International Journal of Multidisciplinary and Current Educational Research (IJMCER)
ISSN: 2581-7027 ||Volume|| 3 ||Issue|| 3 ||Pages 159-163 ||2021||

Artificial Intelligence for Offence and Defense - The Future of Cybersecurity

[1,]Alex Mathew
*Dept. of Cybersecurity Bethany College,*USA

ABSTRACT: Artificial intelligence offense perspective refers to the capability of cybercriminals using intelligence to sophisticate their attacks. While the AI defense side is about companies and individuals, using AI tools to counter cyber-attacks. The defense systems have become robust, efficient, and flexible to decrease the associated impacts of successful cyber offensive practices. The study has revealed that machine language is a part of AI with potential benefits to the current and future of cybersecurity.

KEYWORDS: offense, defense, future of cybersecurity, machine language, artificial intelligence

I. INTRODUCTION

Digital business or e-commerce has generated a novel ecosystem with advanced capabilities and security complexity. In this new ecosystem, companies ought to strike a balance between the cybersecurity (CS) framework and risks of cyber-attacks for current and future security. In recent years, artificial intelligence (AI) techniques have emerged as essential strategies for improved practices across disciplines and fields (1). The CS field is no exception. AI-oriented techniques offer better cyber defense applications and assist adversaries' enhanced approaches of attack. Cybercriminals are conscious of the innovative prospects too and often used advanced approaches for malicious purposes (1). CS entails employing defense strategies that prevent any unauthorized access of computing resources, programs, networks, destruction, or alteration. On the offense aspect, cybercriminals use artificial intelligence for enhancing their attacks' complexity and capacity. While for the defense aspects, companies use AI-based defense systems and strategies, which are efficient, flexible, and robust to automatically identify threats and adapt the best mitigation approach (1). Machine language (ML) is considered the AI-based strategy for the current and future of CS because of its capacity of discovering patterns, extracting data, and drawing inferences.

II. PROPOSED METHODOLOGY BLOCK DIAGRAM

The researcher adopted a systematic literature review for a comprehensive overview of AI and CS connections. The first step was to identify research or academic literature cited for collecting reputable and recent scholarly materials. IEEE Xplore, Google Scholar, web of science, and digital libraries were used to search and extract relevant materials (1). The second step was defining keywords related to the topic for actual search practice. The third step was for determining the reputation and precision of articles; hence, additional conditions, such as publication date 2017 to 2021 and scholarly articles were used as filter conditions. The fourth step entailed using filter criteria to obtain relevant results, which were limited to full articles published within the last five years because the aim was to determine the future of CS. The fifth step entailed reading literature and sorting them based on predetermined conditions. The last step is the compilation, synthesis, and reporting of the information in a comprehensive technical paper.

Block Diagram

Fig. 1 reveals the research approach used to collect relevant data from academic databases. It is the block diagram of the proposed methodology.

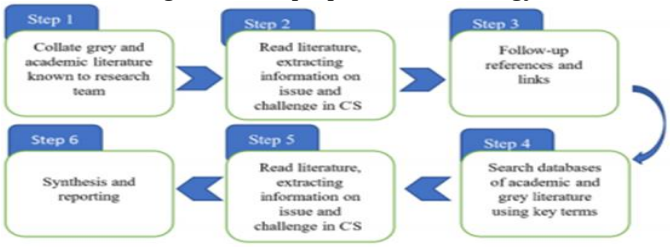

Fig. 1 Block Diagram for Methodology (14)

III. ALGORITHM

The learning algorithm of the proposed AI for defense and offense and the future CS is ML. ML is a part of AI that is essential for empowering systems based on data to learn and enhance without explicit programming (2, 15). It is connected with mathematical techniques facilitating algorithms for data extraction, patterns discovery, and drawing inferences from collected information (2). Three main ML algorithms, namely reinforcement learning, supervised learning, and unsupervised learning categorizes different ML algorithms (2).For a security concept, support vector machines (SVM), decision trees (DT), random forest (RF), Bayesian algorithms, k-nearest neighbor (KNN), principal component analysis (PCA), and association rule (AR) algorithms are the common ML algorithms (1). Experts point out that several ML algorithms are susceptible to intentional invasions by cyber-criminals. In case ML-based malware detection algorithm is likely to be bypassed by adversarial techniques, it cannot be applied in a real-world CS practice. ML is at the core of the emerging and advancing CS techniques that are fueling the milestones in an automated system for various applications (9). CS solutions are attained using ML algorithms because these algorithms categorize and cluster practices to forecast the probability of attacks.

IV. FLOW CHART

Fig. 2 presents the flowchart for the proposed method of data collection. It entailed identification of databases, preprocessing of the information, normalizing to the current study, extracting relevant SVM, and compiling results.

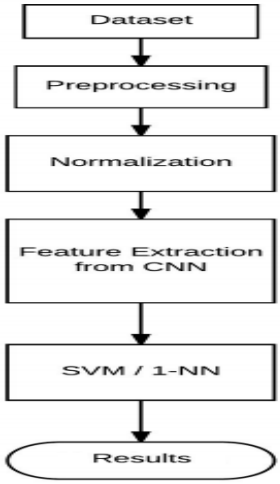

Fig. 2 Flowchart for the Method (15)

V. RESULT ANALYSIS

Results from various studies have shown that cyberspace is expanding rapidly because of many network platforms, connected devices, data emergence, and online services (12). As cyberspace grows, the frequency of cyber-attacks increases too. For instance, Japan through the National Policy Agency had detected an increase of about 4,192 unexpected connection attempts per IP address daily in 2019 (11) (See Fig. 3). The chart is revealing an increasing trend in cyber-attacks; thus, the future of the CS should advance to counter the high frequencies of cyber-attacks and attempts.

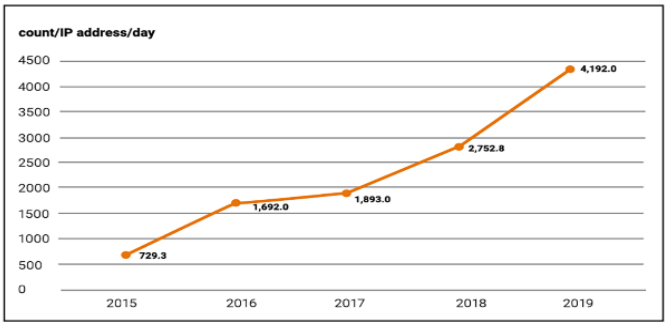

Fig. 3. Threats in Cyberspace in 2019 (11)

New services and technologies, such as the Internet of Things (IoT) and AI, have the potential for the security of the future society through new values and making people's lives sustainable (11). However, a potential risk for malicious use of these technologies is a constant concern; hence, AI for future CS defense and offense is an interest for further studies.

Defense: Scientists have identified innovative procedures applicable for AI strategies for identifying and categorizing phishing, malware, spam attacks, and network intrusions (1). They help to counter an Advanced Persistent Threat (APT) and identification of patterns created by Domain Generation Algorithms (DGAs) (1). Figure 4 presents four main categories used for cyber-attack defense mechanisms (1).

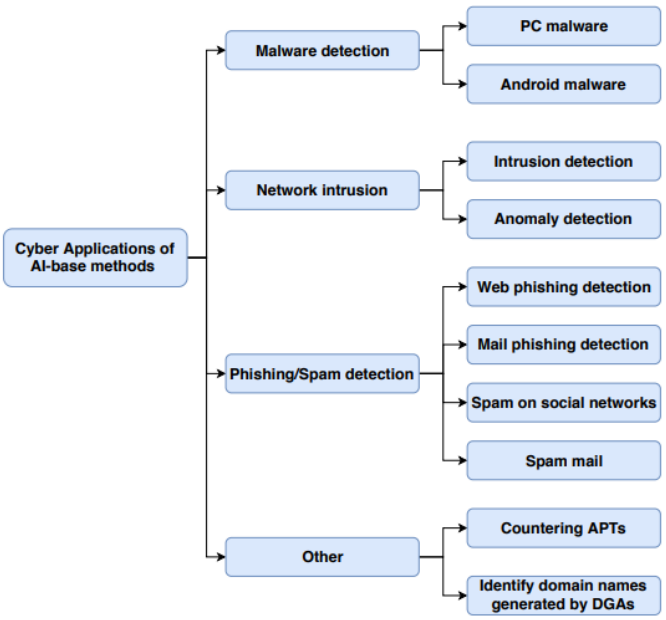

Fig. 4. Cybersecurity AI Defense Techniques (1)

The poisoning of the ML system is largely dependent on the context; however, there are AI techniques to offer defense in the real world against a potential attack (9). There is a need for imperatives of defense since attackers are adopting new approaches for ML attacks because the failure or success of cyber defenses relies on ML security models against manipulation and deception (9). Even though ML systems are identified as potential CS solutions, challenges on creating robust and universal systems that contend with all attackers' procedures are common (10). Innovative defenses are available; however, broken down into routine functions for safeguarding different systems (10). ML algorithms are always used for detecting and avoiding different attacks.

Offence: According to Truong et al (1), the AI offenses are three aspects, namely poisoning training data, adversarial inputs, and model extraction attacks. The first approach entails designing malicious inputs for erroneous model prediction to avoid detection. Scholars of the generative adversarial network (GAN) use the MalGAN algorithm to created adversarial applications bypass the black-box ML-oriented identification system (5). They created samples attack of inert portable executable (PE) for applications and anti-virus domains (6). AI defense models must counter the prediction through advanced applications. Poisoning training data entails polluting the training content of which the ML algorithm is compromised to minimize the chances of being detected by the defense systems (1, 6). Domains vulnerable to poisoning attacks are spam filtering, malware analysis, and network intrusion (7, 8). ML algorithms ought to anticipate poisoning and use countermeasures.

Model extraction attacks are applicable for remodeling the detection systems or acquisition of training data through black-box assessments (1, 8). The cybercriminal learns the functionality of ML algorithms through a reverse method. The malicious actors can understand the detector's intentions and purpose to avoid it (9). Hence, there is a need to improve ML systems to avoid these offenses and enhance the future of CS in cyberspace that continues to expand.

Analysis: Improved ML defenses provide substantial benefits to businesses and systems defending against potential attacks because they introduce new hurdles to the successful practice of offensive practices in a cyberspace (9). Offensive practices necessitate cautious preparation, assessment, and planning of target site. Hence, robust ML defenses are likely to obligate the attackers to change their plans toward the underlying ML models (9). Furthermore, it is necessary to note that hacking ML has its unique problems for attackers.The core challenge attackers have to contend with is figuring out ideal approaches of circumventing and manipulating the systems (9). The use of AI in CS generates a novel frontier for security research. Experts consider AI as a vital reaction to the continuous developments that have increased the complexity and difficulty of cyber-threats materializing (1). On the other hand, they have increased the quick reaction and substantial automatic reactions to security threats and attacks. ML is part of AI that can be exploited to enjoy the benefits and secure the future of CS.

Experts agree on the necessity to boost extents of security computerization with cyber-defense measures and ensure that CS instruments are crafted for effective interoperations that support enriched intelligence and handle emerging threats (12). AI-enabled defenses are augmenting and automating CS tasks for better performance and detections of cyber threats triage (12). Therefore, they are essential current and future mechanisms for CS. Proper implementation of AI improves cybersecurity in different ways; however, importantly, protects systems from cyber-invasions using minimal accessible resources (2). Deep ML analysis is attached to proactive prevention of cyber-criminals activities. It is also a way of taking cybersecurity to a new level of intelligence (2). Various features of AI make it suitable for cyber defense tactics and cyber offenses. Companies should adopt AI-based cyber defense capacities to protect assets, information, and reputation (3). Both offense and defense benefit from AI development; hence, creating the need for enhanced cyber intelligence, such as practical knowledge supporting decision making on cyberspace-associated issues (3, 4). ML and AL have become buzzwords in the CS industry because of the connection in purpose. CS vendors support ML as a hardening defense mechanism against uncertainties (9). The existing AI-enabled offensive instruments are evidence that attackers are using them while defense systems are also using them to avoid malicious use of the system (12, 13). Result analysis has shown that a combination of AI and ML is the future of cybersecurity because as they advance both defense and offense increase.

VI. CONCLUSION

AI for offense and defense is a common feature in the CS domain and continues to require adjustments for future security measures. Companies and businesses must invest in AI and ML approach to handle potential future defensive and offensive needs of CS. The result has hinted that ML has blurred the line between defensive and offensive cyber operations. However, it has potential algorithms that can be exploited for future secured cyberspace.

REFERENCES

[1] T. C. Truong, Q. B. Diep, and I. Zelinka, "Artificial Intelligence in the Cyber Domain: Offense and Defense" Sym., vol. 12, pp. 1-24. 2020.

[2] K. R. Bhatele, H. Shrivastava, and N. Kumari, "Chapter 9 The Role of Artificial Intelligence in Cyber Security," IGI Global., pp. 170-192, 2019.

[3] M. E. Bonfanti, "Artificial Intelligence and Cybersecurity: A Promising but Uncertain Future," - Elcano Royal Institute, pp. 1-9, 2020.

[4] A. Galyardt, R. Gupta, D. DeCapria, E. Kanal, and J. Ettinger, "Artificial Intelligence and Cyber Intelligence: An Implementation Guide," Carnegie Mellon University, pp. 1-21, 2019.

[5] W. Hu, and Y. Tan, "Generating Adversarial Malware Examples for Black-Box Attacks Based on GAN," arXiv:1702.05983, pp. 1-7, 2017.

[6] H. S. Anderson, A. Kharkar, B. Filar, D. Evans, and P. Roth, "Learning to Evade Static PE Machine Learning Malware Models via Reinforcement Learning," arXiv:1801.08917, pp. 1-9, 2018.

[7] P. Li, Q. Liu, W. Zhao, D. Wang, and S. Wang, "BEBP: An Poisoning Method against Machine Learning Based IDSs," arXiv:1803.03965, pp. 1-9, 2018.

[8] S. Chen, M. Xue, L. Fan, S. Hao, L. Xu, H. Zhu, and B. Li, "Automated Poisoning Attacks and Defenses in Malware Detection Systems: An Adversarial Machine Learning Approach. Comput. Secur., vol. 73, pp. 326–344, 2018.

[9] W. Hoffman, "AI and the Future of Cyber Competition," CSET Issue Brief, 1-35, 2021.

[10] N. Carlini, "Are Adversarial Example Defenses Improving?," February 20, 2020, https://nicholas.carlini.com/writing/2020/are-adversarial-exampe-defenses-improving.html.

[11] A. Matsuda and H. Fujita, "Why AI is the Future of Cybersecurity: Cybersecuriti Laws and Regulations 2021," 2020, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/5-why-ai-is-the-future-of-cybersecurity

[12] S. Creese, J. Saunders, L. Axon, and W. Dixon, "Future Series: Cybersecurity, Emerging Technology and Systemic Risk," Ins. Rep., pp. 1-59, 2020.

[13] T. C. King, N. Aggarwal, M. Taddeo and L. Floridi, "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions", Sci Eng Ethics, vol. 26, pp. 89–120, 2019.

[14] S. Abu , S. R. Selamat, A. Ariffin, and R. Yusof, "Cyber Threat Intelligence – Issue and Challenges," Ind. J. Elec. Eng. & Com. Sci., vol. 10, pp. 371-379, 2018.

[15] M. U. Chowdhury, F. Hammond, G. Konowicz, J. Li, C. Xin, and H. Wu, "A Few-shot Deep Learning Approach for Improved Intrusion Detection," Conf. Pap., 1-8, 2017.