ESP-IJACT
ESP International Journal of Advancements in Computational Technology
ISSN: 2583-8628 / Volume 3 Issue 1 February 2025 / Page No: 140-148
Paper Id: IJACT-V3I1P115 / Doi: 10.56472/25838628/IJACT-V3I1P115

Research Article

Machine Learning-Based Detection of Malware Threats: A Proactive Approach to Cybersecurity

Nishchai jayanna Manjula[1], Srikanth Daggumalli[2]
[1]*Senior Solutions Architect- Data and AI, United States.*
[2]*Senior Analytics & AI Specialist Solutions Architect at Amazon Web Services United States.*

Received Date: 10 December 2024 Revised Date: 21 January 2025 Accepted Date: 12 February 2025

Abstract: *With the increasing speed and complexity of cyber attacks malware remains one of the most significant cybersecurity threats faced by organizations, individuals and governments. Traditional signature detection systems struggle to keep pace with evolving zero-day threats, making Machine Learning (ML) a crucial component of modern cybersecurity. With applications in intrusion detection malware analysis fraud prevention and real-time security response systems ML plays a key role in the detection of threats, prevention and incident response. However integrating ML into cybersecurity presents several challenges. The dynamic nature of cyber threats demands regular model updates. At the same time high-quality data, frequent false alarms, vulnerability to attacks and limited resources make its use more difficult. Additionally privacy and ethical concerns related to data collection and monitoring pose significant hurdles. Despite these challenges, ML techniques continue to evolve with advancements in data sharing and privacy regulations driving its responsible use. If these obstacles are effectively addressed ML can provide more adaptive, scalable and efficient cyber security solutions strengthening defense mechanisms against advanced cyber threats.*

Keywords: *Machine Learning, Cybersecurity, Malware, Response, Detection.*

I. INTRODUCTION

Cybersecurity is the study of safeguarding information, systems, and networks from threats, damage, or unauthorized access [1]. The growing number of connected devices, systems, and networks, along with the expansion of the digital economy, has made cybersecurity more complex. As a result, cyber incidents have sharply increased, causing serious consequences. Skilled attackers, including state-backed groups and criminal organizations, persist in their attempts to breach even the most secure networks. Threats like unauthorized access, DoS attacks, botnets, malware, and worms (along with others shown in Figure 1) have become more severe over time, putting organizations at risk of disruption and financial loss [2][3].

Figure 1: Types of Attacks

Traditional signature-based security systems use predefined rules and known malware signatures, but they have failed to keep up with modern threats especially zero-day vulnerabilities [18]. These evolving threats require intelligence-based cybersecurity solutions that can adapt to new risks and manage large amounts of data. A precautionary approach, supported by organizations like the National Institute of Standards and Technology (NIST) includes conducting assessments scans and auditing in real time along with regular monitoring and analysis of collected data to detect[4].

Real-world malware detection systems need fast and effective data analysis tools. Traditional techniques like signature detection are no longer enough to detect modern malware, which evolves quickly [16][17]. Security researchers suggest using attack pattern identification to strengthen defenses against growing cyber threats. Studies show that only 10%

of malware was flagged as malicious and 70% of attacks on Windows endpoints went undetected and only 20% were recognized and reported [15]. To address these challenges Machine learning technologies play a key role. ML enables the smart processing of security data, allowing systems to learn from past threats and continuously improve security measures. By using ML cybersecurity systems can detect and respond to new and evolving threats more effectively making them better suited for today's complex digital landscape.

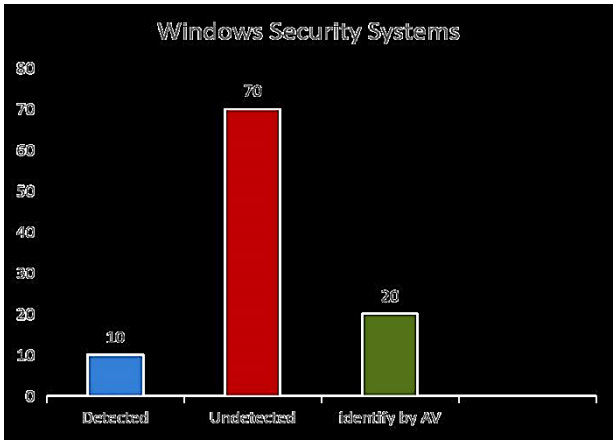

Figure 2: Limitations of Traditional Security Solutions

This research targets leveraging machine learning techniques to enhance cybersecurity, particularly in malware detection intrusion detection and automated threat response. It evaluates various ML models and tests traditional approaches such as decision trees and support vector machines with deep learning models like deep neural networks and convolutional neural networks to determine the most effective detection methods. A key aspect of this study is the exploration of hybrid detection approaches integrating static and dynamic analysis to improve accuracy especially against obfuscated and packed malware. Further the research addresses the challenge of reducing false positives by optimizing feature selection and engineering techniques. It also examines adversarial challenges including model interpretability computational constraints and resilience against evasion techniques. This study also offers future research directions such as adaptive learning, explainable AI federated learning, and blockchain based threat intelligence for contextualization and improvement in robust and scalable ML driven cybersecurity solutions.

II. CYBER SECURITY AND MACHINE LEARNING

This section gives a brief summary on the concept of cybersecurity and artificial intelligence (AI). Explanation of cybersecurity and role in preventing data from cyber threats to systems network, it explains. It also describes the use of artificial intelligence for improved cybersecurity through machine learning and pattern recognition. It acted as a background to comprehend how Artificial Intelligence (AI) driven solutions are tackling evolving cyber threats.

In today's digital world, cybersecurity is a top priority as everyone has an array of connected systems, networks and devices all at their fingertips. It grants protection against cyber attacks by focusing on safety with respect to networks and information security. With more and more frequent and complex cyber threats, strong smart security solutions are crucial. Traditional security methods do give a measure of security but are not good enough in protecting against the ever changing modern cyber threats.

Artificially intelligent content and in particular machine learning is essential to enhancing cybersecurity. Data can be analyzed, unusual patterns of activity can be detected and potential cyber attacks can be predicted – all that can be done by running an ML algorithm in real time, thereby reducing risks. Security systems that are constantly learning new threats so they can adjust fast to new attack method. Thereby making ML an invaluable asset to the digital fortification and securing of digital assets from novel threats. In recent research we look at the intersection of cybersecurity and machine learning, how can advance technologies improve threat detection and response. Classification clustering deep learning and hybrid approaches to tackle evolving cyber threats are evaluated that look at machine learning techniques in the process. The following sections go through these works that explore the obstacles of malware detection and intrusion prevention, and inquire what benefits of ML could make automated security more reliable, less prone to false positives, and much more. In particular, [6] research The potential of machine learning algorithms to detect cyber anomalies and cyber attacks, and multi class cyber attacks by observing the report which looks at The CyberLearning model. It includes different ML methods for classifying and predicting malicious behavior in the cybersecurity system. They are evaluated on a range of algorithms such as Random Forest (RF), Naive Bayes, Logistic Regression, SVM Decision Trees, XGBoost and Artificial Neural Network to assess the performance of the models on UNSW-NB15 and NSL-KDD datasets on both real world network traffic data.

Another contribution of this study is the use of the Pearson correlation coefficients for feature selection such that data dimensionality is reduced without losing accuracy of the model. Among tested algorithms, random forest succeeded in 95% accuracy on anomaly detection of UNSW-NB15 and 99.9% accuracy on NSL-KDD and this indicates that Random Forest is robust to handle the different cyber threats. The emphasis on this is on how algorithm selection and feature engineering improve ML based cybersecurity solutions. Therefore real time intrusion detection using ML could be said to be proved effective for real time intrusion detection in the study. It is a big step towards developing an AI driven security framework.

As seen in (7), machine learning (ML), is seen to be a trans-formative technology in cybersecurity, enabling both the automation of the data analysis, threat detection, and incident response. Security gaps such as intrusion detection, malware analysis, botnet traffic detection and Deep Learning are filled up using ML techniques like classification, regression, clustering, rule based modeling and deep learning which effectively deal with such issues. This research also considers the ways in which malware can be packed to hide malicious code, and so avoid being detected. Packers usually have their set of packers attacking to pack their malware to avoid detection, and ML Classifiers can easily train to detect packed malware, but the classifiers developed biases towards particular packers of malware (leading to false positives). Encrypted and packing techniques are correlated with classifiers that cannot generalize very well.

The study proposes a hybrid approach incorporating static and dynamic analysis with a static analysis, and is suggested to improve the malware detection. It helps detecting behavioral patterns that cannot be identified by static analysis and increases overall detection accuracy. The whole study shows the importance to be made these adaptive real time security solutions by combining ML with the novel technologies like blockchain and adversarial machine learning to tackle ongoing cyber threats properly.

The research [8] investigates how machine learning can improve malware detection by considering the effect that static analysis and packing have on machine learning classifiers. As illustrated by the study, although software authors packing techniques designed to obfuscate malicious code make it harder to detect malicious code, they remain far from being fully immune to them. However, classifiers will encounter cases with strong encryption, and new packing methods, which may cause many cases to be false negatives and missed detection.It also makes one of the key contributions to study about packed malware limitations in the static analysis. The research however does not confirm that the static analysis methods cannot accurately identify the malware applying advanced packing methods. Static analysis is less effective against malware that is meant to hide from viewing, because it does not execute the file. The study suggests that dynamic analysis and observing the runtime behavior of an executable should be integrated together. It provides a more complete view and does provide some detection that static analysis will omit, and is therefore a very important supplement to other methods.

It also goes on the look at the issues posed by packing and encryption. "Static analysis will not automatically infer malicious intent, in other words," it states, pointing out that packing by itself does not make writing an executable automatically malicious and that strong encryption will block static analysis from detecting malware, even though strong encryption is not inherently malicious. The paper highlights the need for hybrid approach in detection, a combination of static and dynamic analysis, in order to overcome these applied challenges. Integrating dynamic features classifier can become more adaptable by means of dynamic classifiers, which helps in making the classifier more adaptable allowing for better performance on a broader class of malware While this method is vital since the malware tactics evolve using advanced packing or locking techniques, the study advises an augmentation of ongoing improvements in conducting the trainer with the continuously changing landscape of malware threats.

Various researcher have recommended an inventive machine learning technique for detecting dangerous Remote Desktop Protocol (RDP) sessions, a main point of interest during advanced essential precariousness. This study uses Windows event logs to generate machine learning models with the aim to classify RDP sessions as benign or malicious to enhance the APT event detection accuracy.It also shows that LogitBoost (LB) outperforms other classifiers such as Logistic Regression LR Decision Trees DT Random Forest RF and Feed-forward Neural Networks (FNN), providing the highest precision The study also investigates adversarial attacks showing that the proposed model remains resilient against specific adversararial manipulations - a crucial feature for practical application in intrusion detection systems. The authors note the limitations of ensemble methods like MV and WV Majority Voting (WV), pointing out that combining them with standalone classifiers did not improve detection accuracy.

The methodology centers on supervised machine learning using critical event IDs from Windows log files (4624, 4625 and 4634) to detect patterns of RDP sessions. The dataset comprises 56,837 events offering a thorough overview of both harmful and benign activities. Cross-validation was employed to assess the model's performance in ensuring reliable and trustworthy outcomes. Despite challenges related to imbalanced datasets LogitBoost proved to be the most effective model demonstrating resilience against adversarial threats.It emphasizes the importance of feature selection in machine

learning models for cybersecurity and proposes directions for future research such as integrating dynamic analysis with static feature extraction and increasing datasets to improve model generalization.

Machine learning (ML) is transforming cybersecurity by empowering smart and automatic threat detection. A multi-layered cybersecurity solution that includes ML methods such as feature engineering, clustering, classification, and deep learning strengthens security by anticipating and preventing cyber attacks in advance.Critical issues are dealing with big, varied security data, model generalization, avoiding bias, and increasing interpretability [10]. Discovering behavior patterns in security data is critical when building prediction models. K-means clustering, hierarchical clustering, and PCA facilitate the processing of complex security data effectively.ML-based cybersecurity enhances automation and reaction to new threats. Future developments need to emphasize hybrid detection techniques, real-world use cases, and resolving scalability and adaptability, especially in IoT and cloud security, to create more effective and proactive security systems.

Comparative evaluation of ML models [19] indicates that deep neural networks (DNNs) perform better than conventional models such as decision trees and support vector machines in terms of F1 score and accuracy. The DNN model attains the highest accuracy (96.3%) and lowest false positive rate (1.2%), which proves its efficiency in distinguishing benign and malicious files. Deep learning models, however, require extensive computational power and are not interpretable because of their "black-box" nature.

Despite these limitations, ML-based malware detection tools are an iterative and scalable approach to zero-day threat detection. The future should aim at enhancing the interpretability of deep learning models and minimizing computational overhead for the sake of greater practicality in real-world applications of cybersecurity.Table 1 gives a summary of the different machine learning methods and how they are being used in cybersecurity, emphasizing detection, automation, and malware analysis. It compiles major research areas, algorithms, datasets, and primary conclusions from various research studies.

III. METHODOLOGY USED IN ML BASED MALWARE DETECTION

Malware detection has a systematic approach to detect malicious files accurately with minimal false positives. The methodology includes the following major steps[20]:

A. Data Collection and Malware Analysis

The initial step is gathering malware and benign samples from open repositories such as Malware Bazaar, Virus Share, and the Malware Capture Facility Project. For better detection, gathered samples are subjected to malware analysis, which aids in the extraction of valuable information regarding their behavior and attack patterns. Analysis is conducted with three main techniques:

- Static Analysis: Analyzing the malware file without running it (e.g., looking at headers, strings, and binary patterns).
- Dynamic Analysis: Executing malware within a contained (sandbox) environment to monitor its actual operation in real time.
- Hybrid Analysis: Integrating static and dynamic methods to present a complete image of malware traits.

B. Feature Engineering

After malware behavior is grasped, the features that are applicable are derived in order to increase detection rates. The features that are derived are byte patterns, execution patterns, system calls, code constructs, and network communications. Selecting the appropriate features ensures the model can clearly distinguish between malware and clean files.

Table 1. Machine Learning Approaches and Applications in Cybersecurity: Detection, Automation, and Malware Analysis

Name	Focus Area	Key Algorithms	Dataset Used	Main Findings
CyberLearning Model	Cyber-Anomalies & Multi-Attacks	Random Forest, SVM, Naive Bayes, XGBoost, ANN	UNSW-NB15, NSL-KDD	Random Forest performs best
Machine Learning for Data Analysis	Proactive Threat Detection & Automation	Classification, Regression, Deep Learning	N/A	Automation, Incident Response, Predicting Threats
Packed Executables in Malware Detection	Packed Malware Detection using Static Features	SVM, MalConv (Neural Network), Random Forest	392,168 Executables (Benign & Malicious)	Packing does not prevent detection, but strong encryption hinders it

Role of Machine Learning in Malware Detection	Enhancing Malware Detection using Static/Dynamic Analysis	Machine Learning, Dynamic Analysis	N/A	Hybrid approaches (Static & Dynamic)
Detection of Malicious RDP Sessions in APTs	Detection of Malicious RDP Sessions during Lateral Movement in APTs	LogitBoost (LB) outperforms other models in terms of precision and recall	Combined dataset from LANL with red team events for real-world simulation	LogitBoost (LB) classifier achieved high precision and recall and was robust against adversarial attacks
Cybersecurity Data Science: An Overview from Machine Learning Perspective	Cybersecurity Data Science: Leveraging ML for intelligent, data-driven decision-making.	Feature engineering, data clustering (K-means, hierarchical clustering), classification, PCA.	N/A	Techniques like feature engineering, clustering, classification, and deep learning enhance threat detection and automation.
Machine Learning-Based Malware Detection	Enhancing malware detection using machine learning to improve accuracy and adaptability against zero-day threats.	Random Forest, Deep Neural Networks (DNN), Decision Trees, Support Vector Machines (SVM)	Not explicitly mentioned in the text	The DNN model achieves the highest accuracy (96.3%) with a low false positive rate (1.2%), while Random Forest also performs well (94.2% accuracy). Despite improving malware detection, deep learning models require high computational power and lack interpretability, necessitating further research on efficiency and transparency.

C. Model Selection and Training

Machine learning models are chosen depending on how well they can identify malware. Some of the most common models used are:

- Decision Trees: It function by constructing a flowchart-like model where every node corresponds to a decision based on feature values. They offer an understandable and interpret-able method, so it is simple to comprehend why a file has been classified as malware or benign.
- Random Forests: it improves decision trees by producing an ensemble of several trees, minimizing overfitting and maximizing accuracy. They are especially useful in dealing with high-dimensional datasets with rich malware features.
- Support Vector Machines (SVM): Support Vector Machines (SVMs) are suitable for binary classification, separating malware from normal files by determining the best hyperplane for separation. Kernel functions such as linear, polynomial, and radial basis function (RBF) improve performance by dealing with non-linearly separable data.
- Deep Neural Networks (DNN): Deep Neural Networks (DNNs) successfully identify advanced malware, such as zero-day attacks, by learning intricate patterns. Though computationally expensive and uninterpreted, network architectures such as CNNs derive features from byte streams, and RNNs determine behavior patterns within system calls and API calls.

The chosen models are trained on labeled data, and cross-validation methods are used to improve generalization and avoid overfitting.

D. Validation and Performance Assessment

Trained models are tested with critical performance measures including:

Accuracy: The rate at which correctly classified samples occur.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision and Recall: Balancing the detection of malware with reducing the amount of false alarms.

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

F1-Score: A harmonic mean of precision and recall for overall performance.

$$F1 = \frac{2\ X\ precision\ X\ Recall}{precision\ +\ Recall}$$

False Positive Rate: Minimizing false alerts for benign files.

$$FPR = \frac{FP}{FP + TN}$$

Particular focus is given to enhancing the detection of zero-day malware with a low false positive rate to guarantee system reliability.

E. Adaptive Learning and Deployment

As malware is ever-changing, detection systems must be adaptive and scalable. Ongoing updates to datasets and model retraining assist in enhancing detection capabilities. Real-time threat intelligence feeds can also be incorporated to improve responsiveness against new threats. Through this systematic methodology shown in Figure 3, machine learning-driven malware detection systems become more efficient, accurate, and resistant to emerging cyber attacks.

IV. POTENTIAL APPLICATIONS OF MACHINE LEARNING IN CYBERSECURITY

Machine learning has revolutionized cybersecurity by providing automated and accurate threat detection and prevention. The main applications are:

- **Network Risk Scoring**: Examines past threat information to detect risky points in a network, which can help in assessing risk and resource allocation.
- **Intrusion Detection**: Tracks and detects malicious actions in real time, enabling quicker and more effective reaction to security threats.
- **Suspicious Behavior Identification**: Identifies anomalous user behavior, such as out-of-pattern login attempts or large file downloads, to avoid unauthorized access.
- **Fraud Detection**: Employs pattern recognition and anomaly detection methods to anticipate and stop financial frauds.
- **Malware Analysis**: Analyzes historical patterns of attacks to identify, categorize, and stop malware attacks.
- **Cyber-Anomaly Detection**: Detects and classifies security anomalies and multi-vector attacks based on behavioral analysis.
- **Predictive Incident Response**: Forecasts possible cyber breaches and initiates automated defense responses prior to an attack.
- **Task Automation**: Automates repetitive security tasks, such as malware analysis, vulnerability scanning, and log monitoring, to enhance efficiency and scalability.

Through the use of these applications, machine learning strengthens cybersecurity defenses, enabling organizations to react to threats in advance while reducing manual labor.

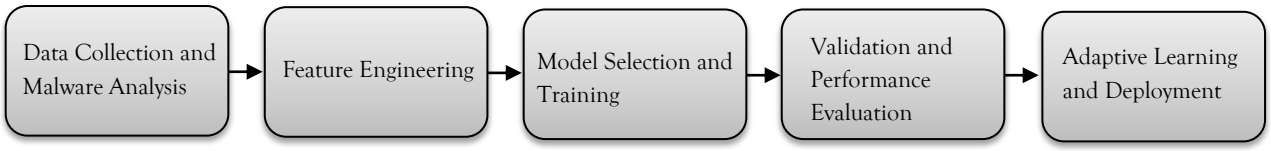

Figure 3. Methodology used in ML based detection

V. CHALLENGES IN CYBERSECURITY

A. Evolving Threat Landscape

Cybersecurity is under constant threat from new and evolved threats as the attackers come up with more complex methods. Polymorphic malware transforms its code to remain undetected, while AI-driven cyber attacks expand phishing

emails, ransomware, and other malicious practices. Zero-day exploits, which take advantage of unknown vulnerabilities in software, are dangerous as no defenses beforehand are available against them. Moreover, the fast growth of IoT devices has escalated the attack surface, and it has become more difficult to detect and block security breaches [11].

B. Data Availability and Quality

Machine learning models need large-scale, high-quality data for successful training. Due to privacy, it is tough to get variable and well-balance cybersecurity information. Most of the organizations resist sharing breach records publicly, and the absence of standardized data procurement practices results in variability. Those models trained over biased or lacking datasets can overlook advanced cyber attacks, and the availability of the data becomes an important challenge [12].

C. High False Positives and False Negatives

Machine learning-driven cybersecurity systems tend to find it difficult to differentiate between genuine threats and benign activities. False positives are created when valid actions are identified as threats, clogging security teams and resulting in alert fatigue. In contrast, false negatives, where real cyber attacks remain undetected, leave organizations vulnerable to critical risks. Obtaining high accuracy while keeping errors low is still a major challenge, especially for real-time security applications where even slight delay or inaccuracy can prove disastrous [1].

D. Adversarial Attacks

Cyber criminals can also trick machine learning models into avoiding detection. Adversarial attacks involve subtle but targeted changes to malware files so that they can circumvent security filters. Data poisoning is another serious threat where attackers introduce deceptive or malicious data into training sets, which undermines the accuracy of the model. All these threats indicate the pressing need for stronger defense mechanisms that can identify and neutralize adversarial manipulations without affecting model performance [14].

VI. CONCLUSION

The integration of machine learning (ML) in cybersecurity threat detection has tremendously improved the capability to detect, counteract, and react to advanced cyber threats. Classical rule-based security tools, as powerful as they are in the identification of well-known threats, fail to cope with the very dynamic nature of cyber attacks. ML algorithms, especially those employing supervised, unsupervised, and reinforcement learning, have proved impressive in detecting anomalies, identifying attack patterns, and enhancing threat intelligence. The use of deep learning, neural networks, and ensemble techniques has further increased the accuracy and agility of these models.

Despite all these developments, there are issues with the reliability, interpret-ability, and resiliency of ML-based security systems. There are still ongoing challenges in problems like adversarial attacks, scarcity of data, and model generalization. Besides, the necessity for large sets of labeled training data and computer resources hampers the utilization of ML within cybersecurity, particularly for small to mid-sized entities. Nevertheless, research is on the way towards overcoming these barriers through federated learning, transfer learning, and explainable AI methods.

In conclusion, ML-based cybersecurity tools have revolutionized threat detection approaches by allowing real-time, adaptive, and proactive defense mechanisms. These developments add to a more robust cybersecurity infrastructure that can effectively counter the increasingly sophisticated methods used by cyber criminals. Nonetheless, ongoing research and development are necessary to break through current limitations and further increase the efficiency of ML-based threat detection systems.

VII. FUTURE WORK

Future research on ML-based cybersecurity threat detection needs to concentrate on a number of important areas to handle the existing constraints and investigate new possibilities. The most important area is adversarial machine learning, addressing the problem of creating more robust models that can identify and counter adversarial attacks. Attackers keep changing their methods to stay undetected, so it is crucial to increase the resistance of ML algorithms against adversarial manipulations.

Another promising avenue is the use of self-supervised and semi-supervised learning, which can minimize the reliance on large labeled datasets. With the challenge of acquiring high-quality labeled cybersecurity datasets, the use of methods that employ unlabeled data for model training can greatly enhance the practicality and scalability of ML-based threat detection systems. Additionally, explainable AI (XAI) will be pivotal in the future of ML-based security solutions. It is imperative that ML model decisions are interpret-able and explainable in order to gain confidence and adhere to regulatory standards. Future research needs to work towards the development of interpretable ML models that give actionable and clear insights to security analysts.

Furthermore, the combination of ML with blockchain technology can be used to boost cybersecurity through a decentralized and tamper-evident method of threat intelligence sharing. Blockchain-based security architectures can provide data integrity, minimize single points of failure, and facilitate secure collaboration between organizations. Finally, real-time threat detection and auto-response functions based on ML and AI will develop further. Future studies need to focus more on minimizing false positives and false negatives in the detection of threats while enhancing the efficiency of automated response systems. Integration of ML with AI-powered SOAR platforms will further advance cybersecurity resilience. By solving for these future trends, ML-powered cybersecurity solutions are able to go beyond and implement better, dynamic, and intelligent threat detection technologies. The synergy among ML, cybersecurity, and future technologies presents an enormous prospect of creating a more secure digital world.

VIII. REFERENCES

[1] Akashdeep Bhardwaj et al., "Secure Framework against Cyber-attacks on Cyber-Physical Robotic Systems," *Journal of Electronic Imaging*, vol. 31, no. 6, 2022. Google Scholar | Publisher Link

[2] Premkumar Chithaluru et al., "Computational-Intelligence-Inspired Adaptive Opportunistic Clustering Approach for Industrial IoT Networks," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7884-7892, 2023. Google Scholar | Publisher Link

[3] Iqbal H Sarker et al., "IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model," *Symmetry*, vol. 12, no. 5, pp. 1-15, 2020. Google Scholar | Publisher Link

[4] Barrett, Technical Report, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2018.

[5] Iqbal H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," *SN Computer Science*, vol. 2, pp. 1-21, 2021. Google Scholar | Publisher Link

[6] Iqbal H. Sarker, "CyberLearning: Effectiveness Analysis of Machine Learning Security Modeling to Detect Cyber-Anomalies and Multi-Attacks," *Internet of Things*, vol. 14, 2021. Google Scholar | Publisher Link

[7] Iqbal H. Sarker, "Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects," *Annals of Data Science*, vol. 10, pp. 1473-1498, 2023. Google Scholar | Publisher Link

[8] Hojjat Aghakhani et al., "When Malware is Packin' Heat; Limits of Machine Learning Classifiers Based on Static Analysis Features," *Network and Distributed System Security Symposium*, San Diego, United States, pp. 1-21, 2020. Google Scholar | Publisher Link

[9] Tim Bai et al., "RDP-Based Lateral Movement Detection using Machine Learning," *Computer Communications*, vol. 165, pp. 9-19, 2021. Google Scholar | Publisher Link

[10] Iqbal H. Sarker et al., "Cybersecurity Data Science: An Overview from Machine Learning Perspective," *Journal of Big Data*, vol. 7, pp. 1-29, 2020. Google Scholar | Publisher Link

[11] Robin Sommer, and Vern Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," *IEEE Symposium on Security and Privacy*, Oakland, CA, USA, pp. 305-316, 2010. Google Scholar | Publisher Link

[12] Anna L. Buczak, and Erhan Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153-1176, 2016. Google Scholar | Publisher Link

[13] Iftikhar Ahmad et al., "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection," IEEE Access, vol. 6, pp. 33789-33795, 2018. Google Scholar | Publisher Link

[14] "IEEE Transactions on Information Forensics and Security Publication Information," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. C2-C2, 2011. Publisher Link

[15] Frederick Barr-Smith et al., "Survivalism: Systematic Analysis of Windows Malware Living-Off-The-Land," *IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, pp. 1557-1574, 2021. Google Scholar | Publisher Link

[16] Muhammad Shoaib Akhtar, and Tao Feng, "Malware Analysis and Detection Using Machine Learning Algorithms," *Symmetry*, vol. 14, no. 11, pp. 1-11, 2022. Google Scholar | Publisher Link

[17] Anand Handa, Ashu Sharma, and Sandeep K. Shukla, "Machine Learning in Cybersecurity: A Review," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 9, no. 4, 2019. Google Scholar | Publisher Link

[18] Mujeeb Ur Rehman Shaikh et al., "Fortifying Against Ransomware: Navigating Cybersecurity Risk Management with a Focus on Ransomware Insurance Strategies," *International Journal of Academic Research in Business and Social Sciences*, vol. 14, no. 1, pp. 1415-1430, 2024. Google Scholar | Publisher Link

[19] Iqra Naseer, "System Malware Detection Using Machine Learning for Cybersecurity Risk and Management," *Journal of Science & Technology*, vol. 3, no. 2, pp. 182-188, 2022. Google Scholar | Publisher Link

[20] Sudhir Kumar Pandey, and B.M. Mehtre, "A Lifecycle Based Approach for Malware Analysis," *Fourth International Conference on Communication Systems and Network Technologies*, Bhopal, India, pp. 767-771, 2014. Google Scholar | Publisher Link