Advancing Cybersecurity Through Machine Learning: Bridging Gaps, Overcoming Challenges, and Enhancing Protection

Abstract: The greatest technical achievement of the twenty-first century is machine learning (ML). The application of machine learning to detect cybersecurity vulnerabilities is a significant advancement in information security. A void exists in the field since the widespread application of machine learning technologies in cybersecurity remains distant. The primary cause of this gap is that contemporary technology has rendered it challenging for people to comprehend the role of machine learning in cybersecurity.

The review seeks to furnish readers with a comprehensive analysis of machine learning's relevance across several facets of information security, especially for individuals interested in cybersecurity. It highlights the benefits of machine learning compared to human-operated detection methods and the diverse cybersecurity tasks it can do. This research elucidates various fundamental issues that impact real-world machine learning applications in cybersecurity. Ultimately, it examines how diverse businesses might advance machine learning in cybersecurity in the future, as this is crucial for the field's further growth. This study analyzes the contribution of machine learning to the enhancement of cybersecurity, highlighting the necessity of safeguarding sensitive information from theft and loss, as well as protecting critical assets against cyberattacks.

Keywords: Machine Learning Techniques, Role of Machine Learning, Advantage of in Cybersecurity, Security and Privacy, Online Threats.

I. Introduction

The application of machine learning techniques is essential in the field of cybersecurity. Improving digital security is feasible through the utilization of machine learning, due to its capacity to analyse large datasets and identify existing trends. The domain focused on protecting internet-connected systems, including data, software, and hardware, is known as cybersecurity[1].

Machine learning generally produces models and algorithms independent of explicit programming. Rather than depending on explicit programming directives, these systems are provided with vast datasets, allowing them to identify patterns, organize information, and perform activities[2]. Upon analyzing datasets, robots can forecast unseen or forthcoming data. Conversely, cybersecurity encompasses an ongoing array of techniques and activities designed to protect information technology systems against malevolent entities and digital threats[3].Machine learning has proven its effectiveness in data analysis across various sectors, including banking, healthcare, robotics, and quality assurance. The broad spectrum of applications is a crucial factor driving the swift progress of the industry. Machine learning enhances an organization's security posture by improving cybersecurity procedures beyond conventional rule-based methods and signature-based detection systems[4]. Machine learning (ML) is essential for the administration and analysis of data pertaining to cybersecurity concerns. As the digital landscape evolves and cyber threats grow more sophisticated, machine learning algorithms provide effective methods for detecting, analysing, and addressing numerous security concerns.[5], [6], [7].

Several applications of artificial intelligence and machine learning exist in various domains**tocybersecurity canenhance an organization’s network security:**

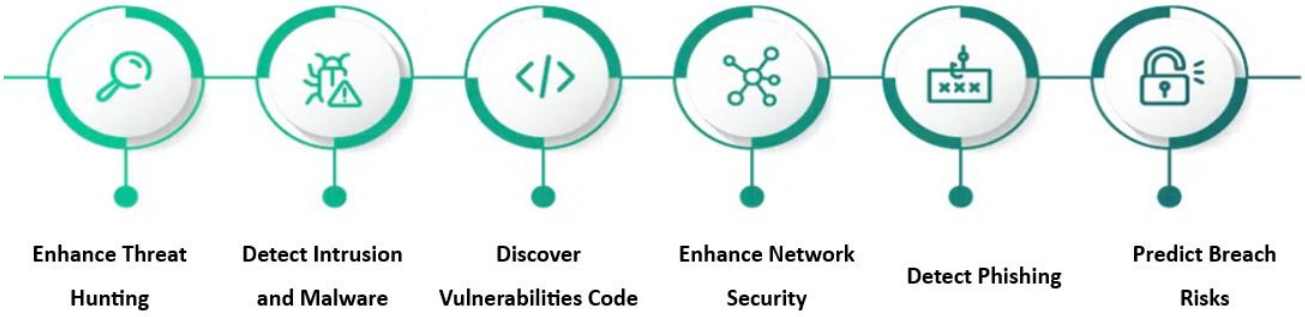

Fig.1 Illustrates the various methods to improve or enhance cybersecurity

As shown in **Figure 1**, The cybersecurity detection engine acquires all relevant input data, including program code and network traffic information. It employs established signatures to correlate input data and detect risks upon feature identification. Nonetheless, the static and reactive characteristics of this matching process frequently result in the identification of assaults long after the system has been compromised.

Anomaly detection: Machine learning models can analyse extensive datasets, encompassing system logs, network traffic, and user behaviour patterns. This analysis allows these models to identify anomalies and potential risks. Machine learning is utilized to create an understanding of what defines "normal" behaviour within a particular network or system. This knowledge is utilized to detect any anomalous or potentially hazardous activities, hence augmenting the system's capacity to identify and address security concerns[4].

Malware detection: Machine learning is essential for the detection and identification of novel and changing malware strains. Through the examination of file attributes and the analysis of code behavior, machine learning may detect harmful software that frequently eludes conventional antivirus tools. This proactive strategy facilitates more efficient and adaptable protection against emerging threats in the constantly changing realm of cybersecurity[8].

Phishing detection: Machine learning algorithms evaluate email content, URLs, and user behavior to identify trends, enabling the recognition and mitigation of phishing attempts. Behavioral analysis: Machine learning continuously monitors and analyzes user behavior to identify unauthorized or suspicious activities. This is commonly known as user and entity behavior analytics, or "UEBA," a machine learning technology that assists organizations in identifying insider threats and compromised accounts[9].

Threat hunting: Machine learning functions by persistently observing and evaluating user behavior to identify undesired or illegal actions. Through the proficient training and deployment of machine learning threat detection systems, companies can identify complex hazards promptly, reveal zero-day assaults (previously unidentified vulnerabilities), and mitigate advanced persistent threats (APTs). This proactive approach improves overall security by identifying and addressing possible threats more rapidly and effectively[10].

Cloud security: The growing dependence on cloud computing across sectors necessitates the incorporation of machine learning security solutions into cloud settings. This integration assists in recognizing and alleviating cyber risks that conventional perimeter-based methods may inadequately address. Organizations may improve their capacity to identify and address evolving cybersecurity threats in a dynamic and scalable way by utilizing cloud-based machine learning[11][12].

These represent only a portion of the benefits associated with the incorporation of machine learning into organizational cybersecurity initiatives. Cybersecurity experts can substantially reduce cyber threats, address security vulnerabilities, and enhance overall performance by effectively leveraging machine learning skills. Consequently, machine learning should be acknowledged as an essential component of a comprehensive security strategy that encompasses data encryption, access controls, perimeter defences, and cybersecurity awareness training for all staff[13].

Digital protection, referred to as information technology security or electronic data security, is the safeguarding against detrimental assaults on computers, servers, mobile devices, electronic systems, networks, and data. This extensive phrase includes catastrophe recovery and end-user training. It underscores the protection of information pertaining to individuals, legislation, and enterprises, with the objective of shielding it from abuse or external interference[14].

To accomplish this, cybersecurity must emphasize three essential tasks: (a) protecting software and hardware systems along with their data; (b) securing government or organizational assets against various threats; and (c) executing and improving these responsibilities. Throughout the years, numerous defenses to digital assaults have been implemented, with intrusion detection systems (IDSs) serving as a notable example. These technologies are essential for detecting and addressing possible cybersecurity attacks.

Perform an extensive review of the literature on the utilization of machine learning in cybersecurity, with a particular focus on practical applications across five key functions: Identification, Protection, Detection, Response, and Recovery.

Research Questions Addressed by Literature Review

• RQ1: What classification could be employed to elucidate the application of machine learning in delivering cybersecurity?
• RQ2: What particular applications of machine learning find relevance in the field of cybersecurity?
• RQ3: What are the current research trends in utilizing machine learning for cybersecurity?
• RQ4: What are the current major challenges and the future direction of the application of machine learning in the field of cybersecurity?

Until February 2023, an extensive review of numerous articles was conducted to explore and contribute significant findings to the scientific community regarding these research topics. Following this initial review, selected research works underwent further examination to discern the applications of machine learning in cybersecurity, the specific domains where this technology was utilized, and the outcomes achieved.

The literature review led to the following:

- A machine learning classification system in cybersecurity that provides a multi-tiered categorization of the analyzed articles based on cybersecurity functions, solution types, and specific use cases.
- Specific applications of machine learning in cybersecurity, emphasizing potential scenarios to showcase the capabilities of ML.
- A comprehensive examination of the literature employing descriptive analysis to investigate the research patterns in the utilization of machine learning within the field of cybersecurity.
- A thorough assessment of the existing literature critically identifies domains requiring additional investigation, aiming to stimulate further research in the field.

This comprehensive review presents a complete overview of machine learning approaches in the context of cybersecurity, based on substantial research on their integration. This review significantly contributes by comparing the temporal complexity of widely used machine learning models in cybersecurity. Furthermore, the constraints of each machine learning technique are delineated. An evaluative review of the current literature identifies gaps necessitating future research, with the objective of encouraging additional inquiry in this field.

The rest of the article is structured as follows. **Section 1** discusses the relevant background to provide an introduction. **Section 2** describes the research methodology adopted to conduct **the literature review.Section 3** discusses the data extraction process to feed the descriptive analysis and state-of-the-art research presented in **Section 4**. Finally, **Section 5** presents the main conclusions

II. Literature Review

It is essential to evaluate the full range of capabilities provided by machine learning algorithms, including characteristics such as computational time, adaptability, and complexity. The significance of these parameters may fluctuate based on the particular application.Machine learning serves several functions in managing data associated with cybersecurity issues. Machine learning (ML) improves the effectiveness of security systems through advanced threat identification, intelligence integration, and adaptive response mechanisms, hence strengthening an organization's defences against various cyber-attacks.

Srikanth Thudumu et al[15]A triangular model is utilized to illustrate the current state of anomaly detection in high-dimensional big data, highlighting distinct challenges at three vertices: the issue of high dimensionality, the techniques and algorithms for anomaly detection, and the tools employed in big data applications and frameworks.Saad S. Naif et al. [16]Reduce congestion in the AODV routing protocol due to connection failures and the rebroadcasting of RREQ control packets. The MANET-related reactive protocol, Ad hoc On Demand Distance Vector Protocol, broadcasts route request packets across the network to construct a route from a source node to a target node. Salman Muneer et al[17]The paper discusses the growing importance of artificial intelligence (AI) and machine learning (ML) techniques in enhancing cybersecurity measures against cyber threats. It presents a proposed cyber-event detection model that utilizes advanced ML algorithms to analyze real-time network data for identifying and mitigating malicious attacks. The model aims to detect both known and unknown threats, ensuring robust protection of critical assets and sensitive information. Additionally, it emphasizes the necessity for organizations to adopt effective security frameworks and highlights the potential issues associated with false positives and negatives in machine learning applications in cybersecurity.Sh. Zeadally et al[18]The paper discuss the evolving landscape of cybersecurity and the increasing sophistication of cyberattacks over the years, highlighting the inadequacy of traditional cybersecurity solutions in countering these threats. It emphasizes the importance of harnessing artificial intelligence (AI) technologies, particularly machine learning and deep learning, to enhance cybersecurity measures. The authors present an overview of various cyber threats, the limitations of legacy cybersecurity solutions, and the potential of AI to improve detection and mitigation strategies. They also explore the challenges the cybersecurity community faces in adopting AI and underscore the necessity of ongoing research in this field to develop effective solutions against emerging cyber threats. Ashwini and K. V. Reddy et al[19]exhibit diverse machine learning (ML) methods to forecast and examine contemporary user behaviors. The main objective of this study is to identify and classify the closely linked group that a user is most interested in. User online activity data, particularly browsing history, is gathered via a web browser program.Zhiwei Ji[20]Proposed a long short-term memory (LSTM)-based anomaly detection approach (LSTMAD) for discord detection from univariate time series data. LSTMAD derives structural features from standard (non-anomalous) training data and subsequently performs anomaly detection through a statistical method based on the prediction error relative to observed data.Kilian Batzner et al[21]Propose a training loss that prevents the learner from replicating the teacher's feature extractor on atypical photos. It facilitates a substantial decrease in the computing expense of the student-teacher model, concurrently improving the detection of anomalous features. Furthermore, it pertains to the identification of complex logical abnormalities involving improper combinations of standard local properties.JiaweiYu et al[22]Utilized it as a plug-in module with various deep feature extractors, including Res-Net and vision transformer, for unsupervised anomaly detection and localization. In the training phase, Fast-Flow develops the capability to transform the input visual feature into a controllable distribution and assesses the probability of detecting anomalies during the inference phase.Naji A. M. et al.[23]Outline various challenges associated with scheduling algorithms, highlighting the deficiencies that require rectification. They categorize these challenges into two distinct viewpoints: the implementation strategies of algorithms and the criteria-based metrics employed to evaluate the analysis and application of these strategies in performance assessment.Bo Wang et al[24]The ensemble learning model is utilized to analyze and predict anomalies in large system logs, covering all log processing stages including log analysis, feature extraction, anomaly

detection, prediction evaluation, and real-time reliability assessment. The proposed model demonstrates improvements in accuracy, recall rate, and F1 score for anomaly prediction compared to traditional machine learning methods. The evaluation results are employed to improve real-time reliability, especially in light of the low anticipated recall rate, thus markedly increasing the precision of real-time reliability evaluations.Rohit Ranjana and Shashi Shekhar Kumar[25]We have employed a behavioral approach to differentiate between malicious and legal users by applying big data analytics to application-layer logs. We utilize a Machine Learning technique that depends on particular parameters to forecast fraudulent users. This method entails Machine Learning producing a compilation of IP addresses or user identification tokens (UIT) extracted from real-time data, signifying entities participating in or suspected of nefarious actions based on their browsing patterns.Kulvinder Singh and Sudan Jha[26]Employed machine learning algorithms for the analysis and prediction of cyber-attacks.Abel Yeboah-Ofori et al[27]Employed Machine Learning (ML) methodologies alongside Cyber Threat Intelligence (CTI) to assess and predict attacks based on CTI characteristics. This enables the identification of intrinsic weaknesses in Cyber Security Controls (CSC), allowing for the application of appropriate measures to improve overall cybersecurity.Iqbal H. Sarker[28]The paper explored the integration of machine learning (ML) techniques in addressing cybersecurity issues, emphasizing the inadequacy of traditional security solutions in the face of evolving cyber threats. It provided a comprehensive overview of various ML algorithms and their applications in detecting and preventing cyber-attacks, such as intrusion detection and anomaly detection, highlighting the importance of automation and intelligent decision-making in cybersecurity. The study underscored the potential for ML to enhance security systems by offering real-time insights and proactive defense mechanisms, ultimately outlining future research directions that focus on predictive analysis of cyber risks, essential for developing robust cybersecurity frameworks.N. Harki A. et al.[29]Proposed model focuses on fast crisis detection, waiting times, and regional client satisfaction. Demographics and service mechanisms make up programming algorithms. This improvement aims to investigate waiting line solutions, prevent sweeping in any outlet or accessible location, and evaluate performance.Muhammad Shoaib Akhtar and Tao Feng[30]The research study focuses on dynamic malware detection, recognizing the adaptive characteristics of malware. In light of the ongoing evolution of harmful software, the research utilizes dynamic malware detection methodologies. The continuous emergence of new malware presents a constant danger to online security, capitalizing on Internet vulnerabilities. S. Y. Khamaiseh.et al.[31] The Adversarial Attacks and Defence Mechanisms segment examines the vulnerability of deep neural networks (DNNs) to adversarial attacks, particularly in image classification. It highlights the growing concern about security in DNN applications and emphasizes the need for understanding the adversarial threat model. The document outlines various defence methods to protect DNNs from threats, highlighting their limitations and effectiveness. Understanding these strategies is crucial for improving DNN reliability in various applications. The segment also highlights research deficiencies and the need for further exploration of effective defensive mechanisms.

V. K. Krishnamoorthy et al[32]The Case Studies in Specific Applications section emphasizes the practical application of machine learning (ML) methodologies for cyber threat identification in several industries. A prominent bank in financial services employed a supervised learning model to examine transaction patterns, markedly decreasing false positives and enhancing fraud detection rates. A prominent hospital in the healthcare industry implemented an unsupervised learning system

to analyze network traffic for anomalous patterns linked to ransomware threats, thereby improving security and protecting essential patient data. These instances illustrate the efficacy of machine learning in alleviating cyber risks and emphasize its significance in enhancing enterprise security protocols. A. H. Salem.et al.[33] The document, entitled Advancing Cybersecurity A Comprehensive Review of AI-Driven Detection Techniques, analyses the pivotal function of artificial intelligence (AI), specifically machine learning (ML) and deep learning (DL), in improving the detection and prevention of progressively sophisticated cyber-attacks. It evaluates more than sixty contemporary studies, offering a framework to analyse the efficacy and constraints of various AI tools, in conjunction with metaheuristic algorithms. The results underscore the necessity for ongoing revisions to AI approaches to tackle emerging cyber threats and stress the significance of creating adaptive systems capable of efficiently addressing new issues in cybersecurity. J. Bharadiya.et al.[34]The Adversarial Attacks and Defence Mechanisms segment examines the vulnerability of deep neural networks (DNNs) to adversarial attacks, particularly in image classification. It highlights the growing concern about security in DNNs and the need for research into adversarial techniques that can compromise their integrity. The document categorizes adversarial attacks based on their implementation during training or testing phases and emphasizes the need to understand the adversarial threat model. It also outlines defence methods to protect DNNs from threats, highlighting their limitations and effectiveness. The segment also highlights research deficiencies and the need for further exploration of robust defensive mechanisms to enhance DNN reliability in various applications. Kuzlu.et al.[35]The document discusses the growing use of Artificial Intelligence (AI) in cybersecurity for Internet of Things (IoT) systems. It highlights the use of AI in creating algorithms to protect IoT devices and networks from various cyber threats. AI technologies like machine learning, decision trees, and neural networks are used to identify anomalies and threats in real-time. However, cyber-attackers have adapted to exploit AI, using methods like adversarial AI to bypass protective strategies. This highlights the ongoing arms race between cybersecurity professionals using AI for defence and adversaries using AI for malicious purposes. The article emphasizes the need for sophisticated preventive strategies against emerging threats.

III. Machine Learning and Its Applications in Cybersecurity

Machine learning (ML) methodologies possess the capability to improve detection velocity through the constant surveillance of internal and external information sources. The rapid correlation of this information facilitates the swift detection of anomalous activity, thus reducing potential consequences. **Table 1** delineates the principal contributions of each research study to the detection function, detailing solution categories, machine learning use cases, and the roles utilized. The next sections detail solution categories, providing a comprehensive analysis of use cases and their respective benefits.

This field emphasizes the identification and categorization of anomalous behaviors by creating and sustaining operational and dataflow baselines derived from several sources. These baselines provide

as reference points for identifying and analyzing occurrences, facilitating the understanding of assault targets and methodologies.

Table 1: Summary of the categories, use case, role, and advantagesfocusing on research study.

Solution Category	Use Case	Role	Advantages
Anomaly Identification	Identification of Unusual Patterns	Machine learning ML analyzes data to identify patterns and behaviors that are considered normal.	Enables the automated detection of anomalies, even in large.
	Cybersecurity Threat Detection	Analyze network traffic, user behavior, and system logs to detect abnormal activities indicative of cyber threats.	Anomaly detection in cybersecurity helps identify new and evolving threats by recognizing patterns.
	Fraud Detection in Finance	Analyze transaction data, user behavior, and spending patterns to identify anomalous activities.	Machine learning aids in the early detection of financial fraud by recognizing unusual patterns.
	Network Intrusion Detection	Analyze network traffic to identify unusual patterns that may indicate a security breach or unauthorized access.	Anomaly detection in network security enables the identification of sophisticated attacks.
	User Authentication and Access Control	Analyze patterns of user login behavior to identify anomalous access attempts that may signal unauthorized access.	Anomaly detection in user authentication enhances security by identifying potential account compromises.
Information on Threats	Threat Detection and Classification	Machine learning ML analyzes vast datasets to detect patterns indicative of cyber threats, classifying them into different categories.	ML enhances the speed and accuracy of threat detection, enabling organizations to respond proactively to evolving cyber threats.
	Threat Intelligence Integration	ML systems process and integrate threat intelligence data from various sources, providing context and insights into emerging threats.	ML-enhanced threat intelligence helps organizations stay updated on the latest threats AND vulnerabilities.
	Malware Detection	Analyze file characteristics, code patterns, and behaviours to detect known and unknown malware.	ML-based malware detection provides improved accuracy including zero-day threats.
	Network Intrusion Detection	ML is applied to analyze network traffic patterns and identify anomalies that may indicate unauthorized access or suspicious activities.	ML-based intrusion detection systems enhance the ability to detect complex and stealthy attacks that traditional methods may overlook.
	Vulnerability Assessment	ML models analyze system configurations, software versions, and network architectures to identify potential vulnerabilities.	ML-driven vulnerability assessments provide a proactive approach to security by identifying weaknesses before they are exploited
Malware Detection	Heuristic Analysis	Apply heuristic rules to identify potential malware based on characteristics commonly associated with malicious behaviour.	Heuristic analysis allows for the detection of suspicious activities that may not have a known signature.
	Feature Extraction	ML algorithms extract relevant features from files or network traffic to identify unique characteristics of malware.	Feature extraction allows ML models to focus on specific aspects of data that are improving detection accuracy.
	Adversarial Machine Learning	ML in malware detection needs to be robust against adversarial attacks designed to evade detection.	Enhance the resilience of ML models against attempts to manipulate by attackers.
		ML enables the automation of malware	The scalability of ML facilitates the rapid

	Scalability and Automation	detection processes, allowing for the analysis of large datasets in real time.	identification, response, and expansive digital environments
	Continuous Learning	ML Can learn continuously, improving their ability to detect emerging and evolving malware threats.	Continuous learning ensures that the malware detection system remains effective in the face of a dynamic. e.
Behavioural Analysis	Cybersecurity Threat Detection	Analyze patterns of user and network behaviour to detect anomalies,	Identification of abnormal activities, or malware infections, by learning from historical data.
	Fraud Detection in Finance	Analyze transaction patterns, user behaviours, and account activities to detect fraudulent activities.	ML algorithms can identify unusual spending patterns and indicators of financial fraud.
	Insider Threat Detection	Monitor employee activities and interactions with corporate systems to identify potential insider threats.	Behavioural analysis helps detect abnormal user behaviours and compromised credentials.
	Internet of Things (IoT) Security	ML is used to analyze patterns of communication and data exchange within IoT networks to detect abnormal device behaviours.	Behavioural analysis in IoT security helps identify potential security threats and abnormal network activities.
	Social Media and Marketing	ML is applied to analyze user interactions, preferences, and engagement patterns on social media platforms for targeted marketing campaigns.	Behavioural analysis in marketing helps optimize advertising strategies, and enhance user engagement.

This duty entails proactive strategizing to create effective procedures for resolving issues, investigating incidents to determine their source, extent, and consequences, managing incidents, and facilitating communication during and post-attack. The integration of machine learning methodologies for case-related tasks can facilitate expedited incident resolution, necessitating reduced time and effort from security analysts. Table 1 delineates the roles and advantages, providing a thorough summary of the principal studies concentrated on these elements. Comprehensive descriptions of the diverse machine learning applications and cybersecurity solutions within each category are presented above.

Table 2: This review study analyzes the existing research and studies on machine learning applications in cybersecurity. This was achieved by identifying 33 recent research from a selection of 12 pertinent publications sourced from multiple databases, including WoS, Scopus, IEEE, Hindawi, and others, covering a period of 5 years from 2020 to February 2023. This study examines various machine learning (ML) strategies utilized in cybersecurity and clarifies which cybersecurity operations have gained from ML technology. The selected literature is analyzed according to (i) the proposed taxonomy of machine learning in cybersecurity, (ii) the annual publication frequency, (iii) the citation frequency, and (iv) the nature of cybersecurity contributions.

Table 2: Summary of the current studies focused on the approaches to improving cybersecurity

Ref	Year	Implementation	Improvement
Srikanth Thudumu et al [15]	2021	Triangular model for anomaly detection	Addresses high-dimensional data anomaly challenges
Salman Muneer et al [16]	2022	AI and ML for cybersecurity asset protection	Improves cybersecurity by mitigating rising threats
Sh. Zeadally et al [17]	2022	AI analysis for cybersecurity improvement	Explores AI potential in various cybersecurity areas
Ashwini and K. V. Reddy et al [18]	2022	ML to predict user behavior	Classifies user interests based on browsing history
Zhiwei Ji [19]	2021	LSTM-based anomaly detection for time series data	Detects anomalies using prediction error metrics
Kilian Batzner et al [20]	2022	Student-teacher model for anomaly detection	Reduces computing cost while detecting complex anomalies
Jiawei Yu et al [21]	2022	Fast-Flow plugin for deep feature extractors	Transforms input features for unsupervised anomaly detection
Bo Wang et al [22]	2023	Ensemble learning for system log anomaly prediction	Increases precision of real-time reliability assessments
Rohit Ranjana and Shashi Shekhar Kumar [23]	2023	Behavioral analysis for malicious user identification	Forecasts fraudulent user behavior using big data
Kulvinder Singh and Sudan Jha [24]	2023	ML for cyber-attack prediction	Predicts cyber-attacks using ML algorithms
Abel Yeboah-Ofori et al [25]	2022	ML with CTI for attack prediction	Identifies cybersecurity weaknesses and suggests improvements
Iqbal H. Sarker [26]	2021	ML for intelligent data analysis in cybersecurity	Enhances automation and insight generation in cybersecurity
Muhammad Shoaib Akhtar and Tao Feng [27]	2021	Dynamic malware detection	Adapts to evolving malware threats

IV. Discussion

In the modern digital landscape, machine learning methodologies have become essential, particularly in the field of cybersecurity. Both perpetrators of cyber assaults and defenders utilize machine learning methodologies. Malefactors utilize machine learning to investigate innovative techniques for

circumventing firewalls and security measures. From a defensive standpoint, these tactics aid security professionals in protecting security systems from unauthorized intrusions and access.

The three primary threats to cyberspace are malware, unsolicited communications, and unauthorized access detection. Supplementary machine learning models including decision trees, naïve Bayes, random forests, support vector machines, artificial neural networks, and deep belief networks. Each cyber threat possesses an own sub-domain. Anomaly-based, signature-based, and hybrid-based techniques are considered sub-domains of intrusion detection. Malware detection sub-domains can be categorized as hybrid, dynamic, or static detection.

Machine learning (ML) is essential in anomaly detection, utilizing algorithms to recognize patterns, behaviors, or instances that diverge from the anticipated or usual condition. Anomaly detection is utilized across various domains, including industrial processes, finance, cybersecurity, and healthcare. In cybersecurity, machine learning (ML) is a powerful tool for collecting, analyzing, and responding to threat-related information. Organizations can utilize it to enhance their defenses, manage incidents more adeptly, and adapt to the continually evolving world of cyber threats. an essential component of behavioral analysis across various domains, including user experience and cybersecurity.

Behavioral analysis includes the examination of behavioral patterns, identification of anomalies, and the development of predictions based on observed behaviors. A crucial aspect of malware identification is employing statistical models and algorithms to detect patterns, behaviors, and attributes associated with malicious software.

The utilization of machine learning in this context improves the capacity to identify and counteract emerging malware threats. A crucial function in the management and retrieval of information on cybersecurity threats. In the dynamic digital landscape and among escalating cyber threats, machine learning algorithms provide effective methods for discovering, assessing, and mitigating various security challenges.

V. Conclusion

Cybersecurity utilizing machine learning necessitates a holistic approach that encompasses the recruitment of skilled personnel, continuous surveillance, and adaptability to the evolving threat environment. Identifying an appropriate balance between automation and human oversight is essential for sustaining a robust and adaptable cybersecurity framework. A notable innovation in information security is the utilization of machine learning for the detection of cybersecurity incidents.

By employing advanced algorithms and techniques, such as supervised and unsupervised learning, machine learning models can identify patterns, anomalies, and correlations in extensive datasets that would be difficult for human analysts to perceive independently. Moreover, enterprises may remain proactive against emerging cybersecurity risks through the ongoing learning and adaptive response functionalities of machine learning models. It is crucial to take caution while utilizing machine learning for cybersecurity event detection, as false positives or negatives can profoundly affect an organization's security posture.

Disclaimer (Artificial intelligence)
Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

References

[1] J. W. Composto *et al.*, "An implementation of artificial neural networks into behavioral analysis system An implementation of artificial neural networks into behavioral analysis system," 2020, doi: 10.1088/1757-899X/734/1/012161.

[2] "Machine Learning for Malware Detection".

[3] G. Apruzzese *et al.*, "The Role of Machine Learning in Cybersecurity," vol. 4, no. 1, 2023, doi: 10.1145/3545574.

[4] D. T. Mane, S. Sangve, G. Upadhye, S. Kandhare, S. Sonar, and S. Tupare, "Detection of Anomaly using Machine Learning : A Comprehensive Survey Detection of Anomaly using Machine Learning : A Comprehensive Survey," no. November, 2022, doi: 10.46338/ijetae1122.

[5] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, "Machine Learning for Anomaly Detection : A Systematic Review," vol. XX, 2021, doi: 10.1109/ACCESS.2021.3083060.

[6] A. Mathew, "International Conference on IoT based Control Networks and Intelligent Systems (ICICNIS 2020) Machine Learning in Cyber-Security Threats International Conference on IoT based Control Networks and Intelligent Systems (ICICNIS 2020)," no. Icicnis, pp. 893–899, 2020.

[7] S. Mechanism, "Research on Anomaly Network Detection Based on Self-Attention Mechanism," 2023.

[8] N. Chowdhury and A. Haque, "Android Malware Detection using Machine learning : A Review".

[9] G. Kőrösi, "Machine Learning based analysis of users ' online behaviour," no. March, 2022.

[10] Y. He, G. Meng, K. Chen, X. Hu, and J. He, "Towards Security Threats of Deep Learning Systems : A Survey," 2020.

[11] N. Yan, "Online learning behavior analysis based on machine learning analysis," 2019, doi: 10.1108/AAOUJ-08-2019-0029.

[12] S. S. Samy, “A Comparative Study on Detection of Malware and Benign on the Internet Using Machine Learning Classifiers,” vol. 2022, 2022.

[13] S. Ghosh, “Malware Detection & Classification using Machine Learning,” no. July, 2021, doi: 10.1109/iSSSC50941.2020.9358835.

[14] L. A. Review, M. Ahsan, K. E. Nygard, R. Gomes, M. Chowdhury, and N. Rifat, “Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning — A Review,” no. July, 2022, doi: 10.3390/jcp2030027.

[15] S. Thudumu, P. Branch, J. Jin, and J. (Jack) Singh, “A comprehensive survey of anomaly detection techniques for high dimensional big data,” *J. Big Data*, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00320-x.

[16] S. S. Naif, B. A. Idrees, A. J. Ibrahim, and N. A. Majedkan, “A Technique of NLAODV algorithm to get Routes of Nodes-List in Mobile Ad-hoc Network (MANET),” *Sci. J. Univ. Zakho*, vol. 10, no. 3, pp. 147–152, 2022, doi: 10.25271/sjuoz.2022.10.3.909.

[17] S. Muneer and M. B. Alvi, “Cyber Security Event Detection Using Machine Learning Technique,” vol. 2, no. June, pp. 42–46, 2023.

[18] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, “Harnessing artificial intelligence capabilities to improve cybersecurity,” *IEEE Access*, vol. 8, pp. 23817–23837, 2020, doi: 10.1109/ACCESS.2020.2968045.

[19] K. V. Reddy, “Predicting the User Behavior Analysis using Machine Learning Algorithms,” no. July, pp. 1740–1746, 2020.

[20] Z. Ji, J. Gong, and J. Feng, “A Novel Deep Learning Approach for Anomaly Detection of Time Series Data,” vol. 2021, no. Dl, 2021.

[21] K. Batzner, L. Heckler, and R. König, “EfficientAD: Accurate Visual Anomaly Detection at Millisecond-Level Latencies,” pp. 128–138, 2023.

[22] N. Flows, “FastFlow: Unsupervised Anomaly Detection and Localization via 2D Normalizing Flows,” 2021.

[23] N. Harki, A. Ahmed, and L. Haji, “CPU Scheduling Techniques: A Review on Novel Approaches Strategy and Performance Assessment,” *J. Appl. Sci. Technol. Trends*, vol. 1, no. 1, pp. 48–55, 2020, doi: 10.38094/jastt1215.

[24] B. Wang *et al.*, “Research on anomaly detection and real-time reliability evaluation with the log of cloud platform,” *Alexandria Eng. J.*, vol. 61, no. 9, pp. 7183–7193, 2022, doi: 10.1016/j.aej.2021.12.061.

[25] R. Ranjan and S. S. Kumar, “User behaviour analysis using data analytics and machine learning to predict malicious user versus legitimate user,” *High-Confidence Comput.*, vol. 2, no. 1, p. 100034, 2022, doi: 10.1016/j.hcc.2021.100034.

[26] K. Singh and S. Jha, “Cyber Threat Analysis and Prediction Using Machine Learning,” *Proc. - 2021 3rd Int. Conf. Adv. Comput. Commun. Control Networking, ICAC3N 2021*, no. February, pp. 1981–1985, 2021, doi: 10.1109/ICAC3N53548.2021.9725445.

[27] A. Kok, I. Ilic Mestric, G. Valiyev, and M. Street, “Cyber Threat Prediction with Machine Learning,” *Inf. Secur. An Int. J.*, vol. 47, no. 2, pp. 203–220, 2020, doi: 10.11610/isij.4714.

[28] I. H. Sarker, “Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity : Current and Future Prospects,” *Ann. Data Sci.*, vol. 10, no. 6, pp. 1473–1498, 2023, doi: 10.1007/s40745-022-00444-2.

[29] N. A. Majedkan, B. A. Idrees, O. M. Ahmed, L. M. Haji, and H. I. Dino, “Queuing Theory Model of Expected Waiting Time for Fast Diagnosis nCovid-19: A Case Study,” *3rd Int. Conf. Adv. Sci. Eng. ICOASE 2020*, no. June 2021, pp. 127–132, 2020, doi: 10.1109/ICOASE51841.2020.9436601.

[30] M. S. Akhtar, “Evaluation of Machine Learning Algorithms for Malware Detection,” 2023.

[31] S. Y. Khamaiseh, D. Bagagem, A. Al-Alaj, M. Mancino, and H. W. Alomari, “Adversarial Deep Learning: A Survey on Adversarial Attacks and Defense Mechanisms on Image Classification,” *IEEE Access*, vol. 10, no. September, pp. 102266–102291, 2022, doi: 10.1109/ACCESS.2022.3208131.

[32] V. K. Krishnamoorthy *et al.*, “Energy Saving Optimization Technique-Based Routing Protocol in Mobile Ad-Hoc Network with IoT Environment,” *Energies*, vol. 16, no. 3, 2023, doi: 10.3390/en16031385.

[33] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, *Advancing cybersecurity: a comprehensive review of AI-driven detection techniques*, vol. 11, no. 1. Springer International Publishing, 2024. doi: 10.1186/s40537-024-00957-y.

[34] J. Bharadiya, “Machine Learning in Cybersecurity: Techniques and Challenges,” *Eur. J. Technol.*, vol. 7, no. 2, pp. 1–14, 2023, doi: 10.47672/ejt.1486.

[35] M. Kuzlu, C. Fair, and O. Guler, “Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity,” *Discov. Internet Things*, vol. 1, no. 1, 2021, doi: 10.1007/s43926-020-00001-4.