devices and feed it to different types of ML models to be trained and tested. They are Naive Bayes, Support Vector Classifier (SVC) and random forest and K-Nearest Neighbors (KNN).

All these algorithms have their own advantages, and they are selected on the basis of their advantageous points, processed by huge data amounts, detection of unusual traffic traces, or rapid decision-making. The combination of them creates an efficient system of detection capable of identifying DDoS attacks before they appear and evolves to meet new forms of threats as they arise. This is what makes our approach not only correct and responsive at one end but also scalable and viable at the other end to secure the ever growing IoT ecosystems of today.

Formation of IoT Botnets and Their Role in DDoS Attacks

There is a tendency of cybercriminals exploiting weakly-secured Internet of Things (IoT) devices to create large botnets that they employ to conduct Distributed Denial of Service (DDoS) attacks. Everything begins with the attacker searching the internet to find vulnerable IoT devices- devices such as smart cameras, home routers, connected cars, or even medical monitoring devices. Unprotected these devices are easy targets.

After the identification, attackers use malicious code to silently infect these devices and make them remote-controlled bots. With time they accumulate a huge number of such compromised machines, referred to as a botnet. When the botnet is prepared, all these devices are ordered by the attacker to flood a particular server or web site simultaneously.

This leads to the server being overloaded and is unable to cope with the flood of non-authentic requests and the service is not able to be used by verified users. Most of the time the server goes down.

Such an attack shows the severity of the system security threats of IoT. Normal, manageable traffic is caused by ordinary users but the botnet causes a tsunami of malicious requests. Sightseeing this difference would make it obvious how harmful the IoT devices are when compromised. This is why the practice of high security and early warning systems in the networks of IoT is more significant than ever.

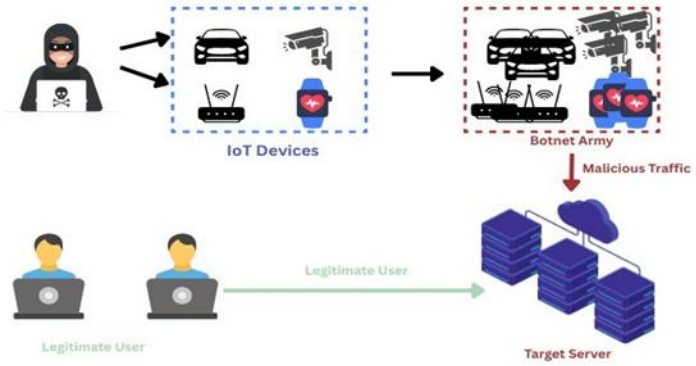

Figure 2: Formation of IoT Botnets

METHODOLOGY

This study presents a carefully developed machine learning architecture that will be used to detect and categorize Distributed Denial of Service (DDoS) attacks on Internet of things (IoT) systems. The security of connected systems has gotten harder as an increasing number of devices are sending traffic over them. To address this, we have a hybridization of classical machine learning models and contemporary data-driven approaches to address the scale and complexity of the current network environments.

The workflow of the proposed system is quite straightforward and logical: the system begins by gathering raw network data, proceeds to preprocess and clean it to make it accurate. At that point, it identifies meaningful features that can be used to identify normal and malicious activity. These characteristics are trained to various machine learning algorithms and the performances are then tested and optimized. Figure 1 shows a graphical representation of this whole process and how the system is trained as well as the real-time operation of the system to identify attacks.

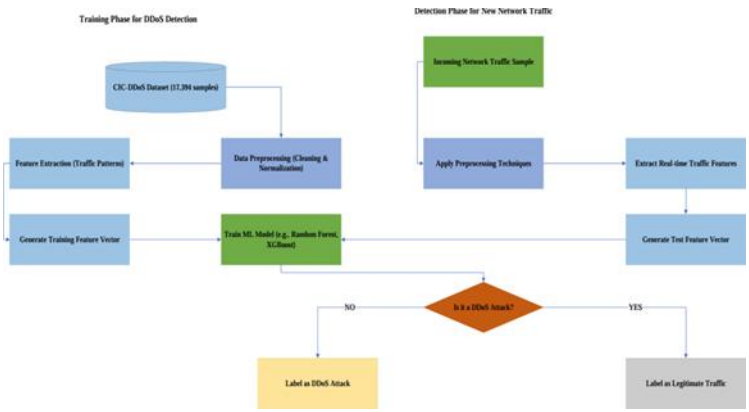

Figure 3: Methodology

Data Collection

This paper used the CIC-dDoS2019 dataset that has been compiled by the Cana- dian Institute of Cybersecurity (CIC) as a privacy source and an effective and practical base of network traffic analysis. This dataset is especially the most appropriate to use machine learning because it has an equal representation of normal and malicious traffic, which are marked accordingly to be used to properly train and test models.

The dataset is comprised of 279 distinct features and covers over 17,000 distinct instances of traffic flows, which is a valuable source of information about different methods of DDoS attacks. Some of the attacks modeled include UDP floods, TCP SYN floods, and HTTP GET floods, which are the case on the ground. The data breadth and depth allow developing machine learning models that can be not only accurate but also not limited to various types of threats. This renders it a powerful resource to build reliable security solutions specifically designed to fit IoT networks.

Data Preprocessing

The uncleaned dataset had to be cleaned with care before it was trained as it contained noise, duplicate records and gaps. In order to resolve these problems, we conducted an organized preprocessing stage. This entailed the elimination of superfluous or unrelated columns, the handling of any empty or null entries and a normalization procedure to have all the numeric variables on the same scale. Also, categorical data was appropriately coded to be applicable in the machine learning algorithms.

This standardization of the dataset allowed us to allay the concerns of having the different data samples in different formats that could be inconsistent. Not only did this contribute to the enhancement of the precision of the models but also provided a strong basis to the successful feature extraction and training. A well-cleaned and prepared dataset is a fundamental requirement of any credible detection system and this measure was important in laying the groundwork to high performance results.

Feature Selection and Dimensionality Reduction

Because network traffic data contains many attributes, it was necessary to do feature selection so that we will not overfit our models and the computation will not be as difficult. We concentrated on the extraction of features which are highly relevant to network behavior- consisting of packet size and time between packets, session duration and protocol specific flags.

In order to find the most influential attributes, we conducted a rigorous sta- tistical analysis of such methods as correlation analysis and recursive feature elimination. These techniques assisted us in

reducing the set of features to those that added the most to the separation of normal traffic and DDoS activity. Such a reduction of the dataset allowed us to create a more effective and precise model, which could identify threats without causing excessive load on system resources.

Algorithms and Equations

Naive Bayes

Where: $$P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)} \quad (1)$$

P (A|B) is the posterior probability of class A (e.g., DDoS or normal) given features. B.

P (B|A) is the probability of features in the case of the class.

P (A) is the prior probability of the class.

P (B) is the probability of features.

Theory & Practical Use:

Naive Bayes operates under the assumption that all features are independent of each other- an assumption that is hardly true in reality yet it works reasonably well in practice.

It is simple and thus can make extremely fast calculations and it is suitable in an environment where devices are limited in their processing power, such as an IoT system.

This algorithm has the capability of swiftly identifying normal traffic and potentially harmful incoming traffic and this makes it viable as a threat detecting algorithm in real-time.

Although it is not always more efficient than more complicated models, it is a great starting point in terms of comparing performance of various algorithms.

k-Nearest Neighbors (kNN)

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \quad (2)$$

Theory & Application:

K-Nearest Neighbors (KNN) is a straightforward and yet effective method that is based on the instance-based learning.

In place of constructing the classic framework, KNN categorizes a novel data point in reference to the k nearest points in the assembly and allocates the most frequent name to them.

It is as though a set of close data points are asked to vote on what the new point is to be identified as.

Since it does not have an actual training step, KNN is especially practical in cases where the dataset is small or rapid, on-the-fly decisions are required- like in certain real-time IoT applications.

Nonetheless, the algorithm may be susceptible to irrelevant or noisy data, thus the need to preprocess the algorithm such as normalization is usually required to enhance its accuracy.

It is also important to select the value of k; either by making it too small or too large it will decrease performance.

KNN is particularly handy in the detection of suspicious activity as it in- volves the comparison of the suspicious activity against patterns that are already known to be related to DDoS attacks.

It is strong in that it is able to spot any slight anomalies that could otherwise be missed in more complicated models.

Random Forest

- Ensemble of decision trees using bootstrap aggregation (bagging).
- Majority vote from multiple trees determines the final prediction.

$$G(t) = 1 - \sum_{i=1}^{C} p_i^2 \quad (3)$$

In the formula, p_i is the probability of the data point in class i at node t.

Theory & Application:

- Random Forest is a superior ensemble learning algorithm that develops a collection of decision trees and integrates their predictions to achieve more precise forecasts.
- All the trees in the forest are then trained on a random subset of the data- a process called bagging- and the ultimate outcome is obtained by majority vote among all the trees.
- It is particularly effective with large datasets, a large number of features and non-linear relationships.
- Among the most important benefits of the Random Forest is that it is less prone to overfitting; the model is based on the aggregated judgement of the entire forest as opposed to the judgement of a single tree and is likely to be more effective in prediction when it is tested on unseen data.
- Random Forest is especially suitable on cybersecurity and activities such as DDoS detection.
- It is able to filter complicated traffic logs, establish abnormal behavioral patterns, and pinpoint the features that are most likely to predict attacks.
- It can identify the slightest anomalies in large amounts of data, which makes it an effective option in the protection of IoT networks.

Support Vector Classifier (SVC)

$$\mathbf{w} \cdot \mathbf{x} + b = 0 \quad (4)$$

$$\min_{w,b} \frac{1}{2}\|\mathbf{w}\|^2 \quad \text{subject to } y_i(\mathbf{w} \cdot \mathbf{x}_i + b) \geq 1 \quad (5)$$

Theory & Application

Support Vector Classifier (SVC) is a formidable machine learning algorithm that is notable in its accuracy in dealing with challenging classification issues.

It is especially useful when high dimensional data, e.g. the fine-grained features present in network traffic, are considered, where it is ideally adapted to cybersecurity applications.

The distinguishing feature of SVC is that it identifies the most appropriate boundary (or hyperplane) that best differentiates among various classes in this case, normal traffic and DDoS attacks.

When the data cannot be separated linearly, SVC can still be effective by subjecting the data to higher-dimensional representation with the help of the kernel functions, including the radial basis function (RBF), after which the data can be separated.

SVC particularly works where there is a very distinct line between normal and malicious behavior.

It has demonstrated strong potential in detecting sophisticated or zero-day DDoS attacks—those not previously encountered—when trained on representative data.

Its ability to adapt to subtle variations in traffic patterns makes it a reliable tool for countering evolving threats in IoT networks.

RESULTS

In order to compare the performance of the different classification algorithms we experimented with five models that are: Support Vector Classifier (SVC), K-Nearest Neighbors (KNN), Naive Bayes, Random Forest, and an Ensemble method. Figure 4 shows the accuracy of each model.

The accuracy of SVC was at a very high level of about 0.87; this indicates that it performs well in the classification task.

KNN was close behind it with a value of approximately 0.85, which implies that it is useful in the creation of local trends within the data.

Naive Bayes on the other hand provided much lower accuracy of 0.73 indi- cating that the data distribution might not be suitable to its assumptions.

The accuracy of Random Forest was about 0.87, which is equal to those of SVC and indicates its strength as an ensemble procedure.

The Ensemble approach (formerly referred to as Hybrid) was marginally better than the single models with the best accuracy of around 0.88. This confirms the benefit of using multiple classifiers in order to exploit their respective strengths. These findings reveal that although individual classifiers like SVC and the Random Forest are good, Ensemble model offers a slight increase in performance which demonstrates the advantage of integrating models in enhancing classification accuracy.

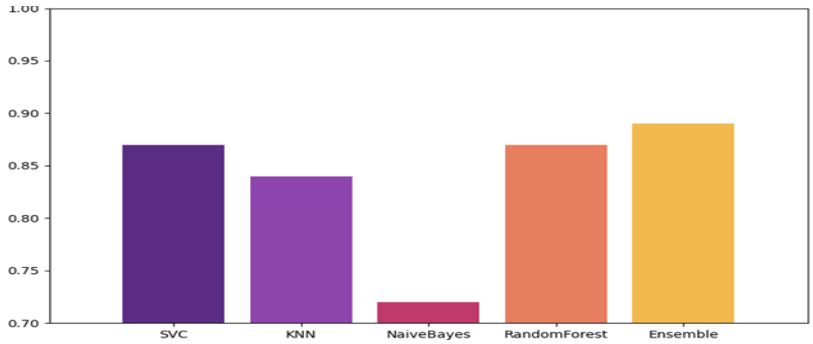

Figure 4: Accuracy Comparison with Ensemble Model

To supplement the accuracy tests, confusion matrices were also performed on each of the classification models in order to gain further understanding of predictive ability of the models. These matrices provide a dissection of the correct and incorrect predictions of each of the classes, and True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN).

Support Vector Classifier (SVC)

The confusion matrix of the SVC model gave 55 true negatives and 32 true positives and 6 false positives and 7 false negatives. These findings indicate the high precision of the model to both detect the positive and the negative cases, with a rather equal ratio of errors. The small misclassification rates show that SVC is generalizable to the dataset.

K-Nearest Neighbors (KNN)

KNN reached 51 true negatives and 32 true positives with 10 false positives and 7 false negatives. Its accuracy in predicting the positive class was identical to that of SVC but its higher false positive rate indicates that KNN is more likely to label a negative sample as positive which might occur because of local decision boundaries created by noise or overlapping classes.

Naive Bayes

Naive Bayes was the worst in performance with 48 true negatives and 23 true positives, and the most number of error (13 false positives and 16 false negatives). This poor performance can be attributed to the conditional independence assump- tion of the model that is not well satisfied by the given dataset, thus the model is unable to capture feature relationships well and to this effect the classification performance is also not good.

Random Forest

Random Forest had the best performance regarding the individual classifiers with 56 true negatives and 32 true positives. It produced a record of 5 false positives and 7 false negatives with the ideal trade off between specificity and sensitivity. These findings underscore the power of the Random Forest to support the interaction between features in a complicated way by the combination of decision trees.

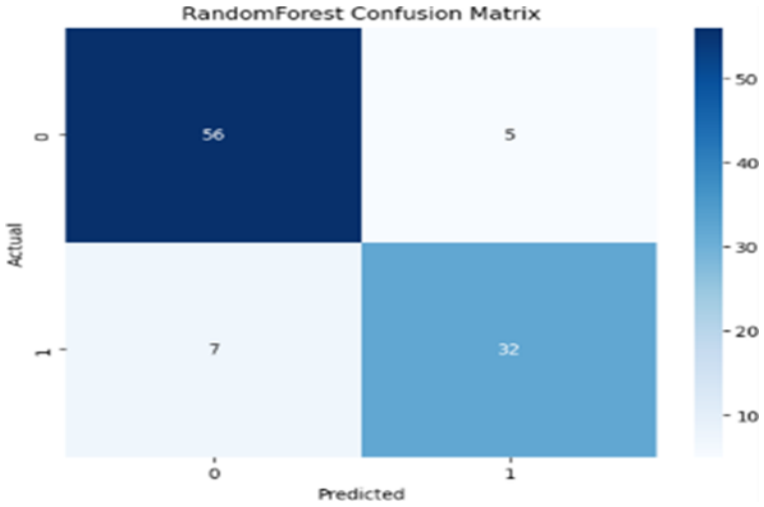

Figure 5: Performance metrics for Random Forest classifier

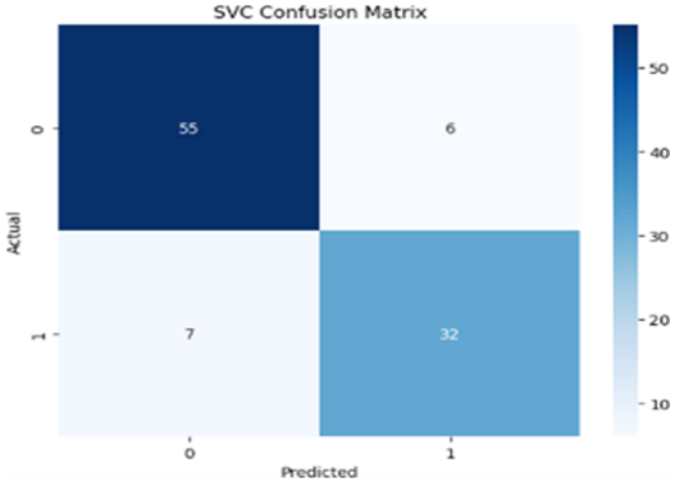

Figure 6: Performance metrics for Support Vector Classifier (SVC)

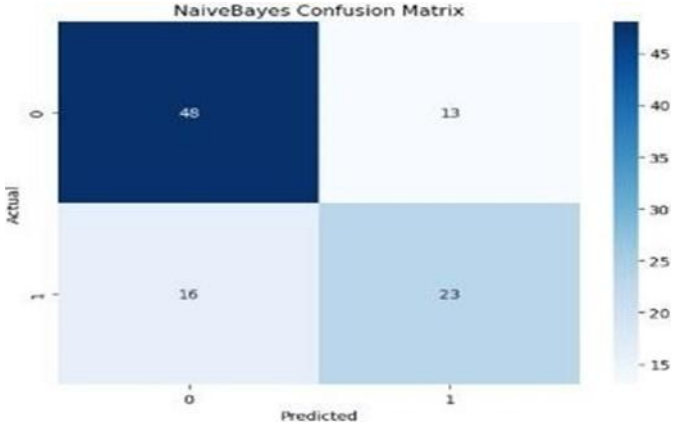

Figure 7: Performance metrics for Na¨ıve Bayes classifier

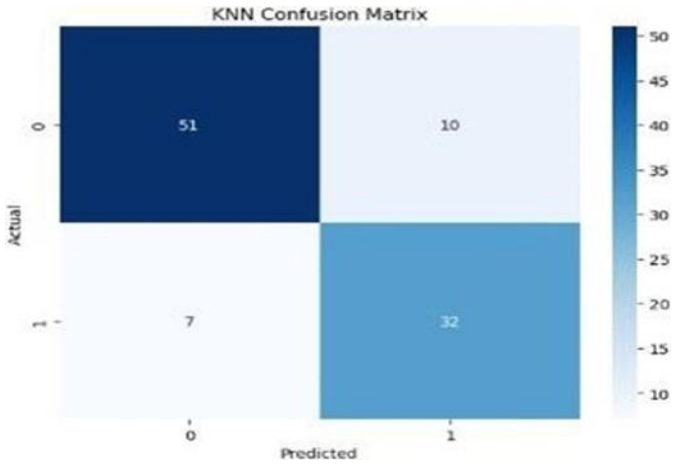

Figure 8: Performance metrics for K-Nearest Neighbors (KNN) classifier

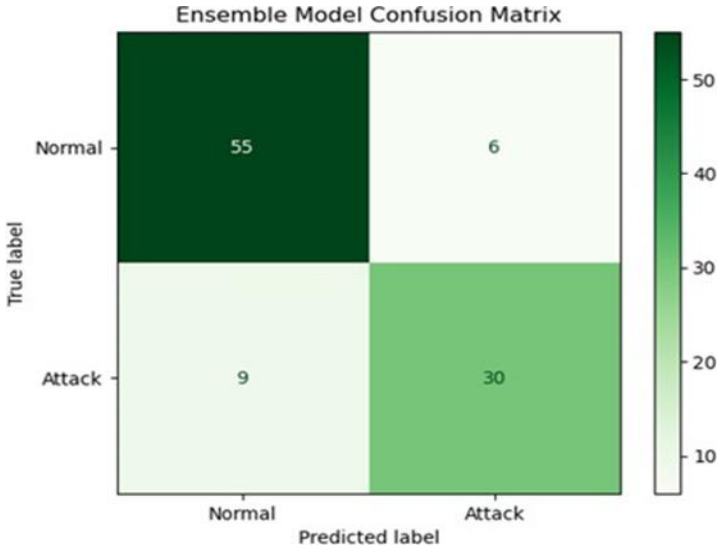

Figure 9: Performance metrics for Ensemble Model classifier

CONCLUSION

In this paper, all these machine learning classifiers, Support Vector Classifier (SVC), K-Nearest Neighbors (KNN), Naive Bayes, Random Forest, and an Ensemble method, were tested based on accuracy scores and analysis of confusion matrices. Random Forest and SVC were among the individual models that showed the best performance with a high accuracy level and balanced classification be- tween both classes. Naive Bayes was computationally simple; however, it was considerably less accurate and more misclassified, which is why it was less applicable to the analyzed dataset.

The best overall accuracy was obtained with the Ensemble model which combined the strengths of several classifiers and thus slightly better than all the individual models. This reinforces the ability of an ensemble learning to increase or improve predictive performance by minimizing both bias and variance.

Overall, the findings highlight that though individual classifiers may do a good job, particularly the Random Forest and the SVC, the Ensemble method is better placed to offer a more reliable and robust way of carrying out classification activities.

KEY TAKEAWAYS & RECOMMENDATIONS

- Random Forest SVC stood out – delivering the best individual accuracy and balanced classification.
- Naive Bayes fell short – fast but less accurate, making it unsuitable for this dataset.
- Ensemble learning led the way – combining models gave the most reliable and robust performance

FINAL STATEMENT

Altogether, this research reveals that the Ensemble approach is the strongest and most reliable, whereas the individual one like Random Forest and SVC offers high accuracy and balanced classification, whereas Naive Bayes offers easy computations but reduced reliability. The Ensemble method minimizes bias and variance by using the combination of several algorithms, thereby producing more reliable results. In an IoT smart home network, where various devices produce a variety of traffic patterns, a single classifier could not be able to identify some attack patterns. Nevertheless, Ensemble model has the potential to combine high-performance of various algorithms, which will render it more efficient in detecting and preventing DDoS attacks in the real environment.

REFERENCES

Bala, Bindu, and Sunny Behal. "AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges." Computer Science Review, vol. 52, 2024, p. 100631.

Pakmehr, Amir, et al. "DDoS attack detection techniques in IoT networks: a survey." Cluster Computing, vol. 27, no. 10, 2024, pp. 14637–14668.

Modi, Pavitra. "Towards Efficient Machine Learning Method for IoT DDoS Attack Detection." arXiv preprint arXiv:2408.10267, 2024.

Khanday, Shahbaz Ahmad, Hoor Fatima, and Nitin Rakesh. "Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks." Expert Systems with Applications, vol. 215, 2023, p. 119330.

Kumari, Pooja, and Ankit Kumar Jain. "A comprehensive study of DDoS attacks over IoT network and their countermeasures." Computers & Security, vol. 127, 2023, p. 103096.

Ahsan, Mostofa, et al. "Cybersecurity threats and their mitigation approaches using Machine Learning—A Review." Journal of Cybersecurity and Privacy, vol. 2, no. 3, 2022, pp. 527–555.

Aslan, O¨ mer, et al. "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions." Electronics, vol. 12, no. 6, 2023, p. 1333.

Salman, Ola, et al. "A machine learning based framework for IoT device identification and abnormal traffic detection." Transactions on Emerging Telecommunications Technologies, vol. 33, no. 3, 2022, p. e3743.

Benlloch-Caballero, Pablo, Qi Wang, and Jose M. Alcaraz Calero. "Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks." Computer Networks, vol. 222, 2023, p. 109526.

Khader, Rozan, and Derar Eleyan. "Survey of dos/ddos attacks in iot."Sustainable Engineering and Innovation, vol. 3, no. 1, 2021, pp. 23–28.

Al-Begain, Khalid, et al. "A DDoS detection and prevention system for IoT devices and its application to smart home environment." Applied Sciences, vol. 12, no. 22, 2022, p. 11853.

Lee, Shu-Hung, et al. "Detection and prevention of DDoS attacks on the IoT." Applied Sciences, vol. 12, no. 23, 2022, p. 12407.

Alshahrani, Mohammed Mujib. "A Secure and intelligent software-defined networking framework for future smart cities to prevent DDoS Attack." Applied Sciences, vol. 13, no. 17, 2023, p. 9822.

Ogini, Nicholas Oluwole, Wilfred Adigwe, and Noah Oghenefego Ogwara. "Distributed denial of service attack detection and prevention model for IoT- based computing environment using ensemble machine learning approach." International Journal of Network Security & Its Applications (IJNSA), vol. 14, no. 4, 2022, pp. 39–53.

Hnamte, Vanlalruata, and G. Balram. "Implementation of Naive Bayes Classifier for Reducing DDoS Attacks in IoT Networks." Journal of Algebraic Statistics, vol. 13, no. 2, 2022, pp. 2749–2757.

Ghali, Abdulrahman Aminu, Rohiza Ahmad, and Hitham Alhussian. "A framework for mitigating DDoS and DOS attacks in IoT environment using hybrid approach." Electronics, vol. 10, no. 11, 2021, p. 1282.

Avcı, I˙sa, and Murat Koca. "Predicting ddos attacks using machine learning algorithms in building management systems." Electronics, vol. 12, no. 19, 2023, p. 4142.

Cherian, Mimi M., and Satishkumar L. Varma. "Mitigation of DDOS and MiTM attacks using belief based secure correlation approach in SDN-based IoT networks." International Journal of Computer Network and Information Security, vol. 14, no. 1, 2022, pp. 52.

Sharma, Deepak Kumar, et al. "Anomaly detection framework to prevent DDoS attack in fog empowered IoT networks." Ad Hoc Networks, vol. 121, 2021, p. 102603.

Shah, Zawar, et al. "Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey." Sensors, vol. 22, no. 3, 2022, p. 1094.

Ibrahim, Rahmeh Fawaz, Qasem Abu Al-Haija, and Ashraf Ahmad. "DDoS attack prevention for internet of thing devices using ethereum blockchain technology." Sensors, vol. 22, no. 18, 2022, p. 6806.

Almaraz-Rivera, Josue Genaro, et al. "Toward the protection of IoT networks: Introducing the LATAM-DDoS-IoT dataset." IEEE Access, vol. 10, 2022, pp. 106909–106920.

Shafiq, Muhammad, et al. "The Rise of 'Internet of Things': Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks." Wireless Communications and Mobile Computing, vol. 2022, no. 1, 2022, article ID 8669348.