Kashf Journal of Multidisciplinary Research
Vol: 02 - Issue 3 (2025)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

STRENGTHENING IOT SECURITY WITH MACHINE LEARNING-BASED ANOMALY DETECTION AND ADAPTIVE DEFENSE MECHANISMS

Aqib Masood Ahmad
Department of Computer Science, NFCIET, Multan, Pakistan
Naeem Aslam
Department of Computer Science, NFCIET, Multan, Pakistan
Muhammad Kamran Abid*
Department of Computer Science, NFCIET, Multan, Pakistan
Yasir Aziz
Department of Computer Engineering, BZU, Multan, Pakistan
Muhammad Fuzail
Department of Computer Science, NFCIET, Multan, Pakistan
Nasir Umar
Department of Computer Science, NFCIET, Multan, Pakistan
Talha Farooq Khan
Department of Computer Science, USP, Multan, Pakistan

Corresponding author: Muhammad Kamran Abid (kamran.abid@nfciet.edu.pk)

Article Info

Abstract

This paper highlights the growing cybersecurity challenges resulting from the growing use of Internet of Things (IoT) devices. With an emphasis on the advancement of IoT security, the study employs adaptive defensive mechanisms and machine learning-based anomaly detection as proactive strategies to combat present and potential cyber threat sources. The graphic highlights the importance of having infrastructures with robust security mechanisms in place to secure connected devices and explains the Internet of Things' fast expansion. IoT security statements draw attention to the IoT's hidden vulnerabilities and threats; in these cases, state-of-the-art security measures are beneficial. Through the use of adaptive defense mechanisms and machine learning anomaly detection, the objectives center on improving IoT security.

The data sources, preprocessing tasks, Random Forest, Decision Tree, SVM, and Gradient Boosting algorithms selected for anomaly detection are described in the methodology section. The integration of the adversary negotiating function and self-adaptive protection mechanisms strengthens information technology ecosystems that can simplify dynamically. In addition to providing metrics for accuracy, precision, and recall, the results and discussion section assesses the efficacy of the selected machine learning models. The most significant finding is that 89.34% more precision is achieved with gradient boosting. It has been demonstrated that the most successful model is gradient boosting. The discourse includes an explanation of the results, an acknowledgement of the limitations, and a discussion of the major difficulties encountered in conducting the study. The conclusion restates the importance of machine learning in IoT security implementation in order to build a robust system that can adjust to counter ever-evolving cyberattacks and keep up with the changing trend of securing IoT through the connected world.

Keywords:
IoT, Machine Learning, Deep Learning, IOT Anomaly Detection

Introduction

The power of the Internet of Things (IoT) technology enabling IoT devices to communicate and share data unquestionably has had a pronounced impact on how we navigate through our daily lives. Nevertheless, this upsurge of cyber threats has twofold negative outcome – a complicated security environment and the presence of vulnerabilities. Particularly in these circumstances, therefore, this study aims to solve the acute problem of the enhancement of IoT safety with the help of Machine Learning application. Attack prevention and cybersecurity reinforcement via anomaly detection and adaptive defenses will be among our critical areas of focus in the quest to turn the IoT ecosystem into a strong infrastructure impenetrable of emerging cyber threats. Machine learning (ML) and deep learning (DL) are becoming indispensable techniques for resisting security risks as the Internet of Things (IoT) grows in popularity. This paper investigates the inner workings of various machine learning techniques, such as Convolutional Neural Networks (CNNs), Random Forests, and Support Vector Machines (SVMs). In the context of the Internet of Things, anomaly detection refers to the identification of unusual patterns or behaviors in data that depart from the expected norm. In the healthcare industry, anomaly detection is crucial since errors can have serious effects. Precision is essential[1].

The Internet of Things (IoT), which connects computer-based systems to the physical world, presents a bright future for technology that will boost productivity and generate profits. An implantable network of electronics, sensors, and software that allows devices to communicate and exchange data is known as the Internet of Things (IoT). Devices, home appliances, and automobiles are a few examples of these items [2]. You can contact any "thing" that is identified as a part of the Internet of Things over the internet. IoT has an impact on several industries, such as smart cities, healthcare, automotive, and logistics tracking. IoT device utilization is predicted to have an impact on all facets of human living.

Machine learning is a subfield within artificial intelligence. It is defined as a machine's ability to make predictions and decisions that resemble those of a person. Utilizing computer algorithms to learn from their surroundings in an effort to mimic human intelligence, the field of "machine learning" is a rapidly emerging field [3]. It enables more accurate outcome prediction for software programs. Neural networks, decision trees, Bayesian networks, and support vector machines are examples of machine learning algorithms.

The development of the IoT landscape over the last decade can be equated to a snowball that was propelled forward by different factors like advances in technology, decreasing IC prices, and the ever-increasing desire for connected solutions. Low-cost sensors, wireless connectivity, and cloud computing infrastructure are essential aspects of IoT technology. With their advent more and more people are getting access to IoT based devices which is a step forward towards the mass adoption of this technology within specific sector and industries.

Internet of Things technologies has challenged significantly been a game-changer in the transportation industry, enabling real-time tracking, monitoring, and optimization of transportations and traffic. From the smart cars installed in sensors and the navigation systems to intelligent transportation systems, IoT technology is proliferating the smart, safe, and convenient driving experience in urban mobility.

The spread and expansion of the IoT have the greatness to augment progress by involving innovative approaches, however, it, on the other hand, emanate some certain challenges and risks. The main ones would include issues linked to data security and privacy, information exchange, and how well this new initiative scales up. The of connected devices that become online also increases a possible surface area that malicious actors can take advantage of and then break data or information security.

Problem Statement

There has been a profound rise in the generation of data directly due to the ongoing IoT devices explosion but also in complexity in the connection of these devices. On the positive side, the multitude of devices and technologies are reducing the barriers for many individuals to engage in this new trend; but the fast growth also leads to a wide range of security challenges identified as a major threat to the secure and reliable functioning of the IoT ecosystems. Only conventional cybersecurity solutions sometimes cope with the fast and changing of cyber risks that emerge with the use of IoT devices. In the long run, there are many shortcomings, such as the imperfect ways of authentication, the lack of encryption mechanisms, and inadequate compliance to standardized security practices, which the case remains that unauthorized individuals exploit perceived weaknesses to initiate cyberattacks and thus causing disruption. Due to this reason, the security system of IoT devices needs improvement in order to well counter these issues and aid the interconnected devices to be resilient in the IoT world.

Literature Review

Insight into IoT is the security coverage summing up challenges and solutions in the domain. The platform for the security of the Internet of things can be referred to as the multi-faceted approach secured for the inter-connected sensors and the data they generate. The principal elements are authentication, encryption, and entrance control which serve the purpose of preserving confidentiality and integrity of data. Moreover, giving priority to secure device administration procedures along with timely software updates are also among the most effective methods to stay away from facing security risks[8]. Being aware of the security aspects specific to huge multitudes of devices, with limited resources, a holistic knowledge of controlling methods to suit the diverse environment should be obtained. This portion is going to help in understanding the very basic things concerning IoT security and put the reader on a steady footing ahead of a detailed exploration on machine learning powered anomaly detection and adaptive defense mechanisms[9].

IoT security domain is a wide field with a range of problems and issues on top of which considered is the communication between sensors and data they yield. At its core, the foundation of IoT threat model consists of multiple levels which are important for keeping information transmitted by IoT devices private, accurate, and accessible. Elements of IoT security include authentication, encryption, authorization control, secure device contract, and timely software update[11].

Identity verification processes of IoT devices and users play a decisive role in creating secure environment in IoT spaces. Utilization of robust authentication procedures, such as cryptographic keys and biometrics, will help reduce the threat of unauthorized access and information in this communication channel validity ascertain. Looking over, encryption techniques are also used to encrypt data in order to prevent data confidentiality and integrity during transition and while to be at rest, making sure that the sensitive information is not hacked during transition.

The web of IoT which is filled in with different kinds of threats and attacks each of which can have a great discourage the security and reliability of connected objects. As a result, context-aware attacks, data breaches, denial of service (DoS) attacks, man-in-the-middle attacks, eavesdropping, and even physical tampering are among the main techniques that tend to be used for IoT devices. Such attacks will target the deficiency of Internet of Things virtual network to breach regulators, falsify data, disrupt communication all channels and even compromise the secretive and even integrity of sensible data[14].

Resolution of these security issues has to be a top priority in order to guarantee a secure and stable environment of IoT systems. Machine learning with anomaly dynamical detection as well as adaptive defense tools are emerged as the new points for both of detection and mitigation but it is still not very clear that the application of them in real-time with capability of guaranty in response of emerging risks are efficient or they are not[15].

Machine learning algorithms stand out as a critical factor in securing IoT networks since these algorithms are capable of diverse activities like timely threats detection and smart defense procedures. Utilizing machine learning with big data analysis from vast and differed sources which are network traffic, device logs and external threat intelligence feeds, algorithms can detect patterns of malicious behaviors and predict security threats which might be beyond network boundaries[16].

Fueled by machine learning techniques, anomaly detection algorithms can be used to differentiate deviations from normal IoT working pattern among ecosystems, releasing signals that communicate potential dangers and consequently allowing organizations to proactively address threats[17]. The intelligent defense mechanisms adapt the security controls and the response strategies in real time by using machine learning algorithms and the best of threat intelligence to reply adequately to potential upcoming risks. So, the organization can reduce the effects of security incidents.

Methodology

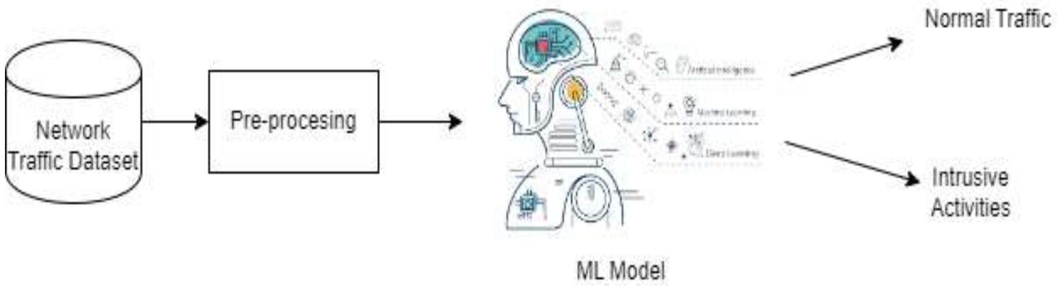


Figure 1: Anomaly detection using ML

Anomaly Detection:

Machine Learning in IoT whereby existing and modern machine learning approaches are to be evaluated. Addressing anomaly detection in the IoT ecosystems is among the biggest concerns in the sense ML algorithms are crucial in identifying, notifying and overcoming any possible security problems. In this section, we drill deeper into some widely used ML algorithms to identify irregularities, namely Random Forest, Decision Tree SVM, and Gradient Boosting Algorithm. Every algorithm out there offers some specific advantages and functionality and, as a whole, they are able to deal with the complex challenges faced in IoT.

Results & Discussion

Random Forest

Table 1: Random forest classifier report (10 iterations) – the machine learning algorithm used for classification tasks. The horizontal axes are those tube entries representing the traffic types which the model was trained on, and the vertical ones are the student marks of each class meeting.

Precision (Positive Predictive Value) is one of the parameters of accuracy level of the model in identifying the certain class. Another example for this is the precision score which can be 1.00 for "Attack class" which implies that all the examples which was identified as 'Attack' by the model were actually attacks.

Sensitivity or recall (True Positive Rate) is the measure of how appropriate the model is at recognizing all the relevant classes among the classes that it is supposed to find. A recall of 1.00 for "Attack" class indicates that all considering the attack cases in our data set have been recognized by the model. F1-Score is the harmonic mean of precision and recall and is applied to appraise the general sentiment of a model posing the right class.

Support is the number of the samples or instances of each class.

Attack" and "PartOfAHorizontalPortScan" traffic: The high precision (1.00) and recall (1.00) guard the model from the miss-identification for the above mentioned categories.

"C&C" and "DDoS" traffic: Nevertheless, the model shows bias against these types of classes with precision low (0.34 and 0.60 respectively) which indicates that very many examples of this traffic class was automatically invalidated as C&C or DDOS traffic.

Overall Accuracy: The accuracy of our model is of 81% which means that the traffic samples have been correctly classified in a ratio of 81%. While it is critical to take into account the class imbalance in the accuracy assessment, it is also vital to analyze unfair bias. This classifier in particular deals with the issue where many more samples are labeled as "Benign" compared to the other types. Thus, a model may acquire a shot at yielding such high accuracy that it would classify everything as benign - even if worse at seeing other kinds of traffic.

Weighted Average metrics usually re-scales the class so the properly size of the class imbalance and appear to give model performance a true picture. The weighted macro average precision is 0.82, the weighted macro average recall is 0.81, and the weighted macro average F1-score is 0.81.

	precision	recall	f1-score	support
Attack	1.00	1.00	1.00	756
Benign	0.83	0.82	0.83	5253
C&C	0.34	0.36	0.35	1111
DDoS	0.60	0.67	0.63	9
Okiru	0.95	0.65	0.77	31
PartOfAHorizontalPortScan	0.94	0.94	0.94	2441
Accuracy			0.81	9601
Macro Avg	0.78	0.74	0.75	9601
Weighted Avg	0.82	0.81	0.81	9601

Table 1: Classification Report Table for Random Forest

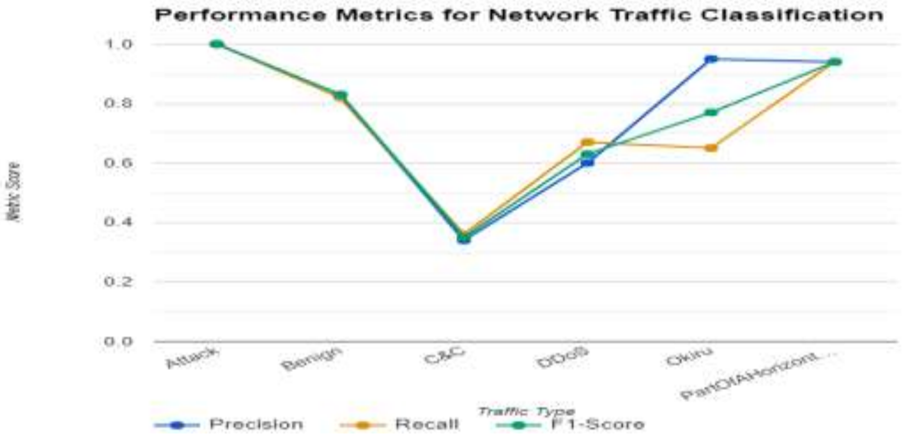


Figure 2: performance metrics

The table 1 presents the mark of a ML model in classifying the network traffic into 4 categories. This model scored 100% accuracy in classifying "Attack" and "PartOfAHorizontalPortScan" traffic but had only a 34% precision in "C&C" and a 60% precision on arresting "DDoS". The model is 81% in general, but it favors the normal traffic (more than half of the topics dealt with the benign traffic). Considering this imbalance, weighted metrics provide a better picture: With precision score of 82%, recall score of 81% our general performance is satisfying but being specific about traffic types lowers our results to a great extent.

Support Vector Machine Accuracy: 0.5472

Table 2: Classification Report table for Support Vector Machine

	precision	recall	f1-score	support
Attack	0.00	0.00	0.00	756
Benign	0.55	1.00	0.71	5253
C&C	0.00	0.00	0.00	1111

DDoS	0.57	0.44	0.50	9
Okiru	0.00	0.00	0.00	31
PartOfAHorizontalPortScan	0.00	0.00	0.00	2441
Accuracy			0.55	9601
Macro Avg	0.19	0.24	0.20	9601
Weighted Avg	0.30	0.55	0.39	9601

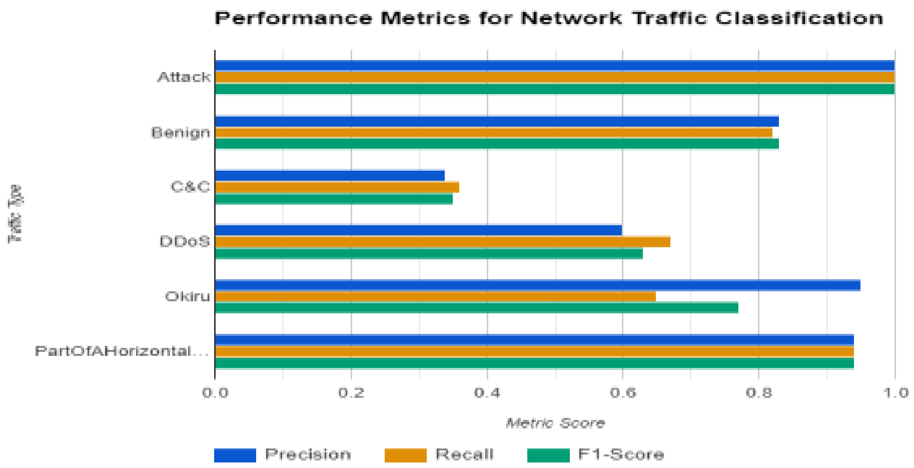


Figure 3: performance metrics for network traffic classification

High SVM error performances are revealed in the table 2 alongside the reduced accuracies compared with the last model. It not even once distinguishes imagined and real traffic labels as 'Attack', 'C&C', 'Okiru', and 'PartOfAHorizontalPortScan' (0% precision). Though the AUC is perfectly rounded, this might be the case because of the class imbalance (many samples fall in the positive side). The overall accuracy is a false figure, and weighted metrics, on the other hand, confirm the very underwhelming performance (precision 30%, recall 55%). Such underpinning needs more research or improvement.

Decision Tree Accuracy: 0.8165

Table 3: Classification Report for Decision Tree

	precision	recall	f1-score	support
Attack	1.00	1.00	1.00	756
Benign	0.83	0.84	0.83	5253
C&C	0.35	0.35	0.35	1111
DDoS	0.60	0.67	0.63	9
Okiru	0.91	0.65	0.75	31
PartOfAHorizontalPortScan	0.94	0.94	0.94	2441
Accuracy			0.82	9601
Macro Avg	0.66	0.63	0.64	9601

Weighted Avg	0.82	0.82	0.82	9601

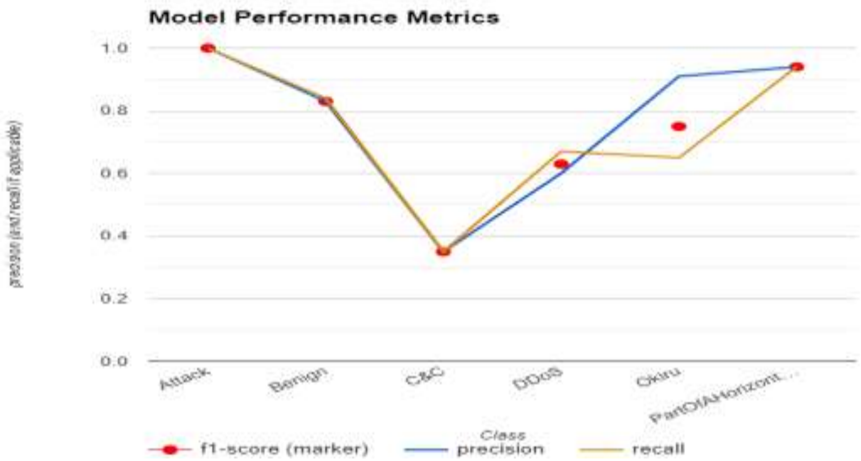


Figure 4: model performance metrics

In the Table 3, the decision tree also produces results similar to those of the random forest (as shown in the preceding example). It operationalizes the "Attack" and "PartOfAHorizontalPortScan" traffic very well (with a precision of 100%) and has a lower performance rate for the "C&C" and "DDoS" attacks around 35%. This can be seen by the large overall accuracy (82%) but again due to the class imbalance the weighted metrics (82 % precision and recall) provide fairer representation of the performance of this system, hence it can be good choice for network traffic classification

Gradient Boosting Accuracy: 0.8934

Table 4: Classification Report for Gradient Boosting

	precision	recall	f1-score	support
Attack	1.00	0.99	0.99	756
Benign	0.85	0.98	0.91	5253
C&C	0.99	0.31	0.47	1111
DDoS	0.50	0.44	0.47	9
Okiru	0.75	0.10	0.17	31
PartOfAHorizontalPortScan	0.96	0.95	0.96	2441
Accuracy			0.89	9601
Macro Avg	0.84	0.63	0.66	9601
Weighted Avg	0.91	0.89	0.87	9601

Gradient Boosting mini model gives great results and gains quite a lot of advantage in comparison with other previous versions as given in Table 4. It beats in this detection of categories "Attack," "Benign," and "PartOfAHorizontalPortScan" (precision above 95%, and recall above 90%). In terms of "C&C" and "DDoS" difficulties, the model fails to keep up (lower precision), but it is far more effective than the models with 99% and 50% precision, respectively. Considering the degree of imbalance in our classes, we achieve good results with the weighted metrics (91% precision, 89% recall) that capture the overall performance of our model above average across nearly all traffic types.

Comparison :

Table 5: Models Comparison

Model	**Accuracy**
Random Forest	0.812415
Support Vector Machine	0.547235
Decision Tree	0.816477
Gradient Boosting	0.893449

This table 5 for five table summarizes the performance of four machine learning models to classify network traffic. Among the algorithms considered, Gradient Boosting managed to attain the most reproducible results (89.34%). With accuracy around 81-82%, Random forests and Decision Trees are the closest ones followed by (Naive Bayes (76%) and KNN-1 respectively). SVM, Support Vector Machine, markedly fails to deliver with 54.72% accuracy To sum up, GBM has most of all needed and delivers pretty good results considering the challenges the model faces like "C&C" and "DDoS".

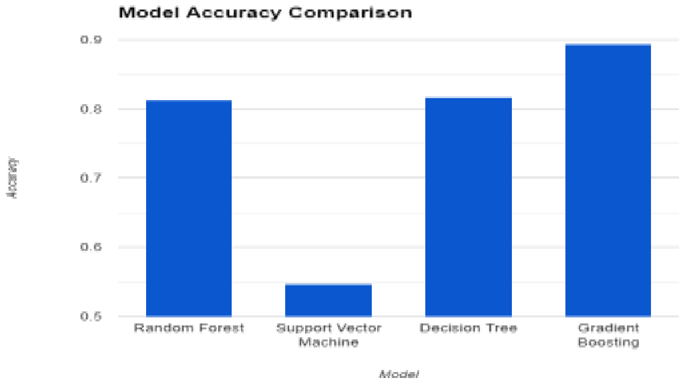


Figure 5: Model Accuracy Comparison

Figure 8 illustrate a learning curve of the random forest model. The learning curve is a representation of how a model's performance improves the more it is trained and as a result of more data. The x axis corresponds to the number of training examples, and the y axis represents the highlighted metric (for instance accuracy). The blue and the red line, in the graph, depict the training score and the cross-validation score. Score training shows how good the model is at the data it was trained on, while score cross-validation votes for the model's performance if the data has not been seen earlier. Optimal situation constitutes that the two lines lay closely to each other. This graph illustrates the dynamics of the training score growth with the passage of time as the model is trained by more data.

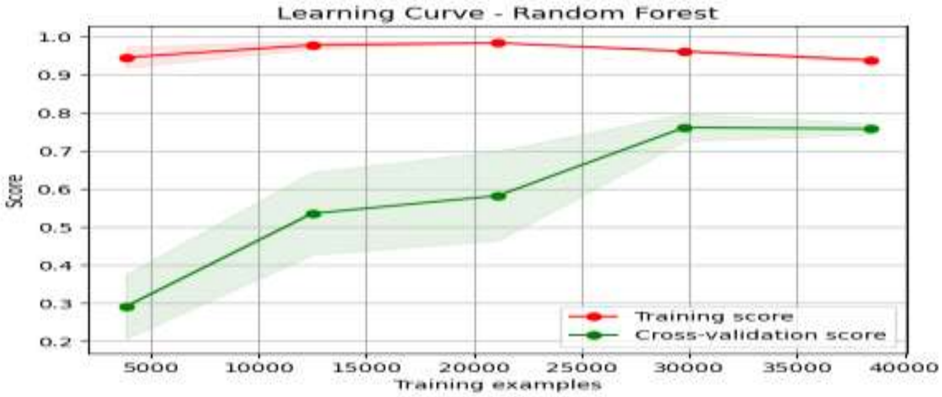


Figure 6: Learning Curve Random Forest

Figure 9 exemplifies the exploration curve of an SVM model classifying a dataset, where its performance increases at first and later stagnated. The x-axis is the number of training events, and y-axis represents the model's score my likely be accuracy. A: The curves S1 and S2 indicate the training score and the cross-validation score. During the training phase, the training score indicates how accurately the model can do on the data it was trained by, on the other hand, the cross-validation score shows how well the model can perform on unseen data. In Figure 4 there is a chance that as there will be unseen data the model will perform less.

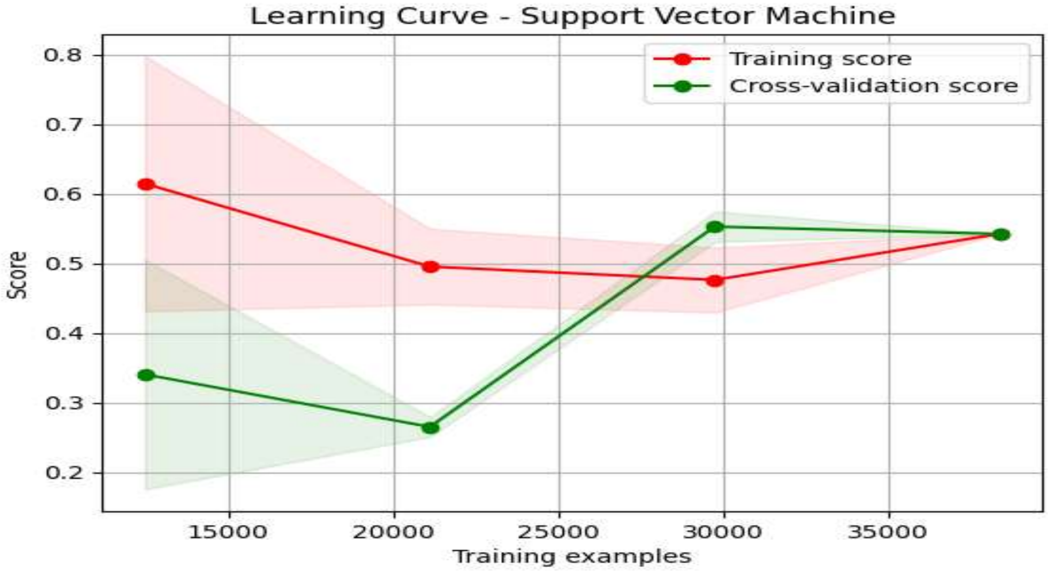


Figure 7: Learning Curve Support Vector Machine

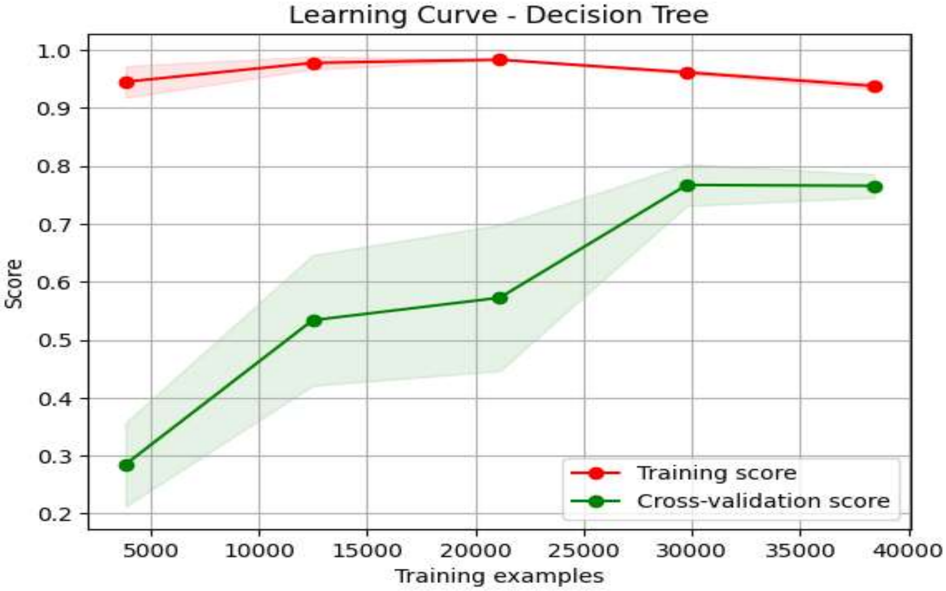


Figure 8: Learning Curve Decision Tree

In figure 5,There are two plots on the graph (the training score and the cross-validation score). And where the training score points to how well the model operates on the provided training data, the cross-validation score shows how well model operates on unseen dataset. both the train score and the cross-validation score are successfully measured to be higher as the model is trained with more data. The training score rises faster than the cross-validation rate, but do not panic. This implies that the model might be somewhat overfitting the data, or, in other words, not generalizing it for all unseen data.

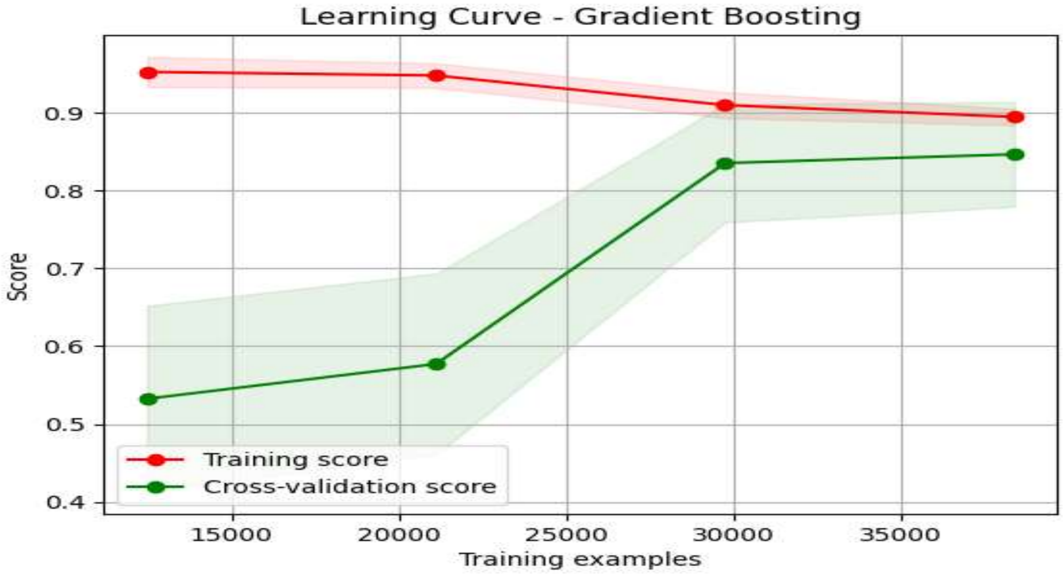
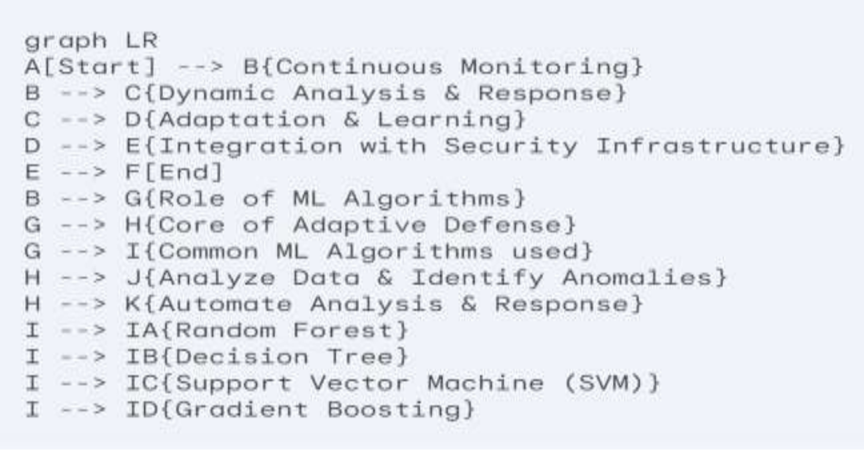


Figure 9: Learning Curve Gradient Boosting

Adaptive Defense Mechanisms: Conceptual Framework

The implementation of adaptive defense in IoT networks focuses attention on the continuous monitoring, investigation and adaptation to gradually changing threats as well as traditional network functionality. Unlike static defenses provision which takes physical actions once the risk is known, the adaptive security implies dynamic adjustment of security measures according to current data and intelligence on threats. IoT security situations with millions of diverse devices create problems that are impossible to solve with a static security solution only. Therefore, adaptive defense becomes a fundamental requirement. Key components of adaptive defense mechanisms.



```
graph LR
A[Start] --> B{Continuous Monitoring}
B --> C{Dynamic Analysis & Response}
C --> D{Adaptation & Learning}
D --> E{Integration with Security Infrastructure}
E --> F[End]
B --> G{Role of ML Algorithms}
G --> H{Core of Adaptive Defense}
G --> I{Common ML Algorithms used}
H --> J{Analyze Data & Identify Anomalies}
H --> K{Automate Analysis & Response}
I --> IA{Random Forest}
I --> IB{Decision Tree}
I --> IC{Support Vector Machine (SVM)}
I --> ID{Gradient Boosting}
```

Figure 10:Algorithm for Adaptive Defense

1. Continuous Monitoring: The techniques that are adaptable use the system of feedback constantly operated. This feeds back by monitoring the network traffic, device actions, and system parameters. This will rely on the aggregation of the data from different sources, like sensor networks, device logs, and feeds from external threat intelligence services. Pattern recognition algorithms through continuous monitoring of the network can help adaptive defense mechanisms respond promptly to anomalies and potential security threats.

2. Dynamic Analysis and Response: Dynamic tools of adaptation use hefty analysis mechanisms to asses to what grade and what type of detected anomalies is. The exercise might be automated with machine learning algorithms used for pattern analysis, detection of malicious behaviors, and rare prediction of potential events. Later on, it is proven that the destructive mechanism can be widely utilized for reaction procedures including devices shut-off, blocking abnormal load, and updating the security strategy.

3. Adaptation and Learning: Such distinctive adaptive defense mechanisms as their ability to adapt and learn from the past can be considered its hallmark. The signature-based checking mechanism can be tuned into adaptive defense mechanism which learns from machine learning methods and this enables it to better detect the new threats with time thereby becoming more effective in mitigating emerging threats. Providing the ability to adapt allows for development of the defense functions which enhance was their level in the environment and network conditions.

4. Integration with Security Infrastructure: Adaptive defense mechanisms normally have an inbuilt interface with the existing security devices, such as a firewall, intrusion prevention system and security information and event management (SIEM) devices. This integration helps adaptive defenses leveraging on the existing security controls step by step as well as threat intelligence feeds to be able to detect and respond to security threats.

4.6.2 Role of ML algorithms in adaptive defense:

At the core of adaptive defense mechanisms there is the machine learning (ML) algorithms which offer critical intelligence and automation services for detecting, analyzing and quickly responding to security issues when happening in real-time. By analyzing the huge amounts of data, and revealing the complex patterns and anomalies that may represent a security threat, the AI programs could discover. Given the architecture of IoT networks, ML algorithms can be learned to notice the typical patterns for different kind of devices and network traffic, and they will be able to identify deviations which may be the manifestation of an attempted hacking into the system. Some common ML algorithms used in adaptive defense mechanisms include:

- **Random Forest:** Random Forest is a covering up technique which has an advantage of working in the complex databases and also it evades the overfitting by merging at a diverse range of trees as the outcomes. By the application of adaptive defense mechanisms, Random Forest may be used as a technique for classifying network traffic and identifying abnormal patterns closely.
- **Decision Tree:** Decision Tree algorithms are based on a set of these if-then rules which explain their high capacity for explanation. Decision Trees is capable directly of adaptive defense mechanism for assessing anomalies by gaining insights into security incident causes.
- **Support Vector Machine (SVM):** SVM is an extraordinary classifier which works great when distinguishing and classifying data with dimensionality above three or four. SVM can be applied to adaptive defense mechanisms as switching devices for classifying network traffic and detecting malicious behavior patterns.
- **Gradient Boosting:** Gradient Boosting is an ensemble learning method which, by design, makes a ’network’ of weak learners that in the end deliver a powerful explanation. Gradient Boosting would offer a chance to undogmatic boost the precision of anomaly detection models whose accuracy could be reshaped to fit in a changing environment.

Conclusion

The present work resewed into the efficacy of several machine learning methods for anomaly detection and adaptive security mechanisms in Internet of Things (IoT) networks. We focused on prevalent security issues in IoT devices and the fact that the traditional security solutions are not sufficient anymore. The research commissioned to compare the execution of Random Forest, Support Vector Machine (SVM), Decision Tree, and Gradient boosting models for network traffic classification was done. Surprisingly, the Gradient Boosting approach gained a higher absolute accuracy (89.34%) in discrimination of network traffic classes, such as attacks, normal traffic, and more specific malicious traffic like Command-and-Control communication or DDoS attacks. Besides, the random forest and the decision tree models also showed good success with accuracy around 81% to 82%. On the one hand, SVM did worst and shows up with the lowest value of 54.72% accuracy, which was not so good.

Model behavior studies, which involve the learning curve analysis, added more colors to my understanding. However, even if the models had some degree of overfitting, Gradient Boosting performed superior in trade-off between data-driven training and capability for unseen data. On the decision tree chart, the lifeline exhibited a fast sharp response at the bottom followed by a leveling that could be brought by overfitting if trained for too long. The learning curve of SVM model indicated on the training process that it was producing exaggerated overfitting, this is the reason the model performs low. It is only evidence that Gradient Boosting can be effectively applied toward anomaly detection in that IoT is such powerful tool. The feature that possesses the competence to intensely learn complicated shapes and also to adapt to moving threats, makes it a precious component of the security systems in IoT ecosystems. Nevertheless, those techniques still need to be explored to prevent the mentioned undesirable effect and implementation of different algorithms for creating even more robust and better adapted systems by using the advantages of diverse machine learning tools. It is also worth noting that designing physical-world implementations, comprising computational efficiency and scalability, is also a major area of necessity to make IoT TSN applicable in large size networks.

References

"Realtime Anomaly Detection in Healthcare IoT: A Machine Learning-Driven Security Framework," 2023.

A. K. Ray and A. Bagwari, "IoT based Smart home: Security Aspects and security architecture," in 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), 2020, pp. 218–222.

H. Salehi and R. Burgueño, "Emerging artificial intelligence methods in structural engineering," Eng Struct, vol. 171, pp. 170–189, 2018.

H. Bangui and B. Buhnova, "Recent advances in machine-learning driven intrusion detection in transportation: Survey," in Procedia Computer Science, Elsevier B.V., 2021, pp. 877–886. doi: 10.1016/j.procs.2021.04.014.

S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.

S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.

M. Nankya, R. Chataut, and R. Akl, "Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies," Sensors (Basel, Switzerland), vol. 23, no. 21. Oct. 30, 2023. doi: 10.3390/s23218840.

D. Javeed, T. Gao, M. T. Khan, and I. Ahmad, "A hybrid deep learning-driven SDN enabled mechanism for secure communication in internet of things (IoT)," Sensors, vol. 21, no. 14, Jul. 2021, doi: 10.3390/s21144884.

M. A. Alsoufi et al., "Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review," Applied Sciences (Switzerland), vol. 11, no. 18. MDPI, Sep. 01, 2021. doi: 10.3390/app11188383.

S. Bharati and P. Podder, "Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions," Security and Communication Networks, vol. 2022. Hindawi Limited, 2022. doi: 10.1155/2022/8951961.

W.-Y. Loh, "Classification and regression trees," Wiley Interdiscip Rev Data Min Knowl Discov, vol. 1, no. 1, pp. 14–23, 2011.

A. Segatori, F. Marcelloni, and W. Pedrycz, "On Distributed Fuzzy Decision Trees for Big Data," IEEE Transactions on Fuzzy Systems, vol. 26, no. 1, pp. 174–192, 2018.

S. Eltanbouly, M. Bashendy, N. AlNaimi, Z. Chkirbene, and A. Erbad, "Machine learning techniques for network anomaly detection: A survey," in 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 2020, pp. 156–162.

F. Y. Osisanwo, J. E. T. Akinsola, O. Awodele, J. O. Hinmikaiye, O. Olakanmi, and J. Akinjobi, "Supervised machine learning algorithms: classification and comparison," International Journal of Computer Trends and Technology (IJCTT), vol. 48, no. 3, pp. 128–138, 2017.

S. Ray, “A quick review of machine learning algorithms,” in 2019 International conference on machine learning, big data, cloud and parallel computing (COMITCon), 2019, pp. 35–39.

B. Mahesh, “Machine learning algorithms-a review,” International Journal of Science and Research (IJSR), vol. 9, pp. 381–386, 2020.

J. T. Senders et al., “An introduction and overview of machine learning in neurosurgical care,” Acta Neurochir (Wien), vol. 160, no. 1, pp. 29–38, 2018.

S. Kotsiantis, I. Zaharakis, and P. Pintelas, “Machine learning: A review of classification and combining techniques,” Artif Intell Rev, vol. 26, no. 3, pp. 159–190, 2006.

E.-A. Minastireanu and G. Mesnita, “An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection,” Informatica Economica, vol. 23, no. 1, 2019.

A. E. Mohamed, “Comparative study of four supervised machine learning techniques for classification,” International Journal of Applied, vol. 7, no. 2, pp. 1–15, 2017.

T. Rumpf, A.-K. Mahlein, U. Steiner, E.-C. Oerke, H.-W. Dehne, and L. Plümer, “Early detection and classification of plant diseases with support vector machines based on hyperspectral reflectance,” Comput Electron Agric, vol. 74, no. 1, pp. 91–99, 2010.

P. Pudil and J. Novovičová, “Novel methods for feature subset selection with respect to problem knowledge,” in Feature extraction, construction and selection, Springer, 1998, pp. 101–116.

E. Gyamfi and A. Jurcut, “Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets,” Sensors, vol. 22, no. 10. MDPI, May 01, 2022. doi: 10.3390/s22103744.

M. Aslam et al., “Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT†,” Sensors, vol. 22, no. 7, Apr. 2022, doi: 10.3390/s22072697.

S. K. Devineni, S. Kathiriya, and A. Shende, “Machine Learning-Powered Anomaly Detection: Enhancing Data Security and Integrity,” Journal of Artificial Intelligence & Cloud Computing, pp. 1–9, Jun. 2023, doi: 10.47363/JAICC/2023(2)184.

I. Ullah, A. Ullah, and M. Sajjad, “Towards a Hybrid Deep Learning Model for Anomalous Activities Detection in Internet of Things Networks,” Internet of Things, vol. 2, no. 3, pp. 428–448, Sep. 2021, doi: 10.3390/iot2030022.

Y. N. Kunang, S. Nurmaini, D. Stiawan, and B. Y. Suprapto, “Attack classification of an intrusion detection system using deep learning and hyperparameter optimization,” Journal of Information Security Applications, vol. 58, p. 102804, 2021.

B. Hussain, Q. Du, B. Sun, and Z. Han, “Deep Learning-Based DDoS-Attack Detection for Cyber–Physical System Over 5G Network,” IEEE Trans Industr Inform, vol. 17, pp. 860–870, 2021.

A. Haider, M. Adnan Khan, A. Rehman, M. Rahman, and H. Seok Kim, “A Real-Time Sequential Deep Extreme Learning Machine Cybersecurity Intrusion Detection System,” Computational Materials and Continua, vol. 66, pp. 1785–1798, 2021.

M. Catillo, M. Rak, and U. Villano, “2L-ZED-IDS: A Two-Level Anomaly Detector for Multiple Attack Classes,” in Proceedings of the AINA Workshops 2020, Caserta, Italy, 2020, pp. 687–696.