World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Machine learning in cybersecurity: A review of threat detection and defense mechanisms

Ugochukwu Ikechukwu Okoli [1], Ogugua Chimezie Obi [2], Adebunmi Okechukwu Adewusi [3] and Temitayo Oluwaseun Abrahams [4, *]

[1] *Independent Researcher, Manchester, UK.*
[2] *Independent Researcher, Lagos, Nigeria.*
[3] *University of Ilorin, Nigeria*
[4] *Independent Researcher, Adelaide, Australia.*

World Journal of Advanced Research and Reviews, 2024, 21(01), 2286–2295

Publication history: Received on 16 December 2023; revised on 23 January 2024; accepted on 25 January 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.21.1.0315

Abstract

The cybersecurity concerns get increasingly intricate as the digital world progresses. In light of the increasing complexity of cyber threats, it is imperative to develop and implement advanced and flexible security strategies. Machine Learning (ML) has become a potent tool in strengthening cybersecurity, providing the capacity to scrutinise extensive information, recognise trends, and improve threat detection and defence methods. This paper examines the significance of ML in the field of cybersecurity, with a special emphasis on the identification of threats and the implementation of protective measures. By incorporating ML algorithms into cybersecurity frameworks, organisations may automate decision-making processes, facilitating prompt responses to ever-changing threats. The initial segment explores the terrain of cyber threats, highlighting the necessity for dynamic and aggressive security methods. Conventional solutions that rely on signatures are frequently inadequate when it comes to handling sophisticated, shape-shifting attacks. ML algorithms, in contrast, have exceptional proficiency in identifying nuanced patterns and irregularities within extensive datasets, therefore offering a more efficient method of detecting potential threats. The second section delves into several ML methodologies utilised in cybersecurity, including supervised and unsupervised learning, deep learning, and reinforcement learning. Every approach is assessed based on its suitability for threat detection, demonstrating its advantages and constraints. Furthermore, the relevance of feature engineering and data pretreatment in improving machine learning models for cybersecurity applications. The versatility of ML algorithms allows them to grow with emerging threats, making them a useful tool in the ever-changing arena of cyber warfare. The final segment focuses on real-world applications of machine learning in cybersecurity, presenting successful use cases across sectors. From anomaly detection to behavior analysis, ML algorithms contribute to the discovery of dangerous activity, lowering false positives and strengthening the overall security posture. Lastly, the paper covers the obstacles and ethical issues related to the adoption of ML in cybersecurity. Issues like as adversarial assaults, skewed datasets, and the interpretability of ML models are examined, highlighting the necessity for a holistic strategy that integrates modern technology with ethical considerations. The fusion of human expertise and machine intelligence offers a formidable defense against evolving cyber threats, paving the way for a more resilient and secure digital future.

Keywords: Cybersecurity; Machine learning; Threat detection; Defense mechanisms; Anomaly detection

1. Introduction

In the contemporary digital era, where virtually every facet of our lives is intertwined with technology, the ubiquitous nature of cyberspace has paved the way for unparalleled connectivity and efficiency [1]. However, this

* Corresponding author: Temitayo Oluwaseun Abrahams

interconnectedness has also given rise to an alarming surge in cyber threats, ranging from conventional malware to sophisticated, targeted attacks. As organizations digitize their operations and individuals become increasingly dependent on online platforms, the importance of robust cybersecurity measures cannot be overstated [1–3].

The traditional paradigms of cybersecurity, often reliant on rule-based systems and static signatures, struggle to keep pace with the dynamic and sophisticated tactics employed by cyber adversaries [4]. The landscape of threats is ever-evolving, with attackers employing polymorphic techniques, zero-day exploits, and social engineering tactics that render conventional defenses inadequate. Against this backdrop, the integration of Machine Learning (ML) emerges as a beacon of hope, offering a paradigm shift in the way we approach cybersecurity [5,6].

Machine learning, a subset of artificial intelligence, empowers systems to learn from data and make intelligent decisions without explicit programming [7–10]. Its ability to discern patterns, anomalies, and trends within massive datasets positions ML as a potent ally in the relentless battle against cyber threats. Unlike traditional methods that rely on predefined rules [11], ML algorithms have the capability to adapt and evolve, making them particularly adept at identifying novel and previously unseen attack vectors [12,13].

This paper seeks to delve deeply into the symbiotic relationship between machine learning and cybersecurity, with a specific emphasis on its applications in threat detection and defense mechanisms. By understanding the limitations of conventional approaches, we can appreciate the transformative potential that machine learning brings to the table [4,14]. The subsequent sections will navigate through the diverse landscape of ML techniques, their real-world applications in cybersecurity, and the ethical considerations that accompany their deployment [15–18].

Positioned at the intersection of human ingenuity and machine intelligence, the integration of ML in cybersecurity not only promises to fortify our defenses against existing threats but also to anticipate and proactively respond to emerging challenges [4]. In this dynamic landscape, the synergy between human expertise and the adaptability of machine learning is poised to redefine the cybersecurity paradigm, ushering in an era of resilience, agility, and unparalleled defence against the ever-evolving array of cyber threats [19,20].

2. Context of Cybersecurity Challenges

The context of cybersecurity challenges is shaped by the dynamic and evolving landscape of the digital world [21]. As technology advances, so do the methods and sophistication of cyber threats. Some of the contextual factors that contribute to cybersecurity challenges are digital transformation that requires the use of adaptive cloud services, IoT devices, and interconnected systems. The expanding attack surface increases vulnerability, requiring robust security measures to safeguard digital assets and sensitive data [22,23].

Cybersecurity challenges refer to the threats and risks faced in the realm of digital security. With the increasing reliance on technology and the proliferation of interconnected devices, individuals, organizations, and governments face numerous cybersecurity challenges. These challenges arise from various sources, including malicious actors, human error, technological vulnerabilities, and the evolving nature of cyber threats [24–27].

The world has witnessed a significant rise in cybercriminal activities [28]. Cybercriminals employ various techniques, such as phishing, ransomware attacks, data breaches, identity theft, and financial fraud, to exploit vulnerabilities in computer systems and networks. The financial impact of cybercrime is substantial, and it continues to evolve as criminals find new ways to exploit technology [29–31].

Governments and their agencies are often prime targets for cyber-attacks [32]. Nation-states engage in cyber espionage, intellectual property theft, and sabotage to gain strategic advantages, disrupt critical infrastructure, or compromise sensitive information. These attacks often involve sophisticated techniques and are a significant concern for national security. The proliferation of IoT devices, including smart home appliances, wearables, and industrial control systems, has introduced new security challenges. Many IoT devices have inherent vulnerabilities, and their compromised security can lead to privacy breaches, unauthorized access, and potential disruptions to critical services [33,34]. Cloud computing has transformed the way organizations store, process, and access data. However, it has also introduced new security concerns. Breaches in cloud environments can lead to unauthorized access to sensitive data, service disruptions, and potential compliance violations. Organizations must implement robust security measures to protect their cloud infrastructure and data [35,36].

Insider threats refer to security risks posed by individuals within an organization. These threats can arise from disgruntled employees, negligent behaviour, or employees being targeted by external entities. Insiders may

intentionally or unintentionally compromise systems, leak sensitive information, or engage in fraudulent activities [37]. Social engineering involves manipulating individuals to divulge confidential information or perform actions that may compromise security [38]. Techniques such as phishing, pretexting, baiting, and tailgating are commonly used to deceive unsuspecting users and gain unauthorized access to systems or sensitive information [39].

Organizations must comply with various regulations and standards related to data protection and privacy, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) [40]. Ensuring compliance with these regulations while maintaining robust security measures poses a challenge, especially for multinational organizations. The rapid adoption of emerging technologies, such as artificial intelligence (AI), machine learning (ML), and blockchain, introduces both opportunities and challenges in cybersecurity. While these technologies can enhance security capabilities, they can also be exploited by threat actors. Developing effective security measures for these evolving technologies is crucial [25,39,41].

Addressing these cybersecurity challenges requires a multi-faceted approach involving robust security practices, user education and awareness, collaboration between public and private sectors, and ongoing research and development to stay ahead of emerging threats.

3. Evolution of Threats in Cyberspace

Cyber-attacks are malicious activities conducted with the intent to compromise the confidentiality, integrity, or availability of computer systems, networks, and data. As cyber threats continue to evolve, organizations and individuals employ various defense mechanisms to safeguard their digital assets. The evolution of threats in cyberspace has been a dynamic and ongoing process. As technology advances and our reliance on digital systems grows, new threats constantly emerge. Some of the common cyber-attacks (Figure 1) and related defence mechanisms include malware, phishing and social engineering, advance persistent threats, supply chain attacks, denial-of-service (DoS) and distributed denial-of –service (DDoS), man-in-the-middle (MitM), SQL injection, cross-site scripting (XSS), zero-day exploits and insider threats [42,43].

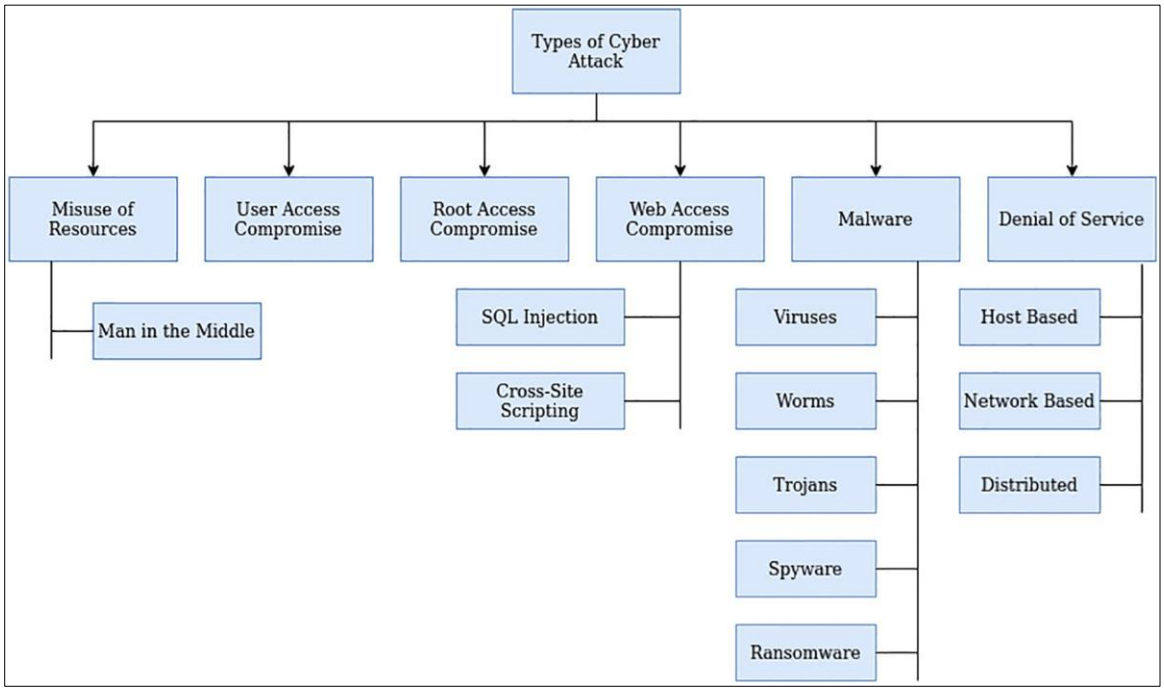

Figure 1 Classifications of cyber-attacks [44]

For instance, malicious software, such as viruses, worms, and Trojan horses, has been a persistent threat since the early days of computing. Malware can infect systems, steal data, or disrupt normal operations. Phishing attacks involve tricking users into revealing sensitive information, such as passwords or credit card details, by impersonating trustworthy entities. Social engineering techniques exploit human psychology to manipulate individuals into divulging confidential information or performing certain actions [38].

Advanced persistent threats (APTs) are sophisticated and stealthy attacks typically conducted by well-funded and highly skilled cyber adversaries, such as nation-states. APTs aim to gain long-term access to targeted systems for espionage, data theft, or sabotage. Ransomware is a type of malware that encrypts a victim's data and demands a ransom in exchange for the decryption key. It attacks have become increasingly prevalent and disruptive, targeting individuals, businesses, and even critical infrastructure [45,46].

With the proliferation of IoT devices, security vulnerabilities have emerged. Insecurely configured or poorly protected IoT devices can be compromised and used as entry points into networks or as launching pads for attacks. Rather than directly targeting a specific organization, supply chain attacks compromise trusted software or hardware suppliers to gain unauthorized access to their customers' systems. This approach can have widespread and far-reaching impacts [47].

Zero-day exploits target vulnerabilities in software that are unknown to the vendor and, therefore, unpatched. Cybercriminals or state-sponsored actors exploit these vulnerabilities to gain unauthorized access or deliver malware. Insider threats involve malicious or negligent actions by individuals who have legitimate access to an organization's systems or data. These individuals may intentionally leak sensitive information, sabotage systems, or inadvertently compromise security through carelessness [37,48].

As organizations increasingly rely on cloud-based services, security risks related to data breaches, misconfigurations, and unauthorized access to cloud environments have become more prominent. Artificial Intelligence (AI) and Machine Learning (ML) technologies are being leveraged both by security professionals and malicious actors. Threats include adversarial attacks that manipulate AI models, automated spear-phishing campaigns, and the use of AI-based tools for reconnaissance and attack automation [13,49,50].

To combat these evolving threats, cybersecurity professionals, organizations, and governments must continually adapt their defenses, employ robust security practices, and stay informed about the latest attack techniques and trends.

4. Related Cyber Defense Mechanisms

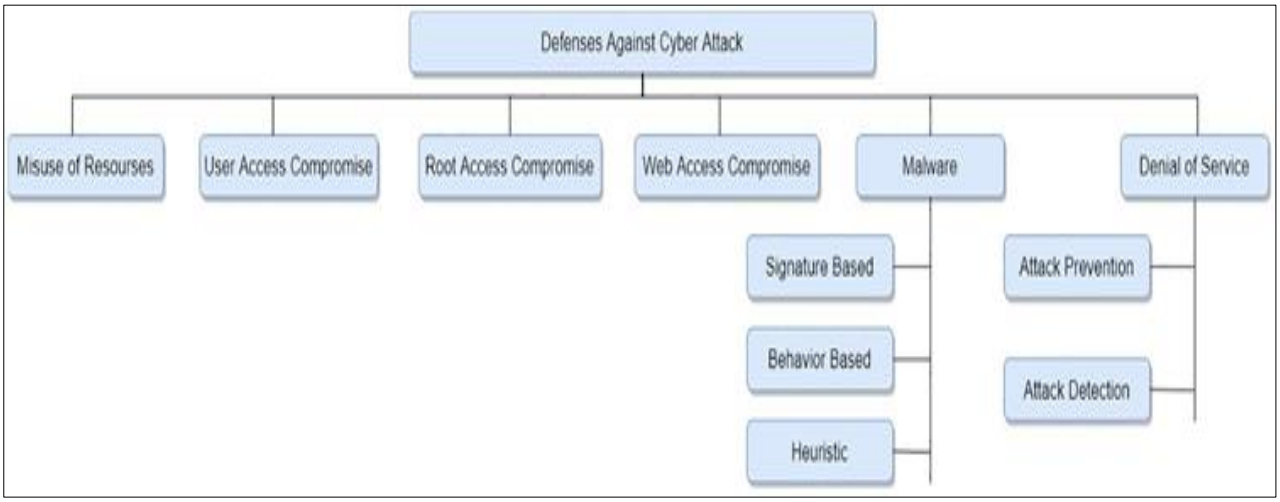

Figure 2 Potential defenses against cyber-attacks [44]

Cyber defense mechanisms encompass a variety of strategies, technologies, and practices designed to protect systems, networks, and data from cyber threats. Some of the related cyber defense mechanisms (Figure 2) include: Firewalls, intrusion detection systems (ids) and intrusion prevention systems (ips), antivirus and anti-malware software, encryption, multi-factor authentication (mfa), security awareness training, patch management, network segmentation, incident response and cybersecurity policies, and endpoint security [51,52].

5. Need for Advanced Threat Detection and Defense in Cyberspace

In today's interconnected world, the need for advanced threat detection and defense in cyberspace is more critical than ever. The rapid advancement of technology and the increasing reliance on digital systems have created a vast landscape

for cyber threats to exploit. Advanced threat detection and defense mechanisms are necessary to identify, mitigate, and respond to these evolving threats effectively.

Cyber attackers are becoming more sophisticated, employing advanced techniques and tools to compromise systems. Traditional security measures are often inadequate to detect and defend against these advanced threats, making it essential to employ advanced threat detection technologies. Modern cyber threats often employ stealthy tactics to avoid detection by traditional security solutions. Advanced attackers may use techniques such as polymorphic malware, zero-day exploits, and advanced persistent threats (APTs) to bypass conventional security measures. Advanced threat detection and defense mechanisms solutions are designed to detect these subtle and evasive tactics [45,48].

Many cyber-attacks are highly targeted, focusing on specific organizations or individuals. Advanced threat actors may conduct thorough reconnaissance and craft tailored attacks, making it challenging for conventional security measures to recognize and prevent these targeted assaults. The cyber threat landscape is dynamic and constantly evolving. New vulnerabilities are discovered, and novel attack methods emerge regularly. Advanced threat detection and defense mechanisms solutions are equipped to adapt and evolve alongside the threat landscape, providing a more robust defense against the latest and most advanced cyber threats. Since not all cyber threats come from external sources, insider threats, whether malicious or unintentional, pose significant risks to organizations. Advanced threat detection tools can monitor and analyze user behavior to identify anomalies and potential insider threats [53].

With the increasing amount of sensitive data stored online, the need to protect data and privacy is paramount. Advanced threat detection helps organizations identify and mitigate potential breaches before sensitive information is compromised. Many industries are subject to stringent regulations regarding data protection and cybersecurity. Implementing advanced threat detection and defense mechanisms helps organizations meet regulatory requirements and avoid potential legal and financial consequences [54].

Advanced threat detection and defense mechanisms solutions enable organizations to adopt a proactive rather than reactive approach to cybersecurity. By identifying and mitigating threats in their early stages, organizations can reduce the potential impact of cyber-attacks and minimize damage. Advanced threat detection encompasses both network and endpoint security. With cyber threats targeting various entry points, a comprehensive approach that covers both the network and individual devices is crucial for effective defense [45,55].

Summarily, the need for Advanced Threat Detection and Defense in cyberspace is driven by the evolving nature of cyber threats, the increasing sophistication of attackers, and the imperative for organizations to protect their sensitive data, ensure regulatory compliance, and maintain a resilient cybersecurity posture in the face of a dynamic threat landscape.

6. Traditional Threat Detection and Defense Mechanism and Associated Drawbacks

Traditional threat detection and defense mechanisms refer to the conventional approaches used to identify and mitigate security threats in various domains. While these methods have been effective to a certain extent, they also come with certain drawbacks and limitations [55,56]. Signature-based detection relies on known patterns or signatures of malicious activities to identify threats. For example, antivirus software uses signature databases to detect known malware. However, this approach is limited to detecting only known threats. It struggles to handle new or evolving threats for which signatures have not yet been identified. Zero-day exploits and polymorphic malware can easily bypass signature-based detection systems. Rule-based detection involves defining specific rules or patterns that indicate malicious behavior. Intrusion detection systems (IDS) often use rule-based detection. The challenge with this approach is that it requires manual rule creation and maintenance, which can be time-consuming and prone to human error. Additionally, rule-based systems may generate false positives or false negatives, leading to inefficient resource utilization or missed detections.

Network-based detection monitors network traffic to identify suspicious activities or anomalies. While this approach can help detect network-based attacks, it may struggle with encrypted traffic or attacks that occur at the application layer. Network-based detection also generates a large volume of alerts, which can overwhelm security teams and make it challenging to focus on critical threats. Host-based detection focuses on monitoring activities and events on individual systems or hosts. It can provide insight into system-level compromises and malicious activities. However, host-based detection is limited to the visibility of the host being monitored. Coordinated attacks that span multiple systems or lateral movement within a network may go undetected. Many traditional threat detection mechanisms rely on human analysts to review alerts, investigate incidents, and make decisions. This manual process can be time-consuming and prone to human error. Human analysts may miss subtle indicators of an attack or may struggle to keep up with the volume of alerts generated by automated detection systems.

Traditional mechanisms often lack contextual awareness and behavioral analysis capabilities. They may focus on individual events or static indicators without considering the broader context of an attack or the behavior patterns associated with advanced threats. This limitation can result in missed detections or an inability to detect sophisticated attacks that exhibit low-and-slow or multi-stage behaviors. Traditional mechanisms may face challenges in terms of scalability and performance. As the volume of data and complexity of threats increase, these mechanisms may struggle to keep up with the processing demands, leading to delays in detection and response times.

To address these limitations, organizations are increasingly adopting more advanced and intelligent approaches, such as machine learning-based anomaly detection, behavior analytics, threat intelligence sharing, and security automation and orchestration. These techniques leverage artificial intelligence and automation to improve detection accuracy, reduce false positives, and enhance the speed of response to emerging threats.

7. Machine Learning for Threat Detection in Cybersecurity

Machine Learning (ML) encompasses a diverse set of techniques and algorithms that enable systems to learn patterns, make predictions, and improve performance over time without being explicitly programmed. Some of the fundamental machine learning techniques include supervised learning, unsupervised learning, semi-supervised learning, reinforcement learning, deep learning, neural networks, decision trees, random forest, support vector machines (SVM) and K-Nearest neighbours (KNN), which can be appropriately applied based on their used cases, either as classification, clustering, regression or otherwise [57].

Machine learning (ML) has proved to be a powerful tool for threat detection in cybersecurity. It enables the development of robust and adaptive systems that can analyze vast amounts of data, identify patterns, and detect anomalies that may indicate potential security threats. ML has been commonly applied in cybersecurity threat detection. Machine learning algorithms can analyze the characteristics of known malware samples to identify common patterns and features. This knowledge can be used to develop models that can detect new and unknown malware variants based on their similarities to known patterns.

ML can be used to create models that learn what "normal" behavior looks like in a system or network. These models can then identify deviations from normal behavior, which could potentially indicate malicious activity or an ongoing attack. ML techniques can be applied to network traffic analysis to identify suspicious activities or anomalies that may indicate an intrusion attempt. By learning from historical data, these models can detect new and emerging attack patterns.

ML can analyze user behavior patterns, such as login times, access patterns, and resource usage, to identify anomalies that may indicate compromised accounts or insider threats. ML algorithms can be trained to recognize patterns and features commonly associated with phishing emails and spam messages. These models can help identify and block such malicious content. ML can analyze network traffic and identify patterns that are indicative of malicious activities, such as Distributed Denial of Service (DDoS) attacks or botnet activities.

ML techniques can be utilized to prioritize vulnerabilities based on their severity and potential impact. By analyzing historical data and correlating it with vulnerability scan results, machine learning models can help security teams focus on the most critical vulnerabilities first.

It is important to note that while machine learning can be a valuable tool in threat detection, it is not a standalone solution. It should be used in combination with other security measures, such as regular patching, secure configurations, and user training, to create a robust cybersecurity strategy. Additionally, machine learning models require continuous monitoring and updating to adapt to evolving threats and avoid false positives or false negatives.

8. Recommendation

Improving accuracy in identifying cyber threats using machine learning is an important and ongoing area of research and development. Machine learning techniques can be leveraged to enhance the effectiveness of cybersecurity systems by automating threat detection, classification, and response. Machine learning models rely on well-labeled and diverse training data to learn patterns and make accurate predictions. It is crucial to have a comprehensive and up-to-date dataset that encompasses a wide range of cyber threats, including known and emerging threats. Identifying relevant features or attributes that can effectively represent cyber threats is essential. Domain knowledge and expertise in cybersecurity can help in selecting and engineering meaningful features that capture the characteristics of different threat types. Ensemble learning involves combining multiple machine learning models to make predictions. By

aggregating the outputs of individual models, ensemble methods can improve accuracy and generalization. Techniques like bagging, boosting, and stacking can be applied to create diverse and robust ensembles.

Anomaly detection techniques can be used to identify novel and previously unseen threats. By learning patterns from normal behavior, machine learning models can flag any deviations as potential threats. Unsupervised learning algorithms such as clustering, autoencoders, and one-class SVMs are commonly employed for anomaly detection. Deep learning models, particularly convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have demonstrated their effectiveness in various domains, including cybersecurity. These models can learn complex patterns and relationships in data, enabling accurate threat identification. Cyber threats are constantly evolving, and models trained on historical data may become outdated. Implementing mechanisms for continuous learning allows the model to adapt and update its knowledge with new threat information in real-time, improving accuracy in identifying emerging threats. Adversarial attacks are techniques employed by threat actors to evade detection by machine learning models. Adversarial machine learning focuses on developing robust models that can withstand such attacks. Techniques like adversarial training, defensive distillation, and input sanitization can be employed to enhance model resilience. While machine learning models can automate and augment threat identification, human expertise remains crucial. Incorporating human input and domain knowledge can help validate and interpret model predictions, improving accuracy and reducing false positives/negatives. Regularly evaluating the performance of machine learning models is essential for identifying areas of improvement. Feedback from analysts and cybersecurity experts can be used to refine and fine-tune the models, ensuring better accuracy over time.

It is important to note that while machine learning can significantly enhance cyber threat identification, it should be part of a comprehensive cybersecurity framework that includes other techniques such as network monitoring, intrusion detection systems, secure coding practices, and user awareness training.

9. Conclusion

The use of ML in proactive defense mechanisms marks a paradigm shift in cybersecurity. By harnessing the power of advanced analytics and pattern recognition, ML contributes to a more intelligent, adaptive, and efficient defense posture. The ability to detect subtle anomalies, automate responses, and continuously learn from evolving threats positions ML as a cornerstone in modern cybersecurity strategies. Machine learning and artificial intelligence algorithms can be leveraged upon to analyze large volumes of data and identify patterns, anomalies, and previously unknown threats. Machine learning models can be trained on historical data to recognize known threat patterns and improve accuracy over time.

In conclusion, while challenges exist, the integration of ML in proactive defense mechanisms represents a strategic imperative for organizations aiming to stay ahead in the cat-and-mouse game with cyber adversaries. As the field continues to evolve, addressing considerations and maximizing the strengths of ML will be pivotal in realizing its full potential in fortifying cybersecurity defenses.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] M.R. Kearney, Navigating the Eisenhower Interstate System: Paving the way for cyberspace, Explor. Media Ecol. 22 (2023) 33–48.

[2] A. Nassar, M. Kamal, Machine Learning and Big Data Analytics for Cybersecurity Threat Detection: A Holistic Review of Techniques and Case Studies, J. Artif. Intell. Mach. Learn. Manag. 5 (2021) 51–63.

[3] M. Abdel-Rahman, Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world, Eig. Rev. Sci. Technol. 7 (2023) 138–158.

[4] D.P.F. Möller, Cybersecurity in Digital Transformation, in: Guid. to Cybersecurity Digit. Transform. Trends, Methods, Technol. Appl. Best Pract., Springer, 2023: pp. 1–70.

[5] K. Bresniker, A. Gavrilovska, J. Holt, D. Milojicic, T. Tran, Grand challenge: Applying artificial intelligence and machine learning to cybersecurity, Computer (Long. Beach. Calif). 52 (2019) 45–52.

[6] I.D. Aiyanyo, H. Samuel, H. Lim, A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning, Appl. Sci. 10 (2020). https://doi.org/10.3390/app10175811.

[7] S. Raschka, J. Patterson, C. Nolet, Machine learning in python: Main developments and technology trends in data science, machine learning, and artificial intelligence, Information. 11 (2020) 193.

[8] F. Chinesta, E. Cueto, Empowering engineering with data, machine learning and artificial intelligence: a short introductive review, Adv. Model. Simul. Eng. Sci. 9 (2022) 21.

[9] A. Nassehi, R.Y. Zhong, X. Li, B.I. Epureanu, Review of machine learning technologies and artificial intelligence in modern manufacturing systems, in: Des. Oper. Prod. Networks Mass Pers. Era Cloud Technol., Elsevier, 2022: pp. 317–348.

[10] O.K. Ukoba, B. Eng, U.S. Anamu, O. Ogundare, M. Eng, M.C. Ibegbulam, O.A. Akintunlaji, A Model to Predict the Inhibitive Property of PKO on Crude Oil Pipeline ., 12 (2011) 39–44.

[11] U.S. Anamu, O.O. Ayodele, E. Olorundaisi, B.J. Babalola, P.I. Odetola, A. Ogunmefun, K. Ukoba, T.-C. Jen, P.A. Olubambi, Fundamental design strategies for advancing the development of high entropy alloys for thermo-mechanical application: A critical review, J. Mater. Res. Technol. (2023). https://doi.org/https://doi.org/10.1016/j.jmrt.2023.11.008.

[12] Y. Wang, T. Sun, S. Li, X. Yuan, W. Ni, E. Hossain, H.V. Poor, Adversarial Attacks and Defenses in Machine Learning-Empowered Communication Systems and Networks: A Contemporary Survey, IEEE Commun. Surv. Tutorials. (2023).

[13] E. Bout, V. Loscri, A. Gallais, How Machine Learning changes the nature of cyberattacks on IoT networks: A survey, IEEE Commun. Surv. Tutorials. 24 (2021) 248–279.

[14] N.D. Trung, D.T.N. Huy, T.-H. Le, IoTs, machine learning (ML), AI and digital transformation affects various industries-principles and cybersecurity risks solutions, Management. 18 (2021).

[15] S. Al-Mansoori, M. Ben Salem, The role of artificial intelligence and machine learning in shaping the future of cybersecurity: trends, applications, and ethical considerations, Int. J. Soc. Anal. 8 (2023) 1–16.

[16] R.H. Jhaveri, A. Revathi, K. Ramana, R. Raut, R.K. Dhanaraj, A review on machine learning strategies for real-world engineering applications, Mob. Inf. Syst. 2022 (2022).

[17] O. Alshaikh, S. Parkinson, S. Khan, Exploring Perceptions of Decision-Makers and Specialists in Defensive Machine Learning Cybersecurity Applications: The Need for a Standardised Approach, Comput. Secur. (2023) 103694.

[18] V. Velayutham, S. Kumar, A. Kumar, S. Raha, G.C. Saha, Analysis of Deep Learning in Real-World Applications: Challenges and Progress, Tuijin Jishu/Journal Propuls. Technol. 44 (n.d.) 2023.

[19] J. Bharadiya, Machine Learning in Cybersecurity: Techniques and Challenges, Eur. J. Technol. 7 (2023) 1–14.

[20] K. Shaukat, S. Luo, V. Varadharajan, I.A. Hameed, S. Chen, D. Liu, J. Li, Performance comparison and current challenges of using machine learning techniques in cybersecurity, Energies. 13 (2020) 2509.

[21] M.T. Nguyen, M.Q. Tran, Balancing Security and Privacy in the Digital Age: An In-Depth Analysis of Legal and Regulatory Frameworks Impacting Cybersecurity Practices, Int. J. Intell. Autom. Comput. 6 (2023) 1–12.

[22] A. Djenna, S. Harous, D.E. Saidouni, Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure, Appl. Sci. 11 (2021) 4580.

[23] A. Lakhani, AI Revolutionizing Cyber security unlocking the Future of Digital Protection, (2023).

[24] T. Krause, R. Ernst, B. Klaer, I. Hacker, M. Henze, Cybersecurity in power grids: Challenges and opportunities, Sensors. 21 (2021) 6225.

[25] F.R. Bechara, S.B. Schuch, Cybersecurity and global regulatory challenges, J. Financ. Crime. 28 (2021) 359–374.

[26] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, M. Michaloliakos, Cybersecurity challenges in the maritime sector, Network. 2 (2022) 123–138.

[27] S. Tufail, I. Parvez, S. Batool, A. Sarwat, A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid, Energies. 14 (2021) 5894.

[28] S. Gangwar, V. Narang, A Survey on Emerging Cyber Crimes and Their Impact Worldwide, in: Res. Anthol. Combat. Cyber-Aggression Online Negativity, IGI Global, 2022: pp. 1583–1595.

[29] G. Sarkar, H. Singh, S. Kumar, S.K. Shukla, Tactics, techniques and procedures of cybercrime: A methodology and tool for cybercrime investigation process, in: Proc. 18th Int. Conf. Availability, Reliab. Secur., 2023: pp. 1–10.

[30] M. Bada, J.R.C. Nurse, Profiling the cybercriminal: a systematic review of research, in: 2021 Int. Conf. Cyber Situational Awareness, Data Anal. Assess., IEEE, 2021: pp. 1–8.

[31] G. Sarkar, S.K. Shukla, Behavioral analysis of cybercrime: Paving the way for effective policing strategies, J. Econ. Criminol. (2023) 100034.

[32] J. Chigada, R. Madzinga, Cyberattacks and threats during COVID-19: A systematic literature review, South African J. Inf. Manag. 23 (2021) 1–11.

[33] M. Alsheikh, L. Konieczny, M. Prater, G. Smith, S. Uludag, The state of IoT security: Unequivocal appeal to cybercriminals, onerous to defenders, IEEE Consum. Electron. Mag. 11 (2021) 59–68.

[34] G. Fortino, A. Guerrieri, P. Pace, C. Savaglio, G. Spezzano, Iot platforms and security: An analysis of the leading industrial/commercial solutions, Sensors. 22 (2022) 2196.

[35] R. Frank, G. Schumacher, A. Tamm, The Cloud Transformation, in: Cloud Transform. Public Cloud Is Chang. Businesses, Springer, 2023: pp. 203–245.

[36] B. Berisha, E. Mëziu, I. Shabani, Big data analytics in Cloud computing: an overview, J. Cloud Comput. 11 (2022) 24.

[37] S. Yuan, X. Wu, Deep learning for insider threat detection: Review, challenges and opportunities, Comput. Secur. 104 (2021) 102221.

[38] W. Syafitri, Z. Shukur, U. Asma'Mokhtar, R. Sulaiman, M.A. Ibrahim, Social engineering attacks prevention: A systematic literature review, IEEE Access. 10 (2022) 39325–39343.

[39] A. Moallem, Cybersecurity, Privacy, and Trust, Handb. Hum. Factors Ergon. (2021) 1107–1120.

[40] P. Mulgund, B.P. Mulgund, R. Sharman, R. Singh, The implications of the California Consumer Privacy Act (CCPA) on healthcare organizations: Lessons learned from early compliance experiences, Heal. Policy Technol. 10 (2021) 100543.

[41] A. Mishra, Y.I. Alzoubi, A.Q. Gill, M.J. Anwar, Cybersecurity enterprises policies: A comparative study, Sensors. 22 (2022) 538.

[42] I. Dobák, Thoughts on the evolution of national security in cyberspace, Secur. Def. Q. 33 (2021) 75–85.

[43] M. Kopczewski, Z. Ciekanowski, J. Nowicka, K. Bakalarczyk-Burakowska, Security threats in cyberspace, Sci. J. Mil. Univ. L. Forces. 54 (2022).

[44] K.A. Al-Enezi, I.F. Al-Shaikhli, A.R. Al-Kandari, L.Z. Al-Tayyar, A survey of intrusion detection system using case study Kuwait Governments entities, in: 2014 3rd Int. Conf. Adv. Comput. Sci. Appl. Technol., IEEE, 2014: pp. 37–43.

[45] A. Sharma, B.B. Gupta, A.K. Singh, V.K. Saraswat, Advanced Persistent Threats (APT): evolution, anatomy, attribution and countermeasures, J. Ambient Intell. Humaniz. Comput. (2023) 1–27.

[46] F. Teichmann, S.R. Boticiu, B.S. Sergi, The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate?, Int. Cybersecurity Law Rev. 4 (2023) 259–280.

[47] Z. Li, Y. Ge, J. Guo, M. Chen, J. Wang, Security threat model under internet of things using deep learning and edge analysis of cyberspace governance, Int. J. Syst. Assur. Eng. Manag. 13 (2022) 1164–1176.

[48] О.С. Саприкін, Models and methods for diagnosing Zero-Day threats in cyberspace, Вісник Сучасних Інформаційних Технологій. 4 (2021) 155–167.

[49] C. Panem, S.R. Gundu, J. Vijaylaxmi, The Role of Machine Learning and Artificial Intelligence in Detecting the Malicious Use of Cyber Space, Robot. Process Autom. (2023) 19–32.

[50] D. Malaviya, Application of machine learning and artificial intelligence for securing cyber space and the role of government organization, Anusandhaan-Vigyaan Shodh Patrika. 10 (2022) 33–37.

[51] S. Vyas, J. Hannay, A. Bolton, P.P. Burnap, Automated Cyber Defence: A Review, ArXiv Prepr. ArXiv2303.04926. (2023).

[52] H.T. Reda, A. Anwar, A.N. Mahmood, Z. Tari, A Taxonomy of Cyber Defence Strategies Against False Data Attacks in Smart Grids, ACM Comput. Surv. 55 (2023) 1–37.

[53] D.C. Le, N. Zincir-Heywood, Exploring anomalous behaviour detection and classification for insider threat identification, Int. J. Netw. Manag. 31 (2021) e2109.

[54] Y. Mirsky, A. Demontis, J. Kotak, R. Shankar, D. Gelei, L. Yang, X. Zhang, M. Pintor, W. Lee, Y. Elovici, The threat of offensive ai to organizations, Comput. Secur. 124 (2023) 103006.

[55] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, N. Ghadimi, A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future, Electr. Power Syst. Res. 215 (2023) 108975.

[56] W. Ahmad, A. Rasool, A.R. Javed, T. Baker, Z. Jalil, Cyber security in IoT-based cloud computing: A comprehensive survey, Electronics. 11 (2021) 16.

[57] I.H. Sarker, Machine learning: Algorithms, real-world applications and research directions, SN Comput. Sci. 2 (2021) 160.