Leveraging AI and ML for advance cyber security

Article *in* Journal of Artificial Intelligence & Cloud Computing · December 2022

DOI: 10.47363/JAICC/2022(1)142

1 author:

Abhishek Shukla
Syracuse University
17 PUBLICATIONS **0** CITATIONS

ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Leveraging AI and ML for Advance Cyber Security

Abhishek Shukla

USA

ABSTRACT

In the era of technology, where almost all tasks are performed through online means. Therefore, a risk cyber-attacks is quite high. Moreover, the cyber threats are continually evolved in complexity and scale, the integration of artificial intelligence and machine learning technologies stands as a beacon of hope for bolstering cybersecurity. This research article will delve into the transformative potential of Machine Learning and Artificial Intelligence in elevating various cybersecurity defenses to an advanced level. Due to this, by analyzing the extensive dataset in real-time, it is possible to exhibit the capacity to detect anomalies, impending attacks, predict and provide proactive response to different cyberattacks. It will lead towards a heralding a new paradigm in cybersecurity. Through automating routine tasks, enabling predictive analysis and improving threat detection, the cybersecurity can be minimized. It can be done through applying machine learning and Artificial intelligence as indispensable tools in safeguarding digital assets. Furthermore, the successful implementation requires expert guidance, ongoing monitoring, and holistic cybersecurity approach. With increased technology, the digital threat landscape continues to evolve and the fusion of AI and ML with cybersecurity emerges as a pivotal strategy for securing the digital frontier.

***Corresponding author**

Abhishek Shukla, USA.

Received: October 10, 2022; **Accepted:** November 20, 2022; **Published:** December 19, 2022

Keywords: Artificial Intelligence, Machine Learning, Cybersecurity, Cyberattacks, Automating Routine Task, Enabling Predictive Analysis, Improving Threat Detection, Digital Threat

Introduction

With time, the digital world is upgrading and increasing. In this world, the technology is underpinning nearly every facet of our lives and the criticality of cybersecurity has never been more pronounced. Due to this, a lot of organizations from government agencies to provide agencies are engaged in a ceaseless battle against an ever-evolving array of cyber threats. Furthermore, as the level of technology is increased so there is a need to apply such tactics by malicious actors, and applying a dynamic and innovative approach for safeguarding digital assets from cyberattacks [1].

In the past, the cybersecurity measures were not tackled properly due to less technological upgrades are grappling with the scale and sophistication of modern threats. Therefore, the static, rule-based security systems were applied to fight against the cybersecurity attacks. These systems face problems to keep pace with the rapid mutation of malware and the emergence of zero-day vulnerabilities with stealthy tactics employed by cybercriminals. In this high-stakes environment, the integration of artificial intelligence and machine learning technologies are standing as a beacon of hope. Also, these technologies are offering a transformative solution to fortify cybersecurity defenses in detail [2].

The main fact is that Artificial Intelligence and Machine learning is often referred to as the driving force behind the fourth industrial revolution. The reason is that these technologies had demonstrated their potential to revolutionize cybersecurity practices. Furthermore, these technologies also harness the power of intelligence algorithms that can easily learn, make decisions, and adapt solutions based on the data. Secondly, their ability to analyze vast datasets in real-time, give predictive outcomes, and recognize patterns in the data is nothing short of remarkable. At this capacity, it can easily hold the key to advancing the state of cybersecurity beyond what as previously conceivable [3].

Under these points, the article embarks on a journey to explore the multifaceted role of Machine learning and Artificial intelligence in the realm of advanced cybersecurity. Additionally, it will delve into how these technologies can easily automate the routine security tasks, enhance threat detection mechanism, and enabling predictive analysis for the system. On the other hand, by doing such things, it will not only be enhancing understanding level of the potential benefits linked with cybersecurity but also underscores the imperative for organizations. Therefore, they can embrace this paradigm shift in cybersecurity practices without any problem [1].

The main sections of the research article will delve into the transformative outcomes of integrating Machine Learning and Artificial Intelligence into cybersecurity. Secondly, there will be also proper information regarding the working of these technologies for enhancing thread detection accuracy, empower organization, and automate labor-intensive security tasks. On the other hand, it also contains the ability to anticipate and proactively address potential security breaches. There is also some discussion about the main role of human expertise in synergy with Artificial intelligence and Machine learning. It will show that these technologies are not providing standalone solution for the system but also a powerful tool to augment and amplifying human capabilities regarding

cybersecurity threats. However, in the future, the cyber threats will continue to grow in a complexity scale and audacity. The fusion of AI and ML with cybersecurity is representing not merely an option but an important strategic imperative [4].

Literature Review

As the integration of Machine Learning and Artificial Intelligence into the domain of cybersecurity had gathered some substantial attention from practitioners and researchers. Also, this review will also provide an in-depth analysis of the key findings and trends linked with this field that are highlighting the transformative impact of these technologies on various facets of cybersecurity [5].

Over the past decade, the use of Artificial Intelligence and Machine learning has evolved significantly due to advancement in technologies. Therefore, a lot of researchers had explored different applications of these technologies for enhancing security measures. However, particularly the AI technology has been employed to automate security processes and augment human decision-making capabilities. Secondly, the machine learning technology has been instrumental in developing predictive models and enhancing threat detection mechanism [6].

Another primary advantage of using artificial intelligence in machine learning is its ability to automate routine security task. It means that through automating the tasks like incident response, log analysis, user authentication had minimized the level of operational burden on cybersecurity teams in the organization. The reason is that through AI-driven security information and event management systems can correlate and parse security logs in real-time. Moreover, it will also identify potential threats and trigger alerts. Therefore, such automation is not accelerating incident detection but also allowing some security analysis. Another point is that such automation is not accelerating incident detection but also allowing security analyst to focus on strategic and complex aspects of cybersecurity [7].

Additionally, the machine learning and artificial intelligence technologies also demonstrated their effectiveness in improving threat detection capabilities. There were a lot of studies are showing that Machine Learning algorithms can easily identify patterns and anomalies present in vast datasets and enabling the detection of previously unknown threats. On the other hand, the deep learning models like convolutional neural networks and recurrent neural networks are also employed for the detection of malware and phishing attacks through analyzing file content and email text. These models are also learning to recognize malicious patterns and can adapt to evolving attack techniques [3].

The researchers also put focus on the predictive analysis in cybersecurity that leverages ML and AL to forecast any potential security breaches according on the historical data and patterns. The researchers had focus on showing analyzing the historical incident data. Through this, it is possible to identify commonalities and trends for preparing against the future threats [8].

The next author had focused on the vulnerability management because it is a critical aspect of cybersecurity. With the AI-driven vulnerability scanners, is simple to detect the cyberattacks. Therefore, it is emerged as a valuable tool for identifying and prioritizing vulnerabilities present in the organizational network. All these scanners are using machine learning algorithms to accessing the severity of vulnerabilities and recommend possible remedies strategies. Furthermore, through automating the scanning and assessment process, the organizations can easily address high-priority vulnerabilities promptly and minimize the window of opportunity for attackers [3].

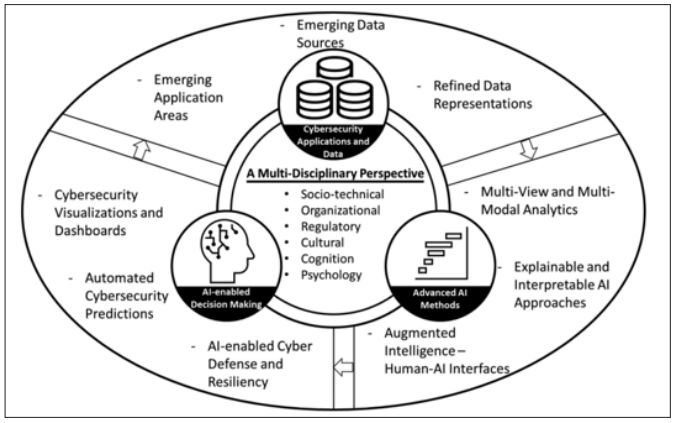

Figure 1: A Figure about Multi-Disciplinary AI for Cybersecurity Road Map Cybersecurity Application and Advanced AI-Enabled Decision-Making and Advanced AI Methods

The above image is showing about the multi-disciplinary perspective of AI technology in cybersecurity. It is consisted of three main phases. These phases include cybersecurity application and data, advanced AI methods, and AI-enabled decision making. In the cybersecurity application and data, it is dealing with emerging applications area, refined data representations, an emerging data source. The second phase is related to Advanced AI method to overcome cybersecurity issues. It includes multi-view and multi-modal analytics, Explainable and Interpretable AI approaches, and Augmented intelligences with Human AI interfaces for handling cyberattacks. Lastly, AI-enabled decision-making process. AI-enabled cyber defense and resiliency that shows relative information about AI, perform automated cybersecurity predictions for the system and cybersecurity visualization and dashboards. All these platforms are providing valuable insights about the data and AI can make efficient and real time decisions to get rid of cyber-security issues [1].

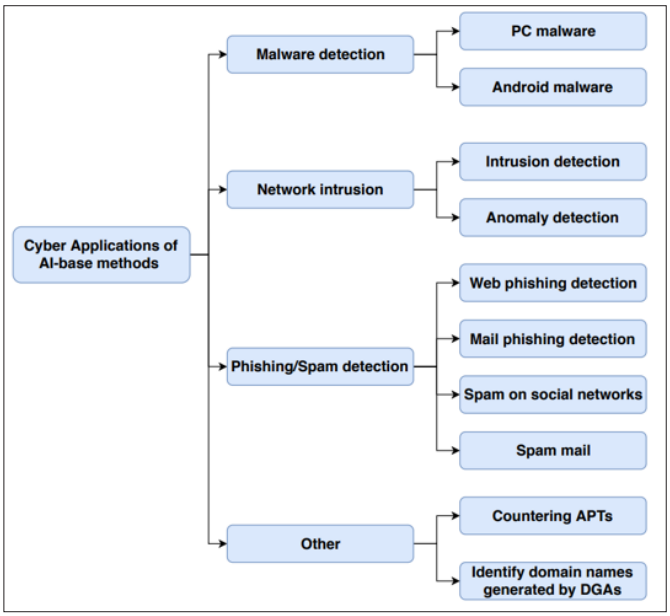

Figure 2: The Main Branches of Cybersecurity Applications Using AI Techniques

The above image is showing relative information about the main important branches of cyber application of AI-based methods. All these branches are related to solving cybersecurity issues present in the system. From this, the first branch is malware detection, the second one is network intrusion, the third one is phishing spam detection, and others. All these branches contain their own sub branches. These sub-branches are necessary to solve relative cybersecurity problems. By using AI-based methods the cybersecurity issues can be solved easily. The malware detection is divided into two important types. These types include PC malware and Android malware. Both these malware are strong and based on the required software because PC and mobile contains two different types of operating systems. However, the network intrusion is divided into two main types include intrusion detection with AI-based technology and Anomaly detection with AI-based technology. On the other hand, there are four main types of phishing/span detection. It includes web phishing detection, spam on social networks, mail phishing detection and spam mail. All these detections were operated through AI-based applications and mainly applied for the internet services [2].

Automating Routine Tasks

It is simple through machine learning and artificial intelligence technologies to automate routine cybersecurity tasks. It can be done through leveraging their ability to process and analyze the large volume of data efficiently. Its working is given below

Log Analysis

Some security logs taken from different sources like firewalls, antivirus software, and intrusion detection systems that will generate vast amount of data. Therefore, the ML and AI algorithms will be applied because they can parse and analyze these logs in real-time, identifying anomalies, and patterns. With such automation, the need of manual log review will be eliminated and it will save time and minimize risk of human errors [5].

User Authentication

With the AI-driven systems, the organizations can automate user authentication processes by analyzing user behavior and device characteristics. It means, if the user behavior is deviating significantly from the typical patterns, the system will trigger multi-factor authentication or flag the activity for further investigation process [8].

Patch Management

ML and AI is also assisting in automating patch management by prioritizing various vulnerabilities based on its potential impact and severity level on the organization. These vulnerability scanners are powered by AI and they can identify unpatched systems, and provide recommendations about most critical patches for immediate deployment [6].

Phishing Detection

The ML models can detect automatically all phishing emails by analyzing sender behavior, email content, and user interaction patterns. Some suspicious email can be flagged or quarantined for review by reducing the likelihood of successful phishing attacks [9].

Improving Threat Detection

AI and ML can easily enhance the threat detection capabilities through applying these techniques

Pattern Recognition

It is simple for ML patterns to identify known attack patterns that are present in large and complex datasets. Through training on the historical data, it is simple for the algorithms to recognize the signatures of different malware strains and attack vectors [3]. Behavioral Analysis: Due to advancement in AI-Driven technologies, they can easily identify known attack patterns even in complex dataset. Secondly, through deviations from established baselines will trigger alerts, enabling detection and minimize threats from attackers.

Enabling Predictive Analysis

The Predictive Analysis in cybersecurity leverages ML and AI to antedate and prepare for any security breaches in the system.

Historical Data Analysis

It is possible for machine learning models to analyze the historical security incident data by identifying trends and patterns linked with past attacks. Through recognizing organizations, and commonalities, the system can predict potential future trends [1].

Behavioral Predictions

Moreover, the AI-driven systems can provide prediction regarding the system behavior and give prediction based on the historical data.

Vulnerability Assessment: AI can predict all vulnerabilities easily based on known software weakness and historical exploration patterns. Through understanding where vulnerabilities are likely to emerge, the organizations can emerge them proactively [7].

Conclusion

Summing up all the discussion from above, it is concluded that leveraging ML and AI into the realm of cybersecurity has steered in a new era of advance thread defense. It will significantly be enhancing the ability to safeguard digital assets in an ever-evolving threat landscapes. When organization will apply AI and ML, then these technologies will improve the accuracy of threat detection by recognizing the main patterns anomalies. Secondly, it is also reducing false positives in the data.

Also, with the proactive and real-time response of the AI driven technologies and machine learning models has minimized cybersecurity attacks to the system. The reason is that these technologies had provided comprehensive support to the system against cyberattacks [10-13].

References

1. Ilias Maglogiannis, Elias Pimenidis, Lazaros Iliadis (2020) Artificial Intelligence Applications and Innovations: 16th IFIP WG 12.5 International Conference, AIAI 2020, Neos Marmaras, Greece, June 5–7, 2020, Proceedings, Part II. Springer Nature https://link.springer.com/book/10.1007/978-3-030-49161-1.
2. Manish Gupta, Raj Sharman, John Walp, Pavankumar Mulgund (2017) Information Technology Risk Management and Compliance in Modern Organizations, IGI Global https://www.igi-global.com/book/information-technology-risk-management-compliance/177555 .
3. A Khraisat, Iqbal Gondal, Peter Vamplew, Kamruzzaman J (2019) Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity file:///C:/Users/hp/Downloads/Survey_of_intrusion_detection_systems_techniques_d.pdf.

4. Liu XW (2021) Research on Transmission Line Fault Location Based on the Fusion of Machine Learning and Artificial Intelligence. Machine Learning for Security and Communication Networks 2021: 6648257.
5. Nir Kshetri (2017) Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications policy 41: 1027-1038.
6. Sircar A, Yadav K, Rayavarapu K, Bist N, Oza H (2021) Application of machine learning and artificial intelligence in oil and gas industry. Petroleum Research file:///C:/Users/hp/Downloads/ProofofMachinelearningpaper_firstpage.pdf.
7. Sairam Jetty SR (2019) Securing Network Infrastructure: Discover practical network security with Nmap and Nessus 7. Packt Publishing Ltd https://pdfcoffee.com/securing-network-infrastructure-discover-practical-network-security-with-nmap-and-nessus-7-pdf-free.html.
8. Rahalkar S (2018) Network Vulnerability Assessment: Identify security loopholes in your network's infrastructure. Packt Publishing Ltd https://search.worldcat.org/title/network-vulnerability-assessment-identify-security-loopholes-in-your-networks-infrastructure/oclc/1053824137.
9. Peltier J, Blackley JA, Peltier TR (2017) Managing A Network Vulnerability Assessment,. CRC Press https://www.routledge.com/Managing-A-Network-Vulnerability-Assessment/Peltier-Peltier-Blackley/p/book/9780849312700.
10. Steinberg J, Cybersecurity For Dummies. John Wiley & Sons https://www.wiley.com/en-in/bersecurity+For+Dummies,+2nd+Edition-p-9781119867180.
11. Magnusson A (2020) Practical Vulnerability Management: A Strategic Approach to Managing Cyber Risk. No Starch Press https://icdt.osu.edu/practical-vulnerability-management-strategic-approach-managing-cyber-risk.
12. Goni I, Gumpy JM, Gumpy JM (2020) Cybersecurity and Cyber Forensics: Machine Learning Approach. Machine Learning Research file:///C:/Users/hp/Downloads/Cybersecurity_and_Cyber_Forensics_Machine_Learning.pdf.
13. Huang MH, Rust RT (2018) Artificial Intelligence in Service. Journal of Service Research file:///C:/Users/hp/Downloads/Artificial_Intelligence_in_Service.pdf.