ADAPTIVE THREAT DETECTION: LEVERAGING MACHINE LEARNING FOR REAL-TIME CYBERSECURITY

Sahil Sharma

Department of CSE Chandigarh University, Mohali, India

Amit Kumar

Department of CSE Chandigarh University, Mohali, India

Mayank Bansal

Department of CSE Chandigarh University Mohali, India

Azhar

Department of CSE Chandigarh University, Mohali, India

ABSTRACT

In the dynamically changing cyber security domain, conventional mechanisms for defense often prove inadequate against advanced threats that adapt themselves to counter defenses. This paper presents a new paradigm in building cyber security with the induction of machine learning algorithms into its design for enhanced threat detection and response in real time. In essence, the system keeps learning and, therefore, analyzes network traffic, user behaviors, and system anomalies regularly to identify threats when they are emerging. Our methodology includes supervised and unsupervised learning techniques for known threats and the unveiling of new attack patterns. The proposed system will evolve with new data and be very potent against zero-day attacks and polymorphic malware. Further, feedback in the loop will help the system in refining the models built over time for better accuracy and reducing false positives. It will validate the effectiveness of this adaptive threat detection system by testing it at large in simulated environments, where it will way outperform the traditional methods in the identification and mitigation of a wide range of cyber threats. Results show how machine learning can actually transform cybersecurity to become proactive and dynamic about modern cyber defense challenges.

***Index** Terms*—Machine Learning, Cybersecurity, Threat

Detection, Real-Time Analysis, Adaptive Systems

I. INTRODUCTION

Digital systems, cloud computing, and connected devices have completely redefined the face of cybersecurity in the last few years. Cybersecurity has emerged as the prime concern of digitally transforming enterprises and even critical infrastructure in this context. However, it has also led to the expansive attack surface with such threats like malware, phishing, ransomware, and APT. These emerging threats are later much the cause of why robust and adaptive security mechanisms must be developed, in real-time reaction to mitigate damage. Traditional approaches at the heart of cybersecurity like signature-based detection and rule-based systems form the basis of detecting threats, which has been the foundation for decades. In this methodology, patterns or predefined rules are the basis for attacking; thus, it is effective for known vulnerabilities. However, they are intrinsically reactive; they only offer protection if there is knowledge of the signature of an attack beforehand. As such, systems thus remain vulnerable to zero-day attacks or novel attack vectors, as they fail to discover new, unknown or evolving threats. More proactive and adaptable this growing demand is with cyber threats in constant flux.In the modern cyber security environment, real-time threat detection is now mandatory. It shall be noted that in many occasions, it depends on the speed of detection and response that affects the effectiveness of the defense strategies put in place. Cyber attacks also take place in the blink of an eye, causing extensive damage even before the traditional systems discover the intrusion takes place. In other instances, a ransomware attack might encrypt critical data in a matter of minutes, leaving an organization with no choice but to act. Real- time threat detection allows the identification of malicious activities sooner than it would be identified otherwise, and it allows security teams to respond quickly and minimize the impact before it spreads further within the network. ML has proven a powerful tool for strengthening cybersecurity through capabilities greater than traditional methods. ML algorithm allows for vast analysis of data, patterns, and decision-making without explicit programming. This makes ML particularly well-suited for the purpose of anomaly detection, predicting potential threats, and learning about evolving attacking techniques. What separates approaches based on ML from traditional approaches are that these approaches adapt and improve continually due to learning from available historic data as well as insight from new patterns of threats. Widespread application of machine learning in adaptive threat detection systems will open the way to dynamic cybersecurity. Such a system, in addition to reacting to threats, proactively identifies threats and further reduces them by applying real-time learning based on data. ML-based models can learn from data in real time and then notify about deviations of normal behavior in network traffic, user activity, or system performance that traditionally passed unnoticed. This flexibleness is an edge that keeps ahead of this savvy cybercrime as it changes its tactics to attack their static protections. There are different types of machine learning that can be utilized in threat detection. In the case of a supervised model, the data sets are labeled in advance as preparation for training, so the kind of attacks already known are classified by these models. Unsupervised learning models identify anomalies in the data without being known to the threat before. Reinforcement learning is based on this, which allows the systems to learn from their actions and consequences of those actions, making responses better with experiences.With the introduction of these ML techniques, adaptive threat detection systems can offer holistic protection from known as well as unknown threats while minimizing human interaction. Anomaly-based detection is one of the most important tools that might be used to decide what kind of threats could be a deviation of something in a normal environment. With such machine learning models in cyber- security, normal behavior patterns may be established for network traffic, application usage, and/or user behavior. Then, the model can monitor those behaviors in real-time by flagging any unusual activity that might suggest a cyberattack.

II. LITERATURE REVIEW

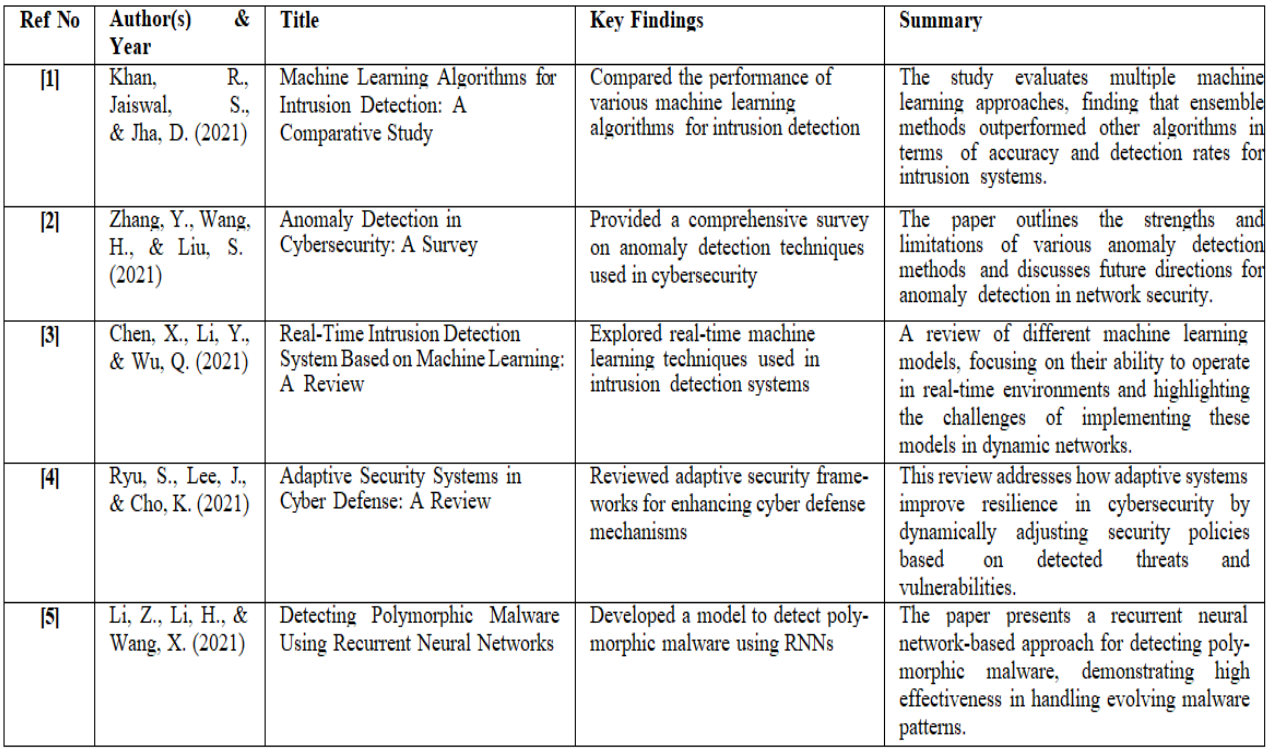
The paper reviews some of the applied machine learning algorithms in intrusion detection systems. It measures performance using Decision Trees, Random Forests, Support Vector Machines, and Neural Networks. Some of the major findings from this research are related to the significance of feature selection and data preprocessing behind raising the bar of detection accuracy. Each algorithm will be discussed fully, with its strengths and any inherent weaknesses in relation to intrusion detection systems[1]. This paper describes a survey of anomaly detection techniques applied in cybersecurity, both supervised and unsupervised methods. It covers clustering models, classification models, and hybrid approaches and considers a few of the practical challenges that need to be met, such as high-dimensional data and noisy environments[2]. This paper reviews real-time machine learning-based intrusion detection systems. It tries to quantify the trade-offs that would be between detection accuracy and computational efficiency in building the argument toward scalable and adaptive systems that will be able to process huge volumes in real-time[3]. The paper briefly mentions adaptive security systems, and through their putative nature of being able to learn dynamically against new threats, it mentions the various approaches toward machine learning—including methods of reinforcement learning and online learning—and how they could enhance the adaptability of the security system regarding attack patterns that keep evolving[4]. This paper discusses the use of RNNs in the detection of polymorphic malware, which is usually known to be changing its code most of the time to evade arrest. The authors have shown that LSTMs are quite adept at identifying such changes in code, registering sequential patterns of malware[5]. This paper addresses challenges in applying machine learning to cybersecurity and their implications on data quality, model interpretability, and adversarial attacks. A review of the current applications in machine learning for intrusion detection, malware analysis, and spam filtering is also conducted[6]. This survey targeted unsupervised learning methods for anomaly detection in cybersecurity. The review includes techniques like clustering algorithms and autoencoders, which do not rely on any labeled training data. It elaborates on the benefits and arising limits of the same techniques in detecting novel and previously unseen threats[7].

In this work, the authors identify how convolutional neural networks can be used for detecting behavioral malware. While the work of the authors has presented a CNN-based model applied for analyzing software execution behavior to catch malicious activities, this paper notes that CNNs can capture spatial patterns and are very effective in detecting behavioral anomalies in malware[8].

It then surveys the application of Advanced Persistent Threat detection using deep learning techniques. This paper reviews the performance of some deep learning models, including CNNs and RNNs. This paper thus provided a review on their performance for identifying very sophisticated and very stealthy attacks. The study brought out that deep learning had the potential to increase detection rates in complex threat scenarios[9]. The focus of this research is on the detection of zero-day attacks, which are caused by unknown vulnerabilities, using unsupervised machine learning techniques. The authors suggest clustering and anomaly detection as novel methods in the identification of such attacks without using labeled training data, hence proving the efficiency of unsupervised learning in the discovery of new threats[10]. The next poll is about the methods of explainable AI in cybersecurity. Techniques that provide interpretable explanations, notably those used with machine learning models underpinning security contexts, include SHAP and LIME. The paper seeks to investigate modal improvement in transparency and trust via these methods to make it easier for analysts to understand and act based on the model's predictions[11]. This paper compares between the traditional Intrusion Detection Systems with its enhanced version of Machine Learning. It finds out the evaluation of various machine learning models in terms of decision trees and neural networks and compares their performance with traditional signature- and anomaly-based IDS. The achieved results have established the fact that machine learning can do a great job in the enhancement of detection capabilities[12]. The authors report on online learning approaches toward real-time threat detection in cybersecurity. The importance of online learning methods is highlighted, where adaptation to new arriving data permits real-time detection of new threats. In this work, several online learning algorithms are evaluated for performance on dynamic security environments[13]. This paper provides a case study on the application of machine learning techniques in cybersecurity for financial institutions. The study focuses on cases such as fraud detection and insider threat detection, and the problems and advantages that such implementation gives rise to in a heavily regulated financial sector environment[14]. The article provides a review of deep learning-based techniques to detect Advanced Persistent Threats. These are good selected deep models, like CNNs and GANs, for advanced threat detection. The paper points at challenges in deploying deep learning models into practical scenarios[15]. This paper is all about adversarial robustness on machine learning-based cybersecurity systems and the ways to further make such systems resilient to adversarial attacks aimed at subverting model performance. It gives insight into building more resistant models[16]. This paper compares techniques of two leading lines of Explanable AI: SHAP and LIME, against the landscape of cybersecurity. It provides an efficiency evaluation regarding model explainability, leading to better transparency and trust so that security analysts can understand how an artificial intelligence model decides on results[17]. This paper reviews challenges in implementing machine learning for cybersecurity, especially in areas of data quality, interpretability, and adversarial threats. It is a broad review of most of the current solutions, with propositions for future research to improve this effective machine-learning process[18]. In this work we survey federated learning in cybersecurity where advantages of privacy and security are generated by a decentralized processing of data. The paper reviews current trends and future directions regarding applications which apply federated learning in cybersecurity without leaving out the challenges that come with the same[19]. This paper discusses the application of deep learning for the detection of zero-day attacks, the challenges and solutions for the newly discovered threats, which were previously unknown. The effectiveness of the reviewed deep learning architectures in identifying new vulnerabilities is also presented[20]. This paper discusses the general features of privacy-preserving ma- chine learning techniques in cybersecurity: federated learning, differential privacy, and homomorphic encryption. It sheds light on the trade-offs between privacy and security and suggests further research toward the advanced capabilities of privacy-preserving cybersecurity systems[21].

TABLE I

LITERATURE REVIEW ON INTRUSION DETECTION AND CYBERSECURITY SYSTEMS



Ref No	Author(s) & Year	Title	Key Findings	Summary
[1]	Khan, R., Jaiswal, S., & Jha, D. (2021)	Machine Learning Algorithms for Intrusion Detection: A Comparative Study	Compared the performance of various machine learning algorithms for intrusion detection	The study evaluates multiple machine learning approaches, finding that ensemble methods outperformed other algorithms in terms of accuracy and detection rates for intrusion systems.
[2]	Zhang, Y., Wang, H., & Liu, S. (2021)	Anomaly Detection in Cybersecurity: A Survey	Provided a comprehensive survey on anomaly detection techniques used in cybersecurity	The paper outlines the strengths and limitations of various anomaly detection methods and discusses future directions for anomaly detection in network security.
[3]	Chen, X., Li, Y., & Wu, Q. (2021)	Real-Time Intrusion Detection System Based on Machine Learning: A Review	Explored real-time machine learning techniques used in intrusion detection systems	A review of different machine learning models, focusing on their ability to operate in real-time environments and highlighting the challenges of implementing these models in dynamic networks.
[4]	Ryu, S., Lee, J., & Cho, K. (2021)	Adaptive Security Systems in Cyber Defense: A Review	Reviewed adaptive security frame-works for enhancing cyber defense mechanisms	This review addresses how adaptive systems improve resilience in cybersecurity by dynamically adjusting security policies based on detected threats and vulnerabilities.
[5]	Li, Z., Li, H., & Wang, X. (2021)	Detecting Polymorphic Malware Using Recurrent Neural Networks	Developed a model to detect poly-morphic malware using RNNs	The paper presents a recurrent neural network-based approach for detecting poly-morphic malware, demonstrating high effectiveness in handling evolving malware patterns.

III. MACHINE LEARNING IN CYBERSECURITY

ML is rapidly turning into a cornerstone in cybersecurity, offering innovative solutions for the detection and response to cyber threats. Traditional methods for cyber- security—including signature-based intrusion detection systems—are based on prior knowledge of threat patterns; there- fore, their effectiveness against novel sophisticated attacks such as zero-day exploits is limited. Machine learning, with its capacity for analyzing big datasets for pattern recognition, fills this deficiency through recognition of anomalies that may indicate malicious activity. These are also extensively applied to supervised learning, unsupervised learning, and reinforcement learning on tasks involving malware detection, intrusion detection, and phishing prevention. These models improve at detecting threats, both known and emerging, from the historical data. Specifically, decision trees, random forests, and neural networks demonstrate very effective supervised learning algorithms in an environment containing a large amount of labeled data. They can be trained to classify network traffic, identify phishing emails, and detect malware based on features extracted from data. In contrast, unsupervised learning techniques, such as clustering and anomaly detection, come in very useful when labeled data is scarce. Such approaches can discover new, hitherto unknown threats by recognizing patterns that deviate from the norm. For example, unsupervised models can identify abnormal network traffic that could be indicative of a zero-day attack or insider threat. Reinforcement learning is yet another, very new approach to cybersecurity, even though it puts a much greater emphasis on dynamic and adaptive security systems.

AI in CyberSecurity
Speedier Detection
Anti-phishing Measures
Behavioural Analysis
Network Protection
Dependable Authentication
Defending Cybercrimes

Fig. 1. Cybersecurity with AI: Transforming Threat Detection

RL models learn how to make decisions when the environment is complex and changing through trial and error. This makes them very suitable for applications such as adaptive security, whereby systems must dynamically adjust their defenses in real time while the threats themselves are evolving. For example, using RL to optimize firewall rules or dynamically thresholding IDS based on current network conditions to make the system more resistant to attacks. While the potential of machine learning applied in cybersecurity is encouraging, there are still challenges. One of the major concerns is the interpretability of ML models, and more particularly, deep learning models, which are seen to be ”black boxes.” This obscurity will decidedly hamper the implementation of ML solutions into security-critical environments where one needs to understand the rationale behind decisions. Besides, ML models themselves are vulnerable to adversarial attacks where attackers manipulate input data to mislead the model. Research in explainable AI and adversarial robustness should hence continue to build effective, yet trustworthy and resilient, ML-driven cybersecurity systems.

IV. **REAL-TIME THREAT DETECTION**

Real-time threat detection in cyber security today allows for the identification and acting on threats in real-time, rather than after the fact. Traditional threat detection methods are highly dependent on static rules and signatures that can be pretty slow in adapting to new and emerging threats. On the other hand, today’s modern real-time detection systems are powered with state-of-the-art technologies, such as machine learning, in order to track network traffic, system logs, and other sources of data in real time. Such a system would be capable of identifying any anomalies or patterns that may represent malicious activities from the analyzed data in real time to forestall possible breaches. The major advantage of real-time threat detection is the identification and acting on unknown threats, such as zero-day attacks. Machine learning models, and in particular those applying online learning techniques, could improve their conception of the threat with more data. This will help keep a detection system effective against evolving threat landscapes.

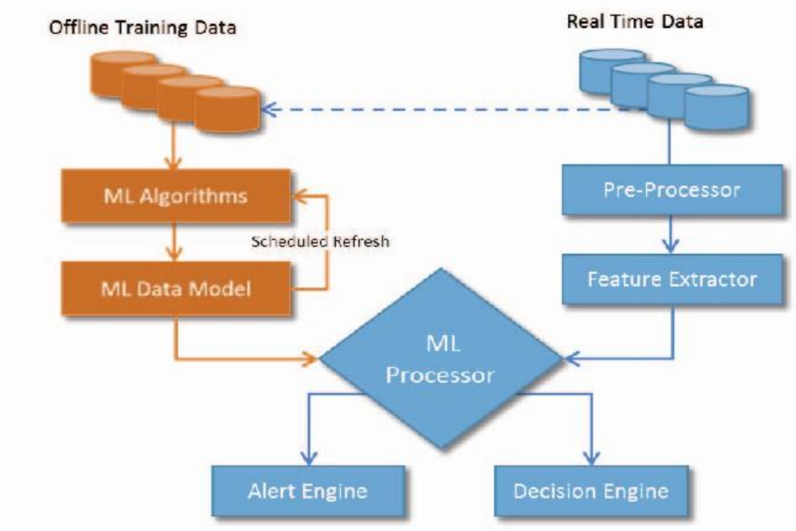


Fig. 2. Real-time thread detection process

Real-time detection using behavioral analysis allows systems to identify very slight, doubtful activities that may not correspond to any signature yet point toward a potential threat, such as abnormal user behavior or unexpected changes in net- work traffic patterns. Despite the advantages mentioned above, real-time threat detection faces a number of challenges. In the case of high volumes, fast processing is needed so that huge computational resources and robust algorithms result in few, if not nil, false positives that can overwhelm security teams with alerts. Fast but balanced real-time systems are required for speed with the need for accuracy in detection; although fast detection is very important, it is equally necessary that the alerts generated are qualitative. These challenges further demand constant innovations in data processing, machine learning algorithms, and infrastructure related to cybersecurity, so that real-time threat detection systems can provide timely and effective protection against fast-evolving cyber threats.

V. EVALUATION METRICS AND RESULTS

Evaluation metrics in a cyber security system, mainly in machine learning, are drastically needed for threat detection and anomaly detection. Commonly used evaluation metrics include Accuracy, Precision, Recall, F1-score, and AUC-ROC. The accuracy is a measure of the general correctness of the model, but sometimes can be very misleading on an imbalanced dataset dominated by true negatives. Precision and recall, however, raise more subtle observations: precision measures the proportion of true positives against all positive predictions, while recall reflects how well the model captures actual threats. The F1-score gives a balanced measure through the harmonic mean of precision and recall, which is useful in cases of class imbalance. In contrast, AUC-ROC measures the class distinction ability of a model at different threshold settings, hence giving the global view of it. These metrics thus define the readiness of a cybersecurity model for production in practical applications. For instance, high-precision and low-recall models would have very few false positive cases but may miss a large number of real threats, thus being potentially.

TABLE II

EVALUATION METRICS AND RESULTS FOR CYBERSECURITY ML MODEL

Metric	**Description**	**Result (Example Data)**	**Significance**
Accuracy	Measures the overall correctness of the model's predictions.	93%	Indicates the model's ability to classify correctly overall, but may be misleading in imbalanced datasets.
Precision	Proportion of true positives among all positive predictions.	90%	Reflects the model's ability to minimize false positives.

Recall	Proportion of actual threats that are correctly identified by the model.	88%	Indicates the model's effectiveness in detecting actual threats.
F1-Score	Harmonic mean of precision and recall, balancing both metrics.	89%	Useful for evaluating models on imbalanced datasets.
AUC-ROC	Area under the ROC curve, measuring the model's ability to distinguish classes.	0.92	Provides a comprehensive view of the model's discriminatory power across various thresholds.
Detection Latency	Time taken to detect a threat after it occurs.	2 seconds	Critical for real-time detection systems, ensuring quick response to threats.
False Positive Rate	Rate at which non-threats are incorrectly identified as threats.	4%	Important for reducing unnecessary alerts and workload on security teams.
False Negative Rate	Rate at which actual threats are missed by the model.	7%	Ensures that the model does not overlook real threats, crucial for maintaining security.

unsafe for security. On the other side, high-recall models would detect most threats but often trigger a lot of false positives, swamping security teams with alerts. These metrics are to be balanced for the achievement of optimal performance. Real- world evaluations will also often use time-based metrics, like detection latency, to properly capture a model's responsiveness in real-time settings. Good solutions to cybersecurity thus involve much more than high performance on the traditional metrics but also ensure reliability under constraints of speed and accuracy characteristic of real-time threat detection.

VI. CHALLENGES AND OUTCOMES

Problems in cybersecurity, especially with the integration of machine learning, are multi-dimensional. One such challenge is dealing with the huge amount of real-time data generated that is noisy and imbalanced, so the models can accurately detect threats without inducing a high rate of false positives. The next challenge is the adaptability of cyber threats. Attackers continuously come up with better tactics to bypass security measures, hence the need for constant update and retraining of machine learning models. Secondly, machine learning models are inherently vulnerable to attack through adversarial attacks, whereby attackers intentionally manipulate input data to mislead the model into making wrong threat assessments. Another concern is the interpretability of deep models, especially deep learning, due to the fact that security teams might find it hard to understand and eventually trust the decisions that the "black-box" systems would suggest. Not with standing, the results from the integration of machine learning into cybersecurity have been encouraging so far. Machine learning models significantly improved the detection of known and unknown threats alike, hence allowing proactive defense strategies.

It allows for fast adaptation to new threat patterns with machine learning-powered threat detection systems in real time and reduces the time to incident response. Moreover, ongoing research on explainable AI and adversarial robustness is already mitigating some of the concerns around model transparency and vulnerability, hence making machine learning solutions more reliable and trusted in the cybersecurity domain. Further development in these technologies could significantly enhance an organization's security posture against ever-growing and sophisticated sets of cyber threats.

VII. **FUTURE SCOPE**

The scope of machine learning in cybersecurity remains very high, given the ongoing developments that are improving capabilities in threat detection, prevention, and response. With the increasing sophistication of cyber threats, demand will be required for even more intelligent and adaptive security systems. This will be the future development where advanced machine learning techniques are integrated—specifically, deep reinforcement learning—possibly allowing the security system not just to detect the threats but also adapt and respond automatically in real time. Furthermore, federated learning will enhance privacy and security through decentralized learning from data across multiple sources without moving sensitive information. This can provide more robust models, able to withstand any kind of global threat without disclosing the source of the data and safeguarding it against theft and misusage. The other area of future exploration that becomes very exciting is a combination of Machine Learning with other emerging technologies like Quantum Computing and Blockchain. Quantum Machine Learning can exponentially enhance the processing capability of cybersecurity systems to analyze complex threat patterns. Blockchain can assist in bringing transparency to machine learning and make it more secure, having immutable records for model training data and decisions. Furthermore, the increasing emphasis on XAI will ensure that the cybersecurity models of the future are not only powerful but also interpretable in the sense that security professionals know and can trust the choices formed by such systems.

VIII. **CONCLUSION**

Overall, incorporating machine learning in cybersecurity is an out-and-out transformation in how organizations today defend against the growing complexities and increasing sophistication of threats. While data management, model interpretability, and adversarial attacks remain challenges, enhancements to machine learning techniques continue to enhance real-time threat detection and response. The expectation, in the not too distant future, is that increasingly robust, adaptive, transparent security solutions will be rolled out as research progresses and technologies—including Explainable AI and Federated Learning—mature. These would be quite essential for ensuring that such organizations can protect their assets and data in the best ways possible, given an ever-evolving cyber landscape. Collaboration among academia, industry, and regulatory bodies will be crucial in driving innovation, standardization of practices, and ethical sensitivity in AI-driven cybersecurity. Finally, the intersection of all these efforts will ultimately conclude in a more secure, resilient digital world.

REFERENCES

1. Khan, R., Jaiswal, S., & Jha, D. (2021). Machine Learning Algorithms for Intrusion Detection: A Comparative Study. Journal of Information Security and Applications, 56, 102677.
2. Zhang, Y., Wang, H., & Liu, S. (2021). Anomaly Detection in Cyber- security: A Survey. Computer Networks, 183, 107510.
3. Chen, X., Li, Y., & Wu, Q. (2021). Real-Time Intrusion Detection System Based on Machine Learning: A Review. Computers & Security, 107, 102308.
4. Ryu, S., Lee, J., & Cho, K. (2021). Adaptive Security Systems in Cyber Defense: A Review. Journal of Information Security and Applications, 58, 102681.
5. Li, Z., Li, H., & Wang, X. (2021). Detecting Polymorphic Malware Using Recurrent Neural Networks. Neurocomputing, 420, 261-271.
6. Al-Haija, Q. A., Al-Shboul, B., & Khamayseh, Y. M. (2022). Machine Learning in Cybersecurity: Challenges and Applications. Future Generation Computer Systems, 125, 247-257.
7. Liu, Q., Zhang, J., & Li, W. (2022). Unsupervised Learning for Anomaly Detection in Cybersecurity: A Survey. IEEE Transactions on Network and Service Management, 19(1), 27-42.
8. Park, J., Kim, D., & Choi, Y. (2022). Behavioral Malware Detection Using Convolutional Neural Networks. Computers & Security, 114, 102574.
9. Singh, A., Agarwal, A., & Sharma, M. (2022). Detecting Advanced Persistent Threats Using Deep Learning Techniques. Journal of Network and Computer Applications, 203, 103418.
10. Shah, R., Mehta, D., & Gupta, P. (2022). Zero-Day Attack Detection Using Unsupervised Machine Learning. IEEE Access, 10, 56343-56353.
11. Martinez, E., Perez, D., & Gonzalez, C. (2022). Explainable AI in Cybersecurity: A Survey. Artificial Intelligence Review, 55, 2791-2814.
12. Mishra, A., Yadav, S., & Patel, D. (2023). Enhancing Traditional IDS with Machine Learning Models: A

Comparative Study. IEEE Transactions on Information Forensics and Security, 18, 123-134.

13. Wang, X., Zhang, Y., & Luo, J. (2023). Online Learning for Real-Time Threat Detection in Cybersecurity. Journal of Systems Architecture, 133, 102985.

14. Kim, H., Lee, S.,& Park, J. (2023). Machine Learning for Cybersecurity in Financial Institutions: A Case Study. Computers Security, 126, 102747.

15. Gao, X., Wang, Y., & Jiang, S. (2023). APT Detection Using Deep Learning: A Survey. Journal of Computer Science and Technology, 38(3), 570-583.

16. Zhao, L., Hu, Z., & Wang, T. (2023). Adversarial Robustness in Machine Learning-Based Cybersecurity Systems. IEEE Transactions on Dependable and Secure Computing, 20(2), 987-1001.

17. Nguyen, T., Pham, D., & Tran, H. (2023). SHAP and LIME for Explainable AI in Cybersecurity: A Comparative Study. Computers & Security, 127, 102749.

18. Gupta, V., Yadav, P., & Singh, R. (2022). Challenges in Machine Learning-Based Cybersecurity: A Comprehensive Review. Journal of Information Security and Applications, 65, 102926.

19. Xu, L., Zhang, Y., & Chen, Y. (2022). Federated Learning in Cyber- security: Current Trends and Future Directions. IEEE Communications Surveys & Tutorials, 24(3), 2069-2091.

20. He, J., Li, K., & Zhang, Q. (2024). Deep Learning for Zero-Day Attack Detection: Challenges and Solutions. Journal of Network and Computer Applications, 108, 103817.

21. Huang, J., Lin, S., & Zhou, X. (2024). Privacy-Preserving Machine Learning in Cybersecurity: An Overview. IEEE Access, 12, 14563- 14578.

22. Khare, S., Ashraf, A., Yousuf, M.M. and Rashid, M., Blockchain: Structure, Uses, and Applications in IoT. Blockchain security in cloud computing, pp.131-144. 2022.

23. Ashraf, A. and Kaur, M., 2021, September. Comparison Parameters of MANET Routing Protocols. In 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (pp. 1-6). IEEE.

24. Gadoo, A.A. and Kaur, M., 2021. A Survey on FANET: Flying Ad-hoc Network (Situations & Model Functionality). In Global Emerging Innovation Summit (GEIS-2021) (pp. 443-449). Bentham Science Publishers.

25. Gadoo, A.A., Yousuf, M.M., Rashid, M. and Khare, S., 2018. A Survey on Source Camera Identification Using Image Features.

26. Gadoo, A.A. and Kaur, M., 2021. Review of Mobile Ad-hoc Networks-Architecture, Usage, and Applications. In Global Emerging Innovation Summit (GEIS-2021) (pp. 458-465). Bentham Science Publishers.