Advanced Exploration of Machine Learning in Cybersecurity: A Comprehensive Analysis

Publisher: IEEE

Subramany V Odeyar ; Chaithra K N ; Venugopal Rao A S ; Anupama K ; Manu M N ; Lavanya M C **All Authors**

Abstract:
In recent years, numerous researchers and professionals have uncovered the susceptibility of wireless communication technologies and systems to a range of cyber threats. ... **View more**

Metadata

Abstract:
In recent years, numerous researchers and professionals have uncovered the susceptibility of wireless communication technologies and systems to a range of cyber threats. These incursions not only jeopardize private enterprises but also pose a significant risk to governmental entities. Across the globe, researchers have proposed various strategies aimed at either preventing or mitigating the damage caused by these cyberattacks. While some of these methods have been adopted, others remain under investigation. This study aims to assess and comprehensively examine the prevailing trends in development, recent breakthroughs, and security challenges within the realm of cybersecurity. The primary constituents of these techniques for detecting cybersecurity risks encompass fraud, intrusion, spam, and virus detection. In this article, we extend the existing body of research on the utilization of machine learning models in cybersecurity and furnish a detailed analysis of machine learning methodologies.

Published in: 2023 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC)

Date of Conference: 04-05 December 2023

DOI: 10.1109/ICMNWC60182.2023.10435798

Date Added to IEEE *Xplore*: 22 February 2024

Publisher: IEEE

ISBN Information:

Conference Location: Tumkur, India

Subramany V Odeyar
Dept. of ISE, Nagarjuna College of Engineering and Technology, Bengaluru, India

Chaithra K N
Dept. of E&C, Nitte Meenakshi Institute of Technology, Bangalore, India

Venugopal Rao A S
Dept. of CS&D, Alva's Institute of Engineering and Technology, Moodbidri, India

Anupama K
Dept. of CS&E, AJ Institute of Engineering and Technology, Mangalore, India

Manu M N
Dept. of ISE, SJB Institute of Technology, Bangalore, India

Lavanya M C
Dept. of CS&E, Vidyavardhaka College of Engineering, Mysuru, India

Contents

In the present era, cyberspace serves as a crucial conduit for node-to-node information exchange, despite its array of merits and drawbacks [1]. The internet stands out as a vital reservoir, offering unfettered access to a wealth of global knowledge and resources. In 2017, worldwide, 48% of individuals utilized the internet, a figure that surged to 81% in developing nations later that same year [2]–[5]. Cyberspace, with its expansive scope, encompasses more than just the internet, encompassing users, system resources, participant technical proficiency, and much more. Cybersecurity constitutes a compendium of numerous strategies, tools, and protocols designed to safeguard cyberspace from threats and cyberattacks [6].

Authors

Subramany V Odeyar
Dept. of ISE, Nagarjuna College of Engineering and Technology, Bengaluru, India

Chaithra K N
Dept. of E&C, Nitte Meenakshi Institute of Technology, Bangalore, India

Venugopal Rao A S
Dept. of CS&D, Alva's Institute of Engineering and Technology, Moodbidri, India

Anupama K
Dept. of CS&E, AJ Institute of Engineering and Technology, Mangalore, India

Manu M N
Dept. of ISE, SJB Institute of Technology, Bangalore, India

Lavanya M C
Dept. of CS&E, Vidyavardhaka College of Engineering, Mysuru, India

Figures

References

Keywords

Metrics

More Like This

Multidimensional Detection and Evaluation System of Computer Network Security Based on Machine Learning Algorithm
2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC)
Published: 2022

Machine Learning Based Automatic Modulation Recognition for Wireless Communications: A Comprehensive Survey
IEEE Access
Published: 2021

Show More

Advanced Exploration of Machine Learning in Cybersecurity: A Comprehensive Analysis

1st Subramany V Odeyar
Dept. of ISE
Nagarjuna College of Engineering and Technology
Bengaluru, India
subbuodeyar272@gmail.com

2nd Chaithra K N
Dept. of E&C
Nitte Meenakshi Institute of Technology
Bangalore, India
chaithra.kn@nmit.ac.in

3rd Venugopal Rao A S
Dept. of CS&D
Alva's Institute of Engineering and Technology
Moodbidri, India
rao.venugopal@gmail.com

4th Anupama K
Dept. of CS&E
AJ Institute of Engineering and Technology
Mangalore, India
anupamak@ajiet.edu.in

5th Manu M N
Dept. of ISE
SJB Institute of Technology
Bangalore, India
mnmanu@sjbit.edu.in

6th Lavanya M C
Dept.of CS&E
Vidyavardhaka College of Engineering
Mysuru, India
lavanya.mc@vvce.ac.in

***Abstract*—In recent years, numerous researchers and professionals have uncovered the susceptibility of wireless communication technologies and systems to a range of cyber threats. These incursions not only jeopardize private enterprises but also pose a significant risk to governmental entities. Across the globe, researchers have proposed various strategies aimed at either preventing or mitigating the damage caused by these cyberattacks. While some of these methods have been adopted, others remain under investigation. This study aims to assess and comprehensively examine the prevailing trends in development, recent breakthroughs, and security challenges within the realm of cybersecurity. The primary constituents of these techniques for detecting cybersecurity risks encompass fraud, intrusion, spam, and virus detection. In this article, we extend the existing body of research on the utilization of machine learning models in cybersecurity and furnish a detailed analysis of machine learning methodologies.**

Keywords—Cyber security, Machine learning, cyber attacks

I. Introduction

In the present era, cyberspace serves as a crucial conduit for node-to-node information exchange, despite its array of merits and drawbacks [1]. The internet stands out as a vital reservoir, offering unfettered access to a wealth of global knowledge and resources. In 2017, worldwide, 48% of individuals utilized the internet, a figure that surged to 81% in developing nations later that same year [2-5]. Cyberspace, with its expansive scope, encompasses more than just the internet, encompassing users, system resources, participant technical proficiency, and much more. Cybersecurity constitutes a compendium of numerous strategies, tools, and protocols designed to safeguard cyberspace from threats and cyberattacks [6].

In the contemporary realm of computers and information technology, cybercrimes are proliferating at a pace outstripping the current cybersecurity infrastructure. Several factors, such as an inadequate system configuration, inexperienced personnel, and a deficiency of strategies, can heighten a computer system's susceptibility to threats [7]. The escalation of cyber threats necessitates further advancements in cybersecurity methodologies.

A notable limitation lies in the incapacity of antiquated and conventional cybersecurity approaches to counteract novel and polymorphic security attacks. Machine learning stands out as one of the predominant state-of-the-art instruments for identifying cybercrime, offering a robust solution to circumvent the constraints of conventional detection methods [5]. Scholars have engaged in deliberations on the enhancements, constraints, and shortcomings associated with employing machine learning methodologies for cyberattack detection, presenting a comparative analysis between machine learning techniques and traditional approaches. It's important to note that the realm of artificial intelligence encompasses machine learning within its purview.

Machine learning techniques are designed with the inherent capability to acquire knowledge and expertise from data and experiences, obviating the need for explicit coding [8-10]. The utility of ML methodologies is expanding across diverse domains, encompassing healthcare, commerce, education, and cybersecurity. These ML approaches find application not only in the realm of offense but also in defense, essentially playing on both sides of the metaphorical net. On the offensive front, ML tactics are employed to breach defensive fortifications, whereas on the defensive front, ML techniques are leveraged to craft swift and efficient security measures.

Cybersecurity encompasses a wide spectrum of activities, including the prevention of cyberattacks, the protection against data breaches, and the management of associated risks. Security architecture delineates various aspects of security, including security attacks, categorized as either active or passive, and security objectives. The landscape of risks is diverse and can emanate from unexpected sources and avenues, manifesting in various forms such as cyberbullying, identity theft, and threats to digital devices, autonomous systems, wireless sensor networks (WSN), wireless body area networks (WBAN), and even cyber terrorism. The contemporary world, marked by rapid scientific advancements, faces a targeted and highly perilous environment, witnessing increasingly sophisticated cybercrimes and hostile activities. A poignant illustration occurred in 2018 when Atlanta City's administration fell victim to a ransomware attack, underscoring the persistent threat of cyberattacks.

II. Literature Review

To effectively address cybersecurity risks and combat various types of attacks, including intrusion detection systems,

979-8-3503-1702-2/23/$31.00 ©2023 IEEE

2023 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC) | 979-8-3503-1702-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICMNWC60182.2023.10435798

malware detection, phishing detection, spam detection, and fraud detection, machine learning techniques are indispensable.

The primary challenges associated with employing machine learning algorithms for malware detection were examined in detail in paper [11]. According to the authors, machine learning approaches demonstrate the capability to identify polymorphic and novel attacks, leading them to assert that all existing detection techniques will ultimately be supplanted by machine learning methods.

An intrusion detection system (IDS) serves as a safeguard for computer networks, defending against malevolent incursions aimed at identifying network vulnerabilities [12]. In the realm of network analysis, intrusion detection systems can be categorized into three primary types: signature-based, anomaly-based, and hybrid-based. Machine learning methods play a pivotal role in enhancing the detection of a diverse range of intrusions across both host and network systems [13-15]. Nevertheless, there exist several challenges within this domain, notably in the realms of zero-day vulnerability detection and the identification of emerging attacks, which are considered significant hurdles for machine learning techniques.

The authors conducted a comprehensive review of articles employing machine learning to detect cyber threats, with a particular focus on intrusion detection. Notably, their analysis revealed a lack of benchmark datasets and comprehensive performance evaluations for machine learning methods in this context [16].

In papers [17-20], the authors explored the performance of machine learning methods in detecting anomalies and assessed the effectiveness of feature selection within Machine Learning Intrusion Detection Systems (ML IDS). They contended that while the Convolutional Neural Network (CNN) classifier holds promise as an effective cybersecurity classifier, its full capabilities have not been fully harnessed. Moreover, they highlighted a significant challenge stemming from the absence of accurate and complete signatures in intrusion detection system lists, which impede machine learning models from accurately identifying attacks. Additionally, they underscored the need for further research into knowledge-based and behavior-based approaches in this domain.

Researchers have elucidated the RSA factoring problem and have demonstrated that the Generic Ring Algorithm (GRA), which conducts various ring operations like addition and multiplication, inverse ring operations such as subtraction and division, and equality testing to ascertain the need for comparing two results, serves as an effective means to address the challenge of factoring N [21].

In papers [22-26], the utilization of machine learning classification algorithms in the realm of cybersecurity was thoroughly examined. In addition to discussing machine learning models, the authors explored various alternative approaches aimed at reducing error rates in intrusion and attack detection. Nevertheless, this essay primarily delves into the prominent challenges and other online threats within the domain of cybersecurity. Table 1 provides a comprehensive summary of the extensive research conducted by numerous scholars in this field.

III. Cybersecurity Threats

TABLE I. Comparison Result

Dataset	Sub Domain	Model	Accuracy
Spambase [25]	Email Spam	RF	95%
Enron [27]	Email Spam	----	—
Customized [28]	Emails	NB	85%
Spambase [29]	Email Spam	SVM, NB	SVM-79% NB-76%
Customized [30]	Tweets	DNN	86%
UCI Repository [31]	SMS	LSTM, CNN	LSTM-95% CNN-99%
Twitter Dataset [32]	Spam tweets	SVM	98%
KDD-99 [33]	—	NB, DT,RF	95%

The evolution of malicious attack technologies outpaces the development of defense mechanisms in the cybersecurity landscape. Cybersecurity aims to safeguard data, resources, privacy, and data integrity. Within cyberspace, an array of threats and attacks persist. These include but are not limited to fraud detection, malware identification, spam categorization, phishing attempts, firewall and antivirus circumvention, keystroke logging, malicious URL threats, probing activities, and various other internet-related hazards.

Malware and phishing represent substantial threats to the internet ecosystem. Phishing, a deceptive tactic, involves masquerading as a trusted entity to illicitly acquire unauthorized access to data. Typically, phishing entails sending individuals a seemingly legitimate website link that redirects them to a fraudulent page, where they are prompted to disclose their personal information [5].

In contrast, malware constitutes malicious software designed with the specific intent of infiltrating a target computer and disrupting its normal operations. There are three sub-categories within malware detection: static, dynamic, and hybrid. Static malware detection revolves around identifying malicious patterns without actually executing the programs. Another substantial threat to computer and network resources is the proliferation of spam emails or SMS messages. These spam messages consume a significant portion of network and computer resources, affecting both computer and mobile networks. Spam takes various forms on these networks, including emails, images, videos, tweets, and spam blogs, exerting a detrimental impact on their performance and efficiency.

Denial of service, logical bombs, abuse tools, snoopers, Trojan horses, viruses, worms, spam transmission, and botnets constitute some of the most prominent cyber-attack techniques [22-26]. Figure 1 provides an illustrative representation of the primary categories of cyberattacks. When the denial-of-service method is employed, it results in the loss of access for authorized users to the system and vice versa, disrupting the normal operation of the targeted system. Indeed, in a denial-of-service attack, the attacker initiates a flood of messages directed at the target computers, thereby impeding the normal flow of legitimate data. Consequently, the affected system is unable to access the Internet or engage with other systems.

Furthermore, tools that can identify and exploit network vulnerabilities are readily accessible to individuals with varying levels of expertise, making it a concern accessible to a wide range of actors, including those lacking advanced technical skills. Another kind of assault is a logic bomb, in

which a programmer inserts code into a programme so that, in the case of a particular circumstance, the programme automatically carries out damaging actions. Sniffer is another programme that intercepts routed communications and scans each packet in the data stream for certain data, such as passwords.

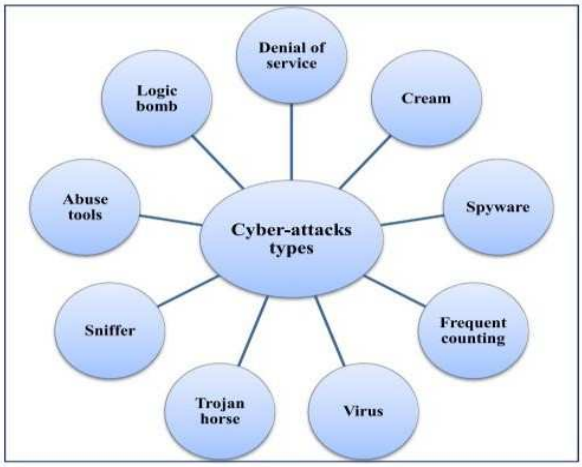

Fig. 1. Cyberattack types

A. Role of Machine Learning

Artificial intelligence (AI), a subfield of computer science, focuses on emulating human brain processes to achieve specific objectives. Within AI, machine learning is a branch that leverages past outcomes as instructions for the future, avoiding the need for explicit programming. Three pivotal types of machine learning include supervised learning, unsupervised learning, and semi-supervised learning. In supervised learning, data labels and target classes are already known. Unsupervised learning involves identifying patterns in data without prior knowledge of target classes, while semi-supervised learning blends aspects of both supervised and unsupervised approaches.

Deep learning (DL), a sub-branch of machine learning, possesses enhanced capabilities. Both machine learning and deep learning rely on experiential learning, with the key difference being that deep learning iteratively refines actions to optimize outcomes. While machine learning often employs a "divide and conquer" approach, deep learning tackles problems comprehensively from start to finish. Table 2 provides an overview of commonly employed machine learning techniques in the context of cybersecurity.

TABLE II. ML TECHNIQUES

Used Techniques	Purpose
SVM	To classify various attacks like DoS, U2R
SVM	Feature selection, Intrusion Detection
KNN	To reduce the false alarm rate
KNN	Anomaly Intrusion Detection
Random Forest	To build Network Intrusion Detection System
ANN	To measure the performance of Intrusion Detection System

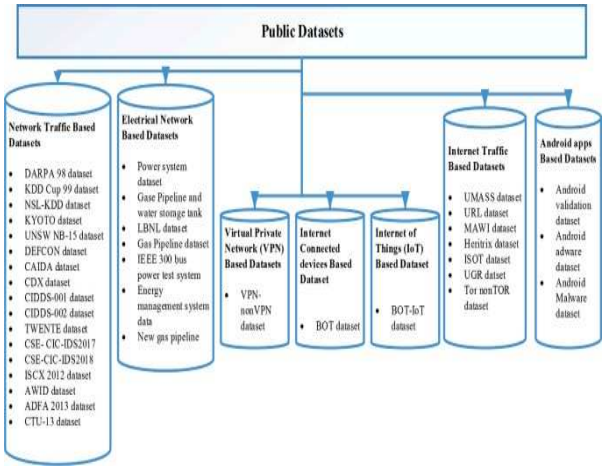

Fig. 2. Public Dataset

Figure 2 shows the publically available datasets for various cyber security threats detection using machine learning. Further the work can be enhanced by combining the dataset.

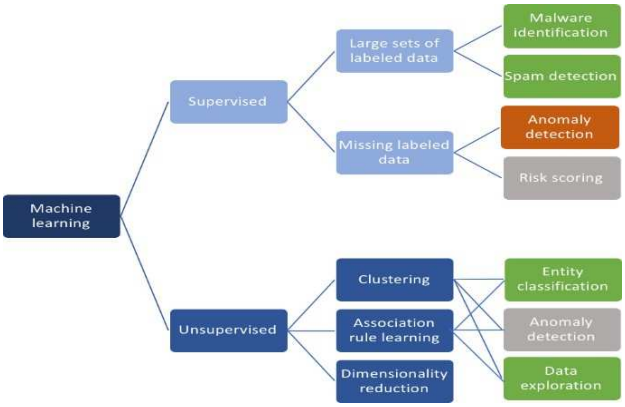

Fig. 3. Role of ML algorithms

Figure 3 illustrates the significant role that machine learning algorithms play in the detection of cybersecurity attacks, encompassing anomaly detection, network security detection, and malware identification. Machine learning is a pivotal component in executing various cybersecurity actions effectively.

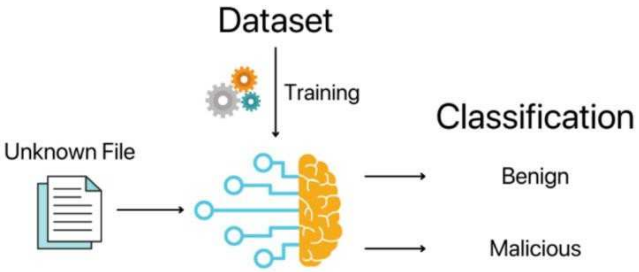

Fig. 4. Architecture for vulnerability detection

The Architecture for cyber attacks detection using machine learning is shown in Figure 4.

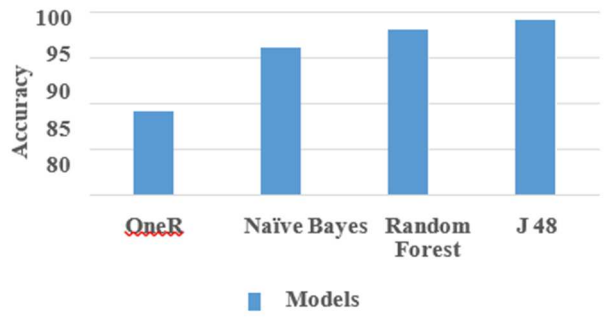

Fig. 5. Accuracy Comparison

The Figure 5 shows the accuracy obtained from various machine learning algorithms in detecting/identifying the cyber threats. The J48 is able to achieve the best accuracy compared to other ML models.

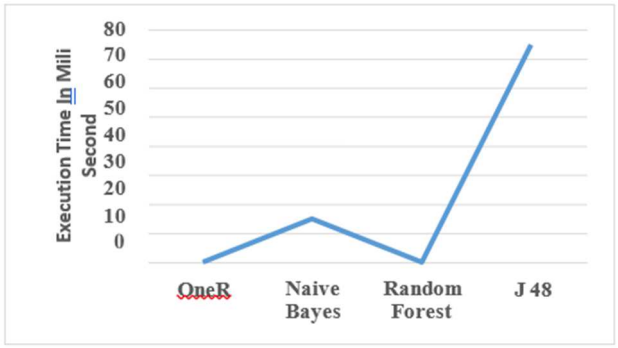

Fig. 6. Execution time

The python script was used to estimate the training time of the algorithm during the K-fold validation. The measured training time is time taken to validate all folds hence in practical scenario the training time can be estimated to be 1/Kth of the plotted time in millisecond as depicted in the Figure 6.

B. *Cyber attacks and Risks*

Cybersecurity risks consider three key factors: threats, vulnerabilities, and impacts. Threats involve those responsible for attacks, vulnerabilities are weaknesses in defenses, and impacts denote the consequences of security incidents. These incidents include malware infections, data breaches, phishing, denial of service attacks, ransomware, and insider threats, all endangering systems and networks. Vigilance, proactive measures, and effective incident response are vital for protection. These are:

- Unauthorized access refers to the act of gaining entry to a network, system, or data without proper authorization, constituting a breach of security policies.
- Malware, also known as malicious software, encompasses any program or software designed with the explicit intent of causing harm to a computer, client, server, or computer network. Common examples of malware include botnets, Trojan horses, worms, adware, ransomware, spyware, malicious bots, and computer viruses. An emerging variant known as ransomware functions by blocking users' access to their devices, personal files, or systems and subsequently demands an anonymous online payment to restore access.
- A denial-of-service attack, often referred to as a DoS attack, inundates the target with traffic, leading to a system or network crash and rendering it inaccessible to its legitimate users. Typically, a single computer and an internet connection are utilized in a denial-of-service (DoS) attack, while a distributed denial-of-service (DDoS) attack leverages multiple computers and internet connections to overwhelm the targeted resource.
- Phishing is a form of social engineering where perpetrators impersonate trustworthy individuals or organizations to deceive victims into revealing sensitive information, including banking and credit card details, login credentials, or personally identifiable information. Phishing typically employs electronic communication methods such as email, text messages, or instant messages.
- A "zero-day attack" refers to the threat stemming from an undisclosed security vulnerability that either lacks a available patch or one that the program developers were unaware of.

C. *Research Challenges*

1) Cybersecurity datasets: In the realm of cybersecurity, the primary tool for data science endeavors is the source dataset. However, a significant challenge arises from the fact that many of the available datasets are outdated, potentially failing to capture the most recent behavioral patterns exhibited by various cyberattacks. While data can be transformed into relevant knowledge through various processing tasks, understanding the characteristics of contemporary attacks and their frequency remains a persistent challenge.

Consequently, despite subsequent processing or the application of machine learning algorithms, achieving a high level of accuracy in making informed decisions remains elusive. Thus, one of the paramount challenges in the field of cybersecurity data science is the imperative need to generate up-to-date datasets tailored to specific problem domains, such as intrusion detection or cyber risk prediction. This would enable more effective analysis and decision-making in the face of evolving cyber threats.

2) Handling quality problems in cybersecurity datasets: In the realm of cybersecurity data science, datasets often exhibit a range of issues including noise, incompleteness, insignificance, imbalance, and instances of inconsistency linked to specific security incidents. These inherent problems within the data can significantly impede the learning process and undermine the efficacy of models reliant on machine learning techniques. It becomes imperative to successfully address and resolve these data challenges prior to the development of cybersecurity models to ensure data-driven and intelligent decision-making for cybersecurity solutions. Addressing such data issues, especially within specific problem domains like malware analysis or intrusion detection and prevention, necessitates a comprehensive understanding and the effective application of existing algorithms or the formulation of novel ones. Consequently, addressing these

data-related challenges represents a prominent research issue within the domain of cybersecurity data science.

3) Security policy rule generation: Security policy rules play a crucial role in managing network traffic by utilizing security zones to control, restrict, and monitor data flow based on user or user group, service, or application specifications. These policies are executed by sequentially comparing incoming traffic against both general and specific rules, with the matching rule being applied to the traffic. In many cybersecurity systems, static policy rules are predominantly employed, typically established through ontology-based methods or human expertise. While association rule learning algorithms have the potential to generate rules from data, the challenge of redundant rule generation complicates policy rule-set management. Therefore, understanding the intricacies of policy rule generation and effectively addressing them using existing or newly proposed algorithms, especially within specific problem domains like access control, represents a potential area of research within the realm of cybersecurity data science.

4) Hybrid learning method: Commercial cybersecurity systems commonly employ signature-based intrusion detection methods, which may struggle to identify unknown threats due to missing attributes or insufficient profiling. A solution to this challenge is found in hybrid strategies that combine both anomaly-based and signature-based detection methods, enhancing the system's ability to detect emerging and previously unknown threats.

D. Applications of Machine Learning

Modern cybersecurity solutions harness the power of machine learning in diverse ways, each contributing valuable insights and capabilities. When considered collectively, these approaches fundamentally transform the landscape of maintaining robust security in an ever-evolving threat environment.

1) Identification and profiling: The sheer volume of devices connecting to workplace networks makes it challenging for IT organizations to maintain awareness of each one. Machine learning offers a solution by enabling the identification and profiling of devices on a network. This profiling process can discern various features and behaviors associated with individual devices, enhancing network management and security.

2) Automated anomaly detection: Machine learning presents a compelling use case in the realm of security by facilitating the rapid identification of known malicious behaviors. Once devices are profiled and machine learning systems familiarize themselves with regular activities, they become adept at distinguishing between normal and abnormal behaviors, bolstering security efforts.

3) Zero-day detection: Traditional security systems typically require observing a harmful activity at least once to recognize it as a threat, as seen in legacy signature-based malware detection. However, machine learning introduces a proactive approach by intelligently identifying previously unknown malware and attacks, offering protection against potential zero-day threats. This shift in approach enhances cybersecurity defenses.

4) Insights at scale: When dealing with vast numbers of devices and distributed data and applications, discerning trends manually becomes an impractical task. Machine learning offers a solution by automating insights at a scale that surpasses human capabilities, allowing organizations to extract valuable information and make informed decisions efficiently.

5) Policy recommendations: The process of establishing building security regulations can often be labor-intensive and riddled with challenges. Machine learning can provide invaluable support in the form of policy recommendations for security devices, such as firewalls, by identifying the devices in place and understanding typical behavior. Machine learning can further streamline this process by autonomously generating specific recommendations, eliminating the need for users to manually navigate through complex access control lists for different devices and network segments. This automation enhances security management efficiency.

IV. Conclusion

The global concern for cybersecurity has escalated in response to the need for enhanced measures to detect and respond to cyberattacks effectively. Traditional security systems, once relied upon, have proven inadequate in the face of emerging new and polymorphic threats. Machine learning techniques have emerged as indispensable tools in cybersecurity systems, finding applications across various domains to bolster security measures.

Our examination has revealed a rapidly growing interest in the convergence of machine learning and cybersecurity within the academic, business, and government sectors. This heightened interest has translated into a notable increase in publications, particularly over the last decade. Through our research, we have endeavored to bridge the gap between machine learning techniques and the evolving threats posed to computer networks and mobile communications. This survey provides a comprehensive overview of the literature concerning machine learning algorithms applied to malware detection, spam detection, and intrusion detection across computer networks and mobile devices over the past ten years.

This study briefly explores the applications of machine learning models in the realm of cybersecurity, with a specific emphasis on advancements and developments observed over the past decade.

References

[1] Shaukat, K.; Rubab, A.; Shehzadi, I.; Iqbal, R. A Socio-Technological analysis of Cyber Crime and Cyber Security in Pakistan. Transylv. Rev. 2017, 1, 84.

[2] Saad, S.; Briguglio, W.; Elmiligi, H. The Curious Case of Machine Learning In Malware Detection. arXiv 2019,arXiv:1905.07573.

[3] Madhurya, M. J., Gururaj, H. L., Soundarya, B. C., Vidyashree, K. P., & Rajendra, A. B. (2022). Exploratory analysis of credit card fraud detection using machine learning techniques. Global Transitions Proceedings, 3(1), 31-37.

[4] Rani, S. K., Soundarya, B. C., Gururaj, H. L., & Janhavi, V. (2021, October). Comprehensive Analysis of Various Cyber Attacks. In 2021 IEEE Mysore Sub Section International Conference (MysuruCon) (pp. 255-262). IEEE.

[5] Gururaj, H. L., Lakshmi, H., Soundarya, B. C., Flammini, F., & Janhavi, V. (2022). Machine Learning-Based Approach for Fake News Detection. Journal of ICT Standardization, 509-530.

[6] HL, G., MN, N., Flammini, F., KP, V., & BC, S. (2022, March). Analysis of Finger Vein Recognition using Deep Learning Techniques:

Finger Vein Recognition. In 2022 7th International Conference on Machine Learning Technologies (ICMLT) (pp. 136-140).

[7] Gururaj, H. L., Soundarya, B. C., Janhavi, V., Lakshmi, H., & MJ, P. K. (2022, April). Analysis of Cyber Security Attacks using Kali Linux. In 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1-6). IEEE.

[8] Dharamkar, B.; Singh, R.R. A review of cyber attack classification technique based on data mining and neural network approach. Int. J. Comput. Trends Technol. 2014, 7, 100–105.

[9] Sagar, B.; Niranjan, S.; Kashyap, N.; Sachin, D. Providing Cyber Security using Artificial Intelligence–A survey.In Proceedings of the 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 27–29 March 2019; pp. 717–720.

[10] Furnell, S., et al., 2020. Understanding the full cost of cyber security breaches. Comput. Fraud Secur. 2020 (12), 6–12.

[11] Khan, S.K., et al., 2020. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. Accid. Anal. Prev. 148, 105837.

[12] Rodríguez-deArriba, M.-L., et al., 2021. Dimensions and measures of cyber dating violence in adolescents: A systematic review. Aggress. Violent Behav. 58, 101613.

[13] Zhao, J., et al., 2020. TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. Comput. Secur. 95, 101867.

[14] Zhao, Z.-g, et al., 2021. Control-theory based security control of cyber–physical power system under multiple cyber-attacks within unified model framework. Cogn. Robot. 1, 41–57.

[15] Zou, T., et al., 2020. Smart grids cyber–physical security: Parameter correction model against unbalanced false data injection attacks. Electr. Power Syst. Res. 187, 106490.

[16] Tan, S., et al., 2021. Attack detection design for dc microgrid using eigenvalue assignment approach. Energy Rep. 7, 469–476.

[17] Thomson, J.R., 2015. Cyber security, cyber-attack and cyber-espionage. In: Thom-son, J.R. (Ed.), High Integrity Systems and Safety Management in Hazardous Industries. Butterworth-Heinemann, Boston, pp. 45–53 (Chapter 3).

[18] Topping, C., et al., 2021. Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. Comput. Secur. 108, 102324.

[19] Tosun, O.K., 2021. Cyber-attacks and stock market activity. Int. Rev. Financ. Anal. 76, 101795.

[20] Varga, S., Brynielsson, J., Franke, U., 2021. Cyber-threat perception and risk management in the Swedish financial sector. Comput. Secur. 105, 102239.

[21] Zhang, T., 2017. A comparative study on sanction system of cyber aider from perspectives of German and Chinese criminal law. Comput. Law Secur. Rev.

[22] Abdallah, A.E., Mahbub, K., Palomar, E., Wagner, T.D., 2018. A novel trust taxonomy for shared cyber threat intelligence. Sec. Commun. Netw. https://doi.org/10.1155/2018/9634507. Article 9634507.

[23] HL, G., MN, N., Flammini, F., KP, V., & BC, S. (2022, March). Analysis of Finger Vein Recognition using Deep Learning Techniques: Finger Vein Recognition. In 2022 7th International Conference on Machine Learning Technologies (ICMLT) (pp. 136-140).

[24] T. Vyas, P. Prajapati, and S. Gadhwal, ''A survey and evaluation of supervised machine learning techniques for spam e-mail filtering,'' in Proc. IEEE Int. Conf. Electr., Comput. Commun. Technol. (ICECCT), Mar. 2015, pp. 1–7.

[25] Z. Khan and U. Qamar, ''Text mining approach to detect spam in emails,'' in Proc. Int. Conf. Innov. Intell. Syst. Comput. Technol. (ICIISCT), 2016, p. 45.

[26] I. J. Alkaht and B. Al Khatib, ''Filtering SPAM using several stages neural networks,'' Int. Rev. Comput. Softw., vol. 11, no. 2, p. 123, Feb. 2016.

[27] A. Tyagi, ''Content based spam classification—A deep learning approach,'' M.S. thesis, Dept. Comput. Sci., Univ. Calgary, Calgary, AB, Canada, 2016.

[28] H. Xu, W. Sun, and A. Javaid, ''Efficient spam detection across online social networks,'' in Proc. IEEE Int. Conf. Big Data Anal. (ICBDA), Mar. 2016, pp. 1–6.

[29] E.-X. Shang and H.-G. Zhang, ''Image spam classification based on convolutional neural network,'' in Proc. Int. Conf. Mach. Learn. Cybern. (ICMLC), vol. 1, Jul. 2016, pp. 398–403.

[30] G. Jain, M. Sharma, and B. Agarwal, ''Spam detection on social media using semantic convolutional neural network,'' Int. J. Knowl. Discovery Bioinf., vol. 8, no. 1, pp. 12–26, Jan. 2018.

[31] M. Bassiouni, M. Ali, and E. A. El-Dahshan, ''Ham and spam e-mails classification using machine learning techniques,'' J. Appl. Secur. Res., vol. 13, no. 3, pp. 315–331, Jul. 2018.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[32] Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. The Journal of Defense Modeling and Simulation, 19(1), 57-106.

[33] Apruzzese, Giovanni, Pavel Laskov, Edgardo Montes de Oca, Wissam Mallouli, Luis Brdalo Rapa, Athanasios Vasileios Grammatopoulos, and Fabio Di Franco. "The role of machine learning in cybersecurity." Digital Threats: Research and Practice 4, no. 1 (2023): 1-38.