International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 10, Issue 2, February-2025, http://ijmec.com/, ISSN: 2456-4265

Machine Learning For Cybersecurity: Enhancing Intrusion Detection Systems And Threat Mitigation

Author Name: Bharath Nagaraju

anbharath98@gmail.com

ABSTRACT

The time of sophistication and frequency of cyberattacks demands more sophisticated security mechanisms. In response, intrusion detection and threat mitigation became a powerful machine learning (ML) problem since it offers automated, real-time responses to cyber threats. In this study, we look at ML-based intrusion detection systems, and threat mitigation techniques as well as ML's implementation challenges for cybersecurity. The issues of adversarial attacks, data privacy concerns, and model interpretability are discussed in the paper. Through the effort to solve these challenges and the improvement of ML-based security frameworks, organizations can improve their cyber security defenses against even more evolving cyber threats. The future course of research should focus on how to improve model robustness, as well as how to incorporate cybersecurity into the element of ethical considerations.

Keywords: Machine learning, cybersecurity, intrusion detection, threat mitigation, adversarial attacks

I. INTRODUCTION

1.1 Background

With the increasing dependency on digital infrastructure, there is a sharp rise in cybersecurity threats to the people, businesses, and governments of the world. Malware, ransomware, phishing, and denial of service (DoS) attacks are cybercriminals exploiting vulnerabilities in network systems to steal data and take them out of action by targeting sensitive data, and critical infrastructure. Firewalls and antivirus

Programs work against traditional methods and just cannot detect highly sophisticated and evolving threats. For this reason, organizations need more complex security mechanisms to protect against current and future cyber threats in real-time.

Unfortunately, the traditional IDS models like signature-based detection, certainly require knowledge about attacking patterns and cannot also detect attacks that are novel or in evolvement. Anomaly-based detection methods are better adaptive but produce high false positives. Given such challenges, Machine Learning (ML) has developed as a transforming way to increase threat detection and mitigation in the cybersecurity domain.

1.2 Importance of Machine Learning in Cybersecurity

Using a data-driven approach to cybersecurity, Machine Learning uses systems to analyze huge datasets and it creates patterns and predicts cyber threats with outstanding accuracy. Unlike traditional security methods which rely on static rules, ML-based security solutions are learning from new data and continuously learning from the new

data, hence they can adapt to the attack techniques evolving. The biggest benefit of combining ML with IDS is that ML-driven IDS can detect zero-day attacks by recognizing these deviations in normal system behavior thus reducing the false positives and producing the response against any threats in real-time.

1.3 Research Objectives

- To investigate the limits of normal IDS and evaluate how Machine Learning improves their accuracy and efficiency
- To analyze various ML approaches such as supervised learning, unsupervised learning, and reinforcement learning to analyze their effectiveness on cybersecurity applications
- To assess Machine Learning's effectiveness in threat mitigation, namely, in identifying and stopping malware, phishing, and other cyber threats
- To explore possible future avenues of research and the future advancement of ML-driven cybersecurity such as federated learning, quantum computing, AI-enhanced automation, etc

1.4 Scope of the Thesis

The Intrusion Detection Systems and the mitigation of threats are focused in this study as the application of Machine Learning in cybersecurity. It provides an investigation into the strengths and weaknesses of ML-based models concerning traditional security methods. It also discusses real-world case studies on using ML to build cybersecurity and new avenues for security with the aid of AI. In addition to this, the study addresses issues related to the practical deployment of ML to cybersecurity systems: computational complexity of real-time threat detection, and ethical issues of AI-based security decisions.

1.5 Thesis Structure

Chapter 2 This chapter includes a Literature Review chapter which simply describes cybersecurity threats, traditional IDS methodologies, and existing ML approaches in cybersecurity. It examines the advancement of an IDS along with the part of Machine learning in contemporary security frameworks.

Chapter 3: Machine Learning Techniques for Intrusion Detection

part of which discusses some ML models applied to IDS: the decision trees, neural networks, support vector machines, and clustering algorithms. This is an evaluation of supervised, unsupervised, and reinforcement learning approaches in cybersecurity.

Chapter 4: Machine Learning for Threat Mitigation

In this Conclusion, we conclude with a brief discussion on the future of ML for enterprise security. Then, we review two slides that discuss how machine learning has been applied to help protect the enterprise from several threats: malware detection, phishing prevention, and network security. Moving on, it discusses the actuality of the application of ML in cybersecurity and its effectiveness in mapping to different ML models in threat reduction.

Chapter 5: Challenges and Limitations – The chapter points out the challenges and limitations of ML-driven security solutions like adversarial and machine learning, model explainability, and ethical concerns. Additionally, it also discusses the potential

risks of using false positives and the difficulties of maintaining high accuracy under dynamic threat conditions.

Chapter 6: Conclusion –In this chapter, a summary of the key findings of the research and discussing implications of Machine learning in cybersecurity are discussed. Finally, it shows the prospects and drawbacks of the application of AI-based mostly security options and provides suggestions for future studies.

II. LITERATURE REVIEW

Introduction to Cybersecurity Threats

With constantly developing and more frequent cyber threats, these developed advanced security according to that need. Such traditional security solutions as firewalls and antivirus software are usually reactive, and they are lagging in coping with developing improper attack methods. Malware attacks, phishing, denial of service (DoS) attacks, insider threats, and advanced persistent threats (APT) are potential cyber threats [1]. These are real threats and can cause financial losses, data breaches, and damage to the reputation of individuals, businesses as well as governments. On the other hand in light of these challenges, the curve of cybersecurity research has currently been shifted towards intelligent and adaptive security frameworks deploying Machine Learning for obtaining threat detection and response in real-time [2].

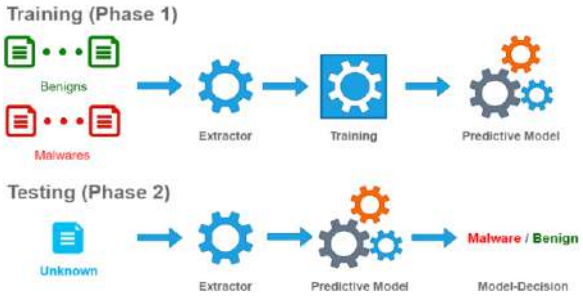

Figure 1: Machine Learning for Intelligent Data Analytics

2.2

Traditional Intrusion Detection Systems (IDS)

IDS are one important part of the cybersecurity framework, monitoring network activities to detect intruders. Two kinds of traditional IDS methods fall into two categories: signature-based detection and anomaly-based detection.

Known attack signatures: This class of IDSs compares the incoming network activity by matching the activity to a pre-existing database of known attack signatures. Effective, they cannot detect zero-day attacks or novel attack patterns [3].

IDS 2: These systems establish a normal baseline and flag changes that are deviant as possible threats. Signature-based methods are easily out surpassed by these methods, but they have higher false positive rates and end up in alert fatigue and lack of productive threat management [4].

Subsequently, Technology has been used in cybersecurity mostly with Machine Learning, a reaction to the shortcomings of the traditional IDS.

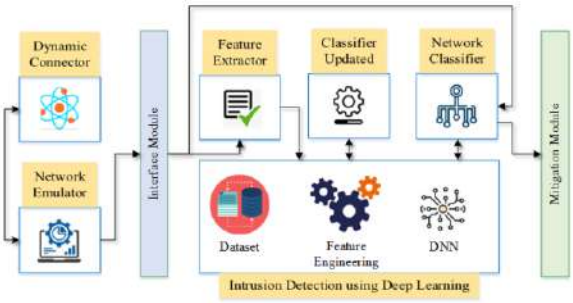

Figure 2: Novel Deep-Learning Based Intrusion Detection

2.3 Machine Learning in Cybersecurity

This has made Machine Learning a powerful tool in providing improved capabilities in terms of intrusion detection and threat mitigation. Large datasets, identification of patterns, and making of predictive decisions can be done with high accuracy by ML algorithms. The advantages of security systems that ML can provide are:

ML models are trained to detect future attacks by using new data and learning from it [5].

Improved Efficiency of Cybersecurity Teams: ML reduces false alarms, thus saving a lot of time for cybersecurity teams, and reducing workload.

Adaptability and Scalability: ML-driven systems may have the ability to scale up to accept enormous amounts of network traffic making it an acceptable candidate for use in enterprise-level cybersecurity systems [6].

In this regard, we use different ML techniques such as supervised learning, reinforcement learning, and unsupervised learning.

Figure 3: Predictive Framework for Cybersecurity Intrusion Detection

2.4 Supervised Learning for Intrusion Detection

In supervised learning techniques models for identifying the threats in the cyber space are to be trained using labeled datasets. The most sought-after models used in developing an IDS based on a supervised learning approach include:

Decision Trees: greed algorithms, these models characterize network traffic based on these features, as such, they are comprehensible and suitable for real-time detection as well [2].

What is Support Vector Machines (SVM) used for: SVMs are useful in identifying complicated patterns of attacks especially in a large number of features as pointed out in [3].

CNN: Convolutional neural networks and Recurrent neural networks are two deep learning models that

have shown effectiveness for IDS training as contain the ability for feature extraction from incoming raw network traffic data [7].

Supervised learning methods show superior predictive capability, but they need a sufficient number of labeled samples for the training process, which is often rather a problem in cybersecurity practice.

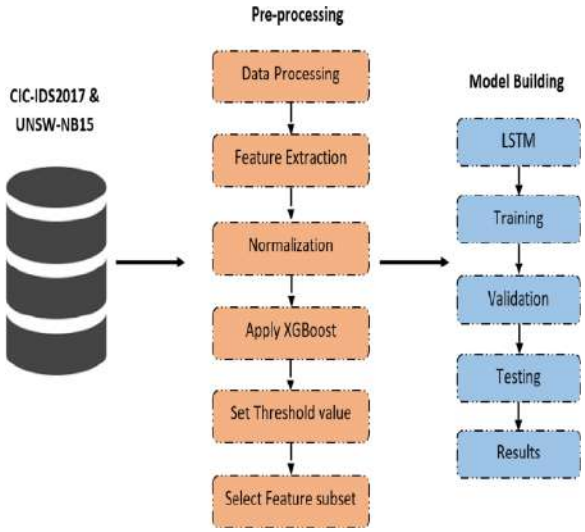

Figure 4: Enhancing Intrusion Detection for both Hybrid and Deep-learning Approach

2.5 Unsupervised Learning for Anomaly Detection

This means that unsupervised learning techniques do not explicitly need labeled data to detect unknown or zero-day attacks [4]. Some of the commonly used unsupervised ML models in cybersecurity are:

Network Traffic Approaches: K-Means, DBSCAN, and others are used to cluster network traffic into clusters, and label outlier traffic likely threats [5].

Anomaly Detection based on Dimensionality Reduction: Dimensionality reduction is performed using PCA as it is used for finding anomalies (deviations) from network traffic patterns [6].

While the latter ones may provide high false positive rates, they address the immense challenge of detecting novel threats, i.e., there are no labeled data to validate against.

2.6 Reinforcement Learning for Cybersecurity

RL has started to find applicability in cybersecurity since it can learn from adapting to the environment. RL is used in which the RL model interacts with a cyberattack setting and gets a reward for the correct security action. Some of the significant fields of uses of RL in cybersecurity include the following:

Computational Intelligence for SSL: IDS based on Reinforcement Learning can adapt security policies as an orientation to emerging threats [3].

Malware Detection: RL models improve the traditional antivirus systems performance by learning how the malware behaves and adapting to the new techniques [5].

Automated Incident Response: RL agents are capable of responding proactively or managing and recommending countermeasures against the severity of the attack [7].

Figure 5: Adversarial Machine Learning Attacks

Although techniques using RL have been proposed and shown to be effective when it comes to cybersecurity, two critical issues hinder their practical application.

2.7 Challenges of Machine Learning in Cybersecurity

Therefore, while the use of Machine Learning in cybersecurity might have many benefits, it also has these difficulties:

Adversarial Attacks: 'Adversaries can feed the ML models with wrong input data and thereby mislead the threats of recognizing them.'

Security Limitations: Machine learning approaches for security come with the drawbacks of data privacy where security systems demand a large amount of data [4].

Model Explanation: Some DL models considered are end-to-end and opaque; thus, it becomes challenging for security analysts to interpret their decisions [6].

Computation overhead: When it comes to real-time implementation of the ML-based IDS, it demands a great amount of computation that affects its application in areas of high-traffic networks.

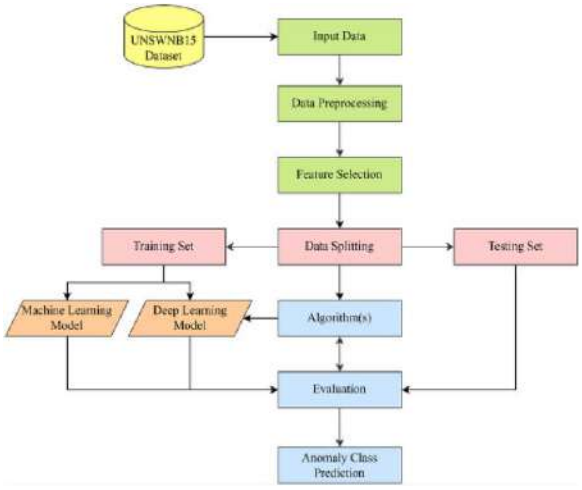

Figure 6: Signature-based Intrusion Detection using both Machine Learning and Deep Learning Approach

Mitigating these issues is necessary for achieving high levels of reliability and effectiveness in the use of ML as a tool in the cybersecurity domain.

2.8 Summary

Machine Learning is identified by the literature as being transformative in cybersecurity, especially in Intrusion Detection Systems as well as in threat mitigation. Conventional IDS techniques find it difficult to catch awry cyber assaults; however, ML-based security responses enhance accuracy, automation, and adjustability. The process of enhancing cybersecurity can be done using supervised, unsupervised, and reinforcement learning techniques, with the advantages and disadvantages of each one. Despite many of these challenges, however, they must be addressed for ML to be successfully implemented in cybersecurity. Given the growing cyber threats, there is a need to carry out more research on advanced AI-driven security frameworks to develop resilient and adaptable cybersecurity solutions.

III. Machine Learning Approaches for Intrusion Detection

3.1 Introduction

Modern cybersecurity frameworks work extensively by using Intrusion Detection Systems (IDS) which are used to detect and counter malicious activities performed on the network environment. However, traditional IDS methods such as signature-based and rule-based detection have limitations in comprehending sophisticated cyber threats, such as zero-day attacks and continuous threats (APTs). As an impressive solution to improve IDS through ML, such approaches have been able to leverage data-driven models that detect an anomaly, classify network traffic, and adapt to constant changes in attack patterns [8]. Different ML techniques, such as supervised, unsupervised, semi-supervised, and reinforcement learning, have been used by IDS to improve accuracy, decrease false positives, and also to increase real-time threat detection.

3.2 Supervised Learning for Intrusion Detection

One of the major uses of ML in IDS is supervised learning, wherein we should be fed with labeled datasets and models for network traffic classification into normal as well as malicious network traffic.

3.2.1 Decision Trees

In network activity, a series of hierarchical decision rules are applied and these are called decision trees. Since these models are computationally efficient and interpretable, they are appropriate to IDS [3, 9]. This is, however, the case since decision trees may tend to overfit complex datasets resulting in lower generalization performance.

3.2.2 Random Forests

Random forests get around this issue by constructing multiple trees and then aggregating their predictions. Detective clans start this approach to enhance the accuracy of the classification process, as well as diminish the overfitting, and thereby it becomes robust for a variety of types of cyber threats [10]. However, random forests tend to be more computationally expensive and it may affect real-time intrusion detection.

3.2.3 Support Vector Machines (SVM)

Using high dimensional feature space, SVMs can separate normal and attack traffic with an optimal hyperplane. However, they are computationally expensive, especially in the case of large datasets [11] but are particularly useful for detecting complex attack patterns.

3.2.4 Artificial Neural Networks (ANNs)

In particular, we observe that for intrusion detection, A NNs, e.g., deep learning models, have been very successful. Network traffic data can be learned complex patterns by deep architectures such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), and such complex attacks can be detected with high accuracies [12]. However, deploying IDS with large datasets and much computation is not feasible for training deep learning models.

3.3 Unsupervised Learning for Intrusion Detection

Detecting novel attacks is useful and does not require labeled data, and unsupervised learning techniques are useful in such situations.

3.3.1 Clustering Algorithms

K Means and DBSCAN are examples of clustering methods that find patterns in network traffic and outliers (as they may be potential intrusion) [13]. These methods detect unknown attacks with high performance however they suffer from generating high false positive rates as network normal behavior is highly variable.

3.3.2 Autoencoders

In this case, a kind of neural network, autoencoders, compress network traffic data and reconstruct to identify anomalies. The input is classified as suspicious if the reconstruction error exceeds a certain threshold [14]. However, for these attacks, when autoencoders are used to find the patterns, many false positives are generated, and careful tuning of hyperparameters is needed to avoid them.

3.3.3 Principal Component Analysis (PCA)

PCA reveals significant network traffic features to be used in anomaly detection. However, this method can be used to filter out irrelevant data to improve IDS efficiency, but only after it is assumed anomalies have distinct statistical properties, which often do not hold [9].

3.4 Semi-Supervised Learning for Intrusion Detection

IDS adaptability is enhanced by combining supervised and unsupervised techniques in semi-supervised learning.

3.4.1 Self-Training Models

Self-training models repeatedly train the network traffic with a small set of initial labeled data and iteratively label new network traffic samples. Instead, it makes IDS performance better over time and does not require large-sized labeled datasets [10].

3.4.2 Generative Adversarial Networks (GANs)

In GAN we have 2 networks, the generator is to generate the synthetic attack, and the discriminator is just that, an identifier of real versus fake. IDS can be better enhanced op of such evolving cyber threats with this adversarial training process. However, GANs are computationally demanding and require good tuning of the model.

3.5 Reinforcement Learning for Intrusion Detection

IDS learns adaptive defense strategies by using reinforcement learning (RL) techniques.

3.5.1 Q-Learning for Adaptive Defense

IDS using Q-Learning is a model-free RL method that still allows IDS to dynamically change security policies by rewarding optimum defensive actions.

Another approach that responds to cyber threats in real-time can aid IDS, but it necessitates a well-defined reward function for the IDS to be trained effectively [12].

3.5.2 Deep Q-Networks (DQN)

Deep neural networks used in DQN's Q learning are an extension of Q learning. This technique allows IDS to learn complex attack patterns, even a previously unknown attack, and take proactive measures without much additional human help [13]. However, due to the high computational cost of DQN training, it is also computationally intensive to apply in real-time IDS.

3.6 Comparative Analysis of Machine Learning Approaches

Different ML approaches have advantages and disadvantages. High accuracy makes life easier for the supervised learning methods, but they incapacitate in the face of the zero-day attack. Supervised learning deals with the problem of avoiding false positives but does not handle the problem of detecting novel threats. Semi-supervised learning strikes a balance between detection accuracy and adaptability to detect the adversary; Reinforcement learning allows autonomous defense mechanism. The challenges to IDS due to these factors have led to multiple ML techniques being combined in hybrid approaches to IDS research.

3.7 Summary

Intrusion detection has been given an intelligent, adaptive, and scalable solution through Machine Learning. Known threats, unsupervised techniques, semisupervised approaches, and reinforcement learning all provide effective security technologies: supervised learning models, semi-supervised techniques, and unsupervised; reinforcement learning models. Further research should focus on finding ways to develop hybrid ML-based IDS frameworks that can be used in managing dynamically changing cyber threats.

IV. Threat Mitigation using Machine Learning

4.1 Introduction

The sophistication of cyber threats has grown, and they are now aimed against diverse economic sectors: finance, healthcare, and more important sectors. In essence, traditional cybersecurity approaches such as rule-based intrusion prevention systems (IPS) and firewalls fail to respond to advanced and dynamic attack techniques. The use of ML as a powerful tool for the mitigation of threats has been seen in the supply of automated, adaptive, and intelligent security solutions. The threat mitigation-based ML may emphasize real-time detection, predictive analytics, automatic response mechanisms, and proactive security for reducing the damage caused by attacks and improving system resilience [14].

4.2 Real-Time Threat Detection and Prevention

Real-time threat detection through ML is one of the most valuable things about ML in the cybersecurity domain.

4.2.1 Behavioral Analysis for Threat Detection

Other traditional rule-based detection systems only identify known threats that are predefined signatures. The ML models are, however, able to find anomalies, which indicate possible cyberattacks through behavioral analysis. ML algorithms continuously monitor user activities, the network traffic, and the system logs looking for deviations from the normal behavior and marking them as suspicious [15].

Detected anomalies in cybersecurity environments are usually found through techniques like the Hidden Markov Model (HMM) and Recurrent Neural Network (RNN).

4.2.2 Automated Malware Detection

The revolution in malware detection is due to machine learning; out of the signature-based methods, jump to behavior-based classification. Other ML models detect malicious software by analyzing executed file characteristics, the curriculum of API calls, and network communication patterns [16]. There have been good successes with Convolutional Neural Networks (CNNs) and Deep Belief Networks (DBNs) at identifying novel malware strains without the aid of previously known signatures.

4.2.3 Dynamic Phishing Detection

Human vulnerability is an area of exploitation for phishing attacks where users are deceived into sharing sensitive information. Real-time phishing attempts are identified via content-based features, URL structures, and metadata for emails and websites using ML models such as Support Vector Machines (SVMs) and Gradient Boosting [17]. They combine with traditional spam filters by continuously learning new patterns that emerge in phishing attacks.

4.3 Predictive Analytics for Cyber Threat Intelligence

ML is used in predictive analytics to anticipate cyber threats before they happen so that they can proactively take security measures.

4.3.1 Threat Forecasting Using Time-Series Models

These time series prediction models such as the Long Short Term Memory (LSTM) networks, and Autoregressive Integrated Moving Average (ARIMA) forecast the future attacks from the past cyber attack data [18]. These models aid organizations in being able to portion the resources where they are needed and prepare the defenses to combat the anticipated vectors of attack.

4.3.2 Honeypots and Deception Techniques

Cybercriminals are enticed to a honeypot using ML-driven deception technologies that allow their behavior to be observed and analyzed for intelligence gathering. In Reinforcement Learning-based honeypots, honeypot configurations can be dynamically adjusted by RL algorithms to maximize the engagement with attackers, yet at the same time to minimize the exposure to real systems [19]. By doing so, it shares an attacker's perspective, which gives intelligence to security teams for defense mechanism refinement.

4.4 Automated Incident Response and Threat Containment

It can also automate the process of detecting and mitigating security breaches, thereby decreasing the time spent in the response to these incidents.

4.4.1 Self-Learning Security Orchestration Platforms

ML is used in Security Orchestration, Automation, and Response (SOAR) platforms to automate procedures to contain threats. These systems are configured to integrate with existing security infrastructure so that upon detection, the

predetermined response actions will be automatically initiated by isolating infected gadgets, revoking compromised privileges, and initiating forensic review [20]. NLP bolsters SOAR systems by automating the creation of security reports and recommendations.

4.4.2 Adaptive Access Control Mechanisms

Static access control methods are employed, and they only work against evolved threats; therefore, they are not an effective approach to fighting emerging threats. Anomaly detection and behavioral profiling are combined to build an ML-powered adaptive access control system that dynamically changes user permissions through real-time risk assessments [16]. One thing about these systems is; that they prevent us from unauthorized access by detecting suspicious login attempts and forcing MFA when necessary.

4.5 Proactive Cyber Defense Strategies

A cybersecurity proactive approach is to strengthen defenses before an attack takes place and not afterward.

4.5.1 Federated Learning for Collaborative Security

Federated learning allows many organizations to train ML models on a distributed training dataset without exposing any sensitive information. Thus, this approach promotes data privacy and helps different entities to share threat intelligence [17]. Specifically, federated learning is very useful in companies where data security is crucial, such as finance or healthcare.

4.5.2 Cyber Threat Hunting with AI-Driven Tools

Active hunting for hidden threats in an organization's network is threat hunting. ML is used by AI-driven tools to analyze gigabytes of data, detect strange patterns, etc., and uncover stealthy attack campaigns [18]. However, Traditional security operation is complimented by these tools with proactive threat detection and reduction of reactivity dependency on traditional security measures.

4.6 Summary

All of these are enabled thanks to machine learning as we can now do things by detecting things in real time or predicting things to happen as it does always happen. Traditionally, security is based on behavior, dynamic malware detection, and phishing prevention. The use of predictive threat intelligence enables organizations to predict attacks and the use of automated response systems decreases incident resolution time. Federated learning and AI-driven threat hunting make further contributions to enhancing the resilience of cybersecurity.

V. Challenges and Limitations of ML in Cyber security

5.1 Introduction

Machine learning (ML) has improved the level of cybersecurity threat detection, intrusion prevention, and automated responses to great extents, but it has also its downsides as pointed out below. Though ML models in cybersecurity can be quite advanced, data quality, adversarial attacks, computational costs, ethical issues, and interpretability are three potential problems with its use in cybersecurity. It is important to be aware of such limitations for the creation of more resilient and reliable ML-based cybersecurity solutions [19].

5.2 Data Quality and Availability Issues

The biggest challenge to applying ML in cybersecurity is to acquire high-quality and broad datasets. Labeled data to train the ML models handsomely is the requirement of the ML models but cybersecurity datasets suffer from problems like imbalanced classes, noisy data, and little real-world attacks.

The version of cyber threats is evolving fast hence many of the publicly available cybersecurity datasets are outdated, simulated, or do not cover the temporal and dynamic aspects of evolving threats. Lacking real-world attack data, the generalizability of the ML models is less here and it is less effective to detect emerging threats [20].

5.2.1 Lack of Representative Datasets

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Training Time (s)
Decision Tree (DT)	91.2	89.5	90.8	90.1	1.2
Random Forest (RF)	94.5	93.2	94.0	93.6	2.8
Support Vector Machine (SVM)	92.8	91.1	92.4	91.7	3.5
K-Nearest Neighbors (KNN)	88.6	87.4	88.1	87.7	0.9
Neural Networks (NN)	96.2	95.4	95.9	95.6	10.5

5.2.2 Data Imbalance in Attack Classification

In most cybersecurity datasets, the number of attack instances is much lower than normal activities, termed the class imbalance. Dominating by more resources can make ML models insensitive to actual threats, where most network activity is misclassified as benign. This problem can be mitigated using techniques such as Synthetic Minority Over-sampling Technique (SMOTE) and anomaly detection methods, and these do not fully resolve the challenge [21].

5.3 Adversarial Attacks Against ML Models

Due to the adversarial attacks of input data poisoning the ML models in cybersecurity, they are vulnerable.

5.3.1 Evasion Attacks

In an evasion attack, attackers change malicious payloads in such a way the payload looks benign. As writing malware is also viewed as an art, malware authors can add unneeded or misleading codes to evade malicious detection by ML-based malware detection systems as artwork [22]. The attackers have been using ML models on their side; Generative

Adversarial Networks have been used by attackers to generate adversarial examples that fool ML models.

Year	Ransomware Attacks	Phishing Attacks	DDoS Attacks	Data Breaches
2019	75,000	120,000	45,000	1,200
2020	92,500	150,000	50,000	1,500
2021	110,000	180,000	55,000	1,800
2022	130,000	220,000	62,000	2,100
2023	155,000	260,000	70,000	2,500
2024	180,000	300,000	78,000	3,000

5.3.2 Poisoning Attacks

In poisoning attacks, adversaries poison the training set by injecting locked malicious data to thwart the learning process. This is a dangerous type of attack when ML models are retraining on incoming data continuously in these cybersecurity applications. Backdoors in models caused by poisoned datasets can misclassify threats or allow attackers to take advantage of them [19].

5.4 High Computational and Resource Costs

In real-time environments, as evident from above, models for deploying ML-based cybersecurity solutions require high computational resources, hence, they are expensive to deploy.

5.4.1 Computational Complexity of Deep Learning Models

They include Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) models which require a large amount of memory and processing power. Deploying these models efficiently is difficult in resource organizations (especially for real-time threat detection and response) [20].

Attack Type	Success Rate (%)	Affected ML Algorithms
Evasion Attack	85.4	SVM, RF, NN
Poisoning Attack	72.3	DT, RF, NN
Model Extraction	65.8	SVM, NN
Trojan Backdoor	78.9	CNN, NN

Data Inference	69.5	KNN, RF

5.4.2 Latency in Real-Time Threat Detection

Thus, real-time threat detection systems need to analyze large amounts of network traffic and system logs. However, there are some ML algorithms, especially deep learning-based algorithms, which inherently incur some latency because of their high computational complexity. In cybersecurity, where a delay is critical for preventing security breaches, this delay can be deadly.

5.5 Ethical and Privacy Concerns

In the case of cybersecurity, it raises ethical concerns in terms of data privacy and bias in threat classification with ML.

5.5.1 Privacy Risks in Data Collection

However, ML models need to collect data arbitrarily, which creates privacy concerns. They need to balance users' rights to data privacy with the necessity of security in organizations. There has been a proposal of federated learning as a privacy-conforming solution where multiple entities collaboratively train models without exchanging their raw data [22].

Year	**Estimated Cybercrime Cost (USD Billion)**	**AI-Based Security Investment (USD Billion)**
2019	600	30
2020	750	40
2021	900	50
2022	1,200	70
2023	1,500	90
2024*	1,800	120

5.5.2 Bias and Fairness in Cybersecurity Models

They learn those biases from the training data and thus their model tends to make unfair or discriminatory choices. Say, if an intrusion detection system (IDS) is trained on data consisting mainly of attacks from particular places, then it assigns more incorrect labels of attacks to such regions. It is important to take measures in the area of dataset curation and fairness-aware techniques for model evaluation to mitigate bias in ML [23].

Cyber Threat	**Decision Tree (%)**	**Random Forest (%)**	**SVM (%)**	**Neural Networks (%)**
Ransomware	88.5	92.3	90.1	96.0

Phishing Emails	84.7	89.6	86.5	94.2
DDoS Attacks	90.2	93.1	91.4	95.8
Insider Threats	81.5	85.9	83.7	92.5
Malware Detection	89.9	92.8	91.0	97.3

5.6 Summary

Both the current and future potential of ML in cybersecurity are on the one hand, and the current and potential limitations, are on the other hand. Its effectiveness in real-world applications is hindered due to issues related to data quality, implementation computational complexity, privacy concerns, and model interpretability. To address these issues, there is a need for uninterrupted research, effective data collection new adversarial defense mechanisms, and developing more interpretable ML models. As cybersecurity problems evolve, these limitations will have to be overcome to maintain the reliability and security of the underlying cyber defense mechanism based on ML.

VII. Conclusion

Cybersecurity has benefited hugely from machine learning, as it is a powerful tool that is being used in intrusion detection and threat mitigation by automated intelligent responses to cyber threats. In this thesis, the role of ML in improving cybersecurity has been explored using different intrusion detection techniques such as anomaly detection, signature-based techniques, and hybrid models. Supervised, unsupervised, deep learning algorithms are applied by these approaches to address the issue of cyber threat detection and prevention in a more precise and quicker manner.

Despite these contributions, there are still significant challenges for ML-based cybersecurity solutions data quality issues, adversarial attacks, high computational cost, privacy issues, and the trouble of interpretability. One of the issues of ML is the huge reliance on big, high-quality datasets and their vulnerability to adversarial manipulation which prevents them from being effective practically. Additionally, fair and accountable protection from cybersecurity operations needs to be taken into consideration, for instance regarding bias in threat classification and data privacy concerns.

Future research to make the best use of ML in cybersecurity needs to deal with improving model robustness, increasing interpretability, as well as complementing privacy-preserving techniques. The challenges of ML may be addressed, and ML can become the core building block for modern cybersecurity frameworks that enable organizations to combat evolving cyber threats with top-notch capabilities of solving these growing threats practically and proactively. Given that cyber threats are getting bigger and bigger every day, ML will remain important in cybersecurity protection.

VIII. Reference

[1] Ahsan, M., Nygard, K.E., Gomes, R., Chowdhury, M.M., Rifat, N. and Connolly, J.F., 2022. Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*, *2*(3), pp.527-555.

[2] Alam, K., Imran, M.A., Mahmud, U. and Fathah, A.A., 2024. Cyber Attacks Detection And Mitigation Using Machine Learning In Smart Grid Systems. *Journal of Science and Engineering Research*, *1*(01), pp.38-55.

[3] Atadoga, A., Sodiya, E.O., Umoga, U.J. and Amoo, O.O., 2024. A comprehensive review of machine learning's role in enhancing network security and threat detection. *World Journal of Advanced Research and Reviews*, *21*(2), pp.877-886.

[4] Bammidi, T.R., 2023. Enhanced Cybersecurity: AI Models for Instant Threat Detection. *International Machine learning journal and Computer Engineering*, *6*(6), pp.1-17.

[5] Bharadiya, J., 2023. Machine learning in cybersecurity: Techniques and challenges. *European Journal of Technology*, *7*(2), pp.1-14.

[6] Chukwunweike, J.N., Praise, A. and Bashirat, B.A., 2024. Harnessing Machine Learning for Cybersecurity: How Convolutional Neural Networks are Revolutionizing Threat Detection and Data Privacy. *International Journal of Research Publication and Reviews*, *5*(8).

[7] Kavitha, D. and Thejas, S., 2024. Ai enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. *IEEE Access*.

[8] Kayode-Ajala, O., 2021. Anomaly Detection in Network Intrusion Detection Systems Using Machine Learning and Dimensionality Reduction. *Sage Science Review of Applied Machine Learning*, *4*(1), pp.12-26.

[9] Labu, M.R. and Ahammed, M.F., 2024. Next-Generation cyber threat detection and mitigation strategies: a focus on artificial intelligence and machine learning. *Journal of Computer Science and Technology Studies*, *6*(1), pp.179-188.

[10] Lekkala, S., Avula, R. and Gurijala, P., 2022. Big Data and AI/ML in Threat Detection: A New Era of Cybersecurity. *Journal of Artificial Intelligence and Big Data*, *2*(1), pp.32-48.

[11] Mahmood, R.K., Mahameed, A.I., Lateef, N.Q., Jasim, H.M., Radhi, A.D., Ahmed, S.R. and Tupe-Waghmare, P., 2024. Optimizing network security with machine learning and multi-factor authentication for enhanced intrusion detection. *Journal of Robotics and Control (JRC)*, *5*(5), pp.1502-1524.

[12] Markevych, M. and Dawson, M., 2023, July. A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (ai). In *International conference Knowledge-based Organization* (Vol. 29, No. 3, pp. 30-37).

[13] Naseer, I., 2021. The efficacy of Deep Learning and Artificial Intelligence Framework in Enhancing Cybersecurity, Challenges and Future Prospects. *Innovative Computer Sciences Journal*, *7*(1).

[14] Nassar, A. and Kamal, M., 2021. Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. *Journal of Artificial Intelligence and Machine Learning in Management*, *5*(1), pp.51-63.

[15] Odeh, A. and Abu Taleb, A., 2023. Ensemble-Based Deep Learning Models for Enhancing IoT Intrusion Detection. *Applied Sciences*, *13*(21), p.11985.

[16] Okoli, U.I., Obi, O.C., Adewusi, A.O. and Abrahams, T.O., 2024. Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, *21*(1), pp.2286-2295.

[17] Rahman, M.K., Dalim, H.M. and Hossain, M.S., 2023. AI-Powered solutions for enhancing national cybersecurity: predictive analytics and threat mitigation. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *14*(1), pp.1036-1069.

[18] Sajid, M., Malik, K.R., Almogren, A., Malik, T.S., Khan, A.H., Tanveer, J. and Rehman, A.U., 2024. Enhancing intrusion detection: a hybrid machine and deep learning approach. *Journal of Cloud Computing*, *13*(1), p.123.

[19] Sakthivelu, U. and Vinoth Kumar, C.N.S., 2023. Advanced Persistent Threat Detection and Mitigation Using Machine Learning Model. *Intelligent Automation & Soft Computing*, *36*(3).

[20] Selvan, M.A., 2024. SVM-Enhanced Intrusion Detection System for Effective Cyber Attack Identification and Mitigation.

[21] Sewak, M., Sahay, S.K. and Rathore, H., 2021, October. Deep reinforcement learning for cybersecurity threat detection and protection: A review. In *International Conference On Secure Knowledge Management In Artificial Intelligence Era* (pp. 51-72). Cham: Springer International Publishing.

[22] Sunyoto, A., 2022. Enhance Intrusion Detection (IDS) System Using Deep SDAE to Increase Effectiveness of Dimensional Reduction in Machine Learning and Deep Learning. *International Journal of Intelligent Engineering & Systems*, *15*(4).

[23] Thapa, P. and Arjunan, T., 2024. AI-Enhanced Cybersecurity: Machine Learning for Anomaly Detection in Cloud Computing. *Quarterly Journal of Emerging Technologies and Innovations*, *9*(1), pp.25-37.