Asif *et al. (IJECI)* 2023

(IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

International Journal for
**Electronic Crime Investigation**

**DOI:** https://doi.org/10.54692/ijeci.2023.0704166

Research Article

Vol. 7 issue 4 Oct-Dec 2023

# Incorporating the Future: Optimizing Cybersecurity through Seamless Integration of Artificial Intelligence

**Muhammad Asif Ibrahim[1] and Syed Khurram Hassan[2]**

[1]Department of Mathematics, The University of Lahore, Lahore.

[2] Institute of Quality and Technology Management, University of the Punjab, Lahore, Pakistan.

Corresponding author: khuramshah6515@gmail.com

**Received:** September 27, 2023; **Accepted:** November 21, 2023; **Published:** December 22, 2023

## ABSTRACT

Cyber-attacks are becoming more sophisticated and common in today's environment. Artificial intelligence (AI) is being used by enterprises to boost their defenses against these developing threats. AI is rapidly altering the cybersecurity field, providing several benefits in terms of improving security measures. However, its implementation causes significant changes in cybersecurity occupations and necessitates the acquisition of new skills by specialists. This article investigates the impact of AI on cybersecurity employment, presents real-world instances of AI integration in the sector, analyzes the future of AI in cybersecurity, and identifies the problems involved with its adoption.

**Keywords:** Artificial Intelligence, Cyberattack, Cybersecurity, employment, skills.

## 1 INTRODUCTION

The Development of Personnel in Changeovers One of the major consequences of AI on cybersecurity is the growth of cybersecurity employees. By 2022, 40% of cybersecurity professionals, according to Gartner, will be using AI in adding to their job, contributing 100% to the ground's work force. Automation of monotonous duties like data processing, monitoring, and risk assessment is rendered possible by AI. Professionals are able to focus on more complex duties like developing and carrying out new security rules, resolving incidents, and risk management because AI relieves them of these monotonous activities [1]. Improving Job Classifications: As AI becomes integrated into cybersecurity, the cybersecurity workforce's descriptions of employment and requirements for skills are evolving. Personnel with knowledge of data analytics, machine learning, and other AI-related abilities are in higher demand among enterprises. The World Economic Forum states that cybersecurity professionals with experience in artificial intelligence, data analytics,

and big data are in considerable demand. The study demonstrates that artificial intelligence and machine learning are going to play an essential role in the future for cybersecurity professionals. Professionals must enhance these AI-related skills and evolve as AI keeps influencing the landscape of cybersecurity in order to be effective in the field [2].

Illustrations of AI in cybersecurity in the real world to enhance their efficiency, a number of cybersecurity enterprises have begun to embrace AI and implement it into the products and services they offer. Here are two notable instances: Palo Alto Networks and Cortex XDR are two companies that collaborate. Major cybersecurity firm Palo Alto Networks automates cyber threat identification and response with artificial intelligence. Their solution, Cortex XDR, utilizes machine learning algorithms to analyze data from various places and find inconsistencies that can point to a security breach. Cortex XDR enables security teams to respond to threats more quickly and efficiently by automating responding to incidents. Cylance security for endpoints and CylanceProtect Cylance utilize es artificial intelligence in order to recognize and prevent attacks online. Their AI-powered initiative, CylanceProtect, utilizes machine learning techniques to evaluate files and find malicious code before they execute. The system additionally utilizes behavioral evaluation to detect unusual behaviors while taking appropriate action. The eradication of new risks has been demonstrated to be extremely effective with this proactive approach to protecting against threats. These practical illustrations demonstrate how AI could significantly improve cybersecurity operations and protect corporations from a variety of threats [3].

## 2. THE FUTURE OF AI IN CYBERSECURITY JOBS

It is projected that AI is going to continue to play a greater part in cybersecurity. Markets & Markets anticipates that the global market for artificial intelligence in cybersecurity will grow at an exponential yearly rate of growth, approaching 23.3%, from $8.8 billion in 2019 to $38.2 billion in 2026. The expanding application of AI in threat identification, mitigation, and responses is what is generating this peak. AI utilization in cybersecurity comes with challenges; however, A lack of AI-savvy cybersecurity specialists is one of the main challenges. The rapid growth of AI technology has resulted in shortages since it has displaced the marketplace's expertise and understanding of development. Thus, in order to remain competitive in the industry, cybersecurity professionals must acquire additional expertise and learn AI-related skills [2].

## 3. AI A GAME-CHANGER IN THE FIELD OF CYBERSECURITY

AI has the capability to transform cybersecurity by advancing its efficacy and effectiveness. One of the most significant effects of AI on cybersecurity is the recognition of threats. AI systems have the ability to sort through huge quantities of data and detect trends steering to potential threats. In addition, by determining

and repairing vulnerabilities before they could be manipulated, AI is able to assist with managing vulnerabilities. AI may additionally help with behavioral exploration, which comprises analyzing user behaviour to identify unusual patterns. This may help to identify threats from inside and prevent worker-triggered breaches of information. Accordingly, automation for security could use artificial intelligence (AI), which could assist automated repetitive tasks and free up cybersecurity professionals to concentrate on more challenging tasks. Cybersecurity assistances tremendously through AI, and this impact is only going to expand in the years to come. To preserve the security and safety of the modern technological environment, investment in artificial intelligence (AI) and cybersecurity is imperative. As the world evolves more and more digitally, it is of the highest importance to use cutting-edge innovations like artificial intelligence (AI) to remain ahead of the curve and to be vigilant when it concerns cyber threats [2].

## 4. AI REVOLUTION IN CYBERSECURITY

Enormous amounts of information can potentially be managed in real time by artificial intelligence (AI) threat detection systems, which may detect potential dangers before they cause an impact. Comparing with conventional, signature-based on signatures antivirus programs, these systems are more effective because they apply machine learning algorithms that obtain information from previous attacks and respond to new attacks. Another field where artificial intelligence has had substantial effects is handling vulnerabilities. Security professionals are better competent to sense vulnerabilities in the network earlier attackers take benefit of them. by using AI-powered vulnerability indicators that can detect and classify network vulnerabilities. Another field where artificial intelligence could be applied to improve cybersecurity is behavioral analysis. Behavioral analytics programs powered by AI have the capability to keep track of user behaviors and detect variations that might indicate a cyberattack. This can speed up the method by which security professionals identify and tackle cyberattacks And last, a key field where AI may assist cybersecurity is automating procedures. Cybersecurity professionals may concentrate on challenging problems by automating everyday tasks like patching, upgrading, and monitoring. However, partner confidence is necessary for the effective implementation of AI solutions for cybersecurity. Establishing trust among partners is a necessity for transmitting information in an appropriate way and combating cyber threats. Because of the exponential growth of data and the increasing sophistication of cyber threats, traditional cybersecurity solutions are no longer suitable to defend our electronic environment. AI-based cybersecurity tools have become essential in detecting and preventing cyber-attacks. AI provides considerable advantages to firms who use it into their defense operations. Given human limits, it is impossible to discover new malware variants, phishing methods, and every single threat encountered by a company and its cloud-based services. Furthermore, evaluating the possibili-

ty of a threat is considerably more difficult due to the intensity and vulnerabilities it may draw to a server. In reaction to a danger, an unknown, undetected threat may inflict tremendous harm to a system [4].

## 5. BENEFITS OF USING AI IN CYBER SECURITY

AI and ML go hand in hand in advanced cyber security. They eliminate time consuming tasks done manually by human experts. AI and ML are assigned the duty to scan a vast amount of data to identify potential threats and minimize false positives. This lets the human experts to focus on more critical threats. AI never stops learning It analyzes network activity using machine learning modules and deep learning algorithms. It will detect deviations or security issues from the typical course of events. This enables for immediate action and improves future security measures by preventing possible threats with similar behavioral features from entering the system. Because AI is always learning, it is difficult for hackers to outwit its intellect. Similar patterns on the network are detected by AI, and when they are recognized, the AI technology will cluster them together and then proceed to determine whether there were any deviations or if any security issue happened in the usual traffic. It ultimately reacts to them after evaluating the traffic. AI will detect undiscovered risks, but detecting all possible threats to a corporation might be daunting owing to hackers' ever-changing techniques. This makes it critical to implement current solutions, such as AI technology, to efficiently identify and prevent unknown dangers, which may cause significant damage if they go undiscovered [5].

AI will be used Managing massive volumes of data within a company's network, resulting in massive amounts of network and system traffic. It takes time for cybersecurity engineers to carefully evaluate all activity for possible risks. AI technology will automatically scan and identify any disguised threats, speeding up the detection process and improving overall system security. AI improves vulnerability management. Given the regular assaults and dangers that various firms encounter, it is critical in addressing network vulnerabilities. It will review existing security procedures to identify the weakest security links, allowing these organizations to concentrate on important security responsibilities. It enhances problem-solving skills and safeguards firm systems faster than cybersecurity engineers [4].

AI is capable of enhancing overall security when hackers and different kinds of threat actors constantly change their attack tactics, making it tough for cybersecurity engineers to prioritize security related tasks. Even when dealing with many threats at the same time, AI is highly useful in recognizing all forms of assaults and prioritizing protection. Human mistake and neglect can also pose security concerns, but AI's self-learning skills can equip it to deal with them. AI technology reduces data redundancy to great extent, it can do numerous activities at once and repeat critical security duties that can weary cybersecurity workers. It will perform frequent detection and

prevention of fundamental security threats, as well as extensive analysis to discover potential security breaches and vulnerabilities. AI empowers enterprises to maintain network security by employing best practices that are regularly applied without the danger of human mistake or boredom [6].

AI can respond quickly and complete the detection phase quicker, when AI technology is used with security software, risks may be detected and responded to quickly. It will prevent permanent damage to enterprises and corporations. When compared to humans, AI can scan whole networks and security systems to spot dangers sooner and simplify security chores. It is Easier to perform Authentication while using AI enabled technologies. There are Websites that have user account features and contact forms containing user credentials and other kinds of sensitive information which is requires as an additional security layer of security for protection. This security technique may be provided by AI by utilizing various technologies such as facial recognition, CAPTCHA, and fingerprint scanners to ensure authentication during routine login attempts. It will detect fraudulent login attempts and prevent credentials from being stolen or stuffed. It is capable of detecting brute force attacks. These brute force attacks could lead to a potential security breach from company network [7].

Machine learning and AI reduces the processing time of threats and system vulnerabilities. AI is the most used critical technology in cybersecurity. It shortens the processing time of several time-consuming jobs that are performed more slowly by human specialists. It then searches massive amounts of data to identify potential dangers. After that, it filters out non-threatening activity to prevent false positives. So that human specialists may devote their attention to more vital security responsibilities. The task of detecting and eliminating bots is much easier on AI enables systems. These Bots are still an emerging threat in cybersecurity. But they are still deadly and dangerous. They can lay havoc on networks and systems through DOS or DDOS attacks. Bots are responsible for malicious activities like spreading malware and stealing data. AI can detect and stop these bots based on their behavioral patterns by producing more secure captchas. They are detected and their mode of operation is kept in the system. AI security software will use several honeypots to trap and destroy them [3].

## 6. UNVEILING THE DISADVANTAGES OF AI IN CYBER SECURITY

AI has made significant advances in a range of fields, including cyber security. Its ability to rapidly analyze enormous amounts of data and detect patterns has reignited enthusiasm in the battle against digital threats. AI in cyber security nevertheless comes with drawbacks comparable to any other type of advancement in technology. Vulnerability to Adversary Attacks: The susceptible nature of AI to adversarial attacks is an important concern in the field of cyber security. Consistently providing malicious material to AI systems with the

objective of misleading or fooling the algorithms is an adversary assault. Such assaults have the ability to deliver biased or erroneous results by taking advantage of deficiencies in AI systems. These vulnerabilities enable cybercriminals to cross through AI -based safety procedures to achieve unauthorized exploitation of networks. Attacks such as those demonstrate how important it is to constantly monitor, update, and upgrade artificial intelligence systems with the aim of reducing the risks associated with adversarial attacks [4].

### *6.1. False Positives and False Negatives*

Even though artificial intelligence algorithms aren't error-free, processes related to cyber security can confront errors such as false positives and false negatives. False positives are the consequence of artificial intelligence (AI) systems inadequately identifying risk-free behavior as harmful, resulting in redundant warnings or interferences. False negatives occur when artificial intelligence systems lack the capacity to recognize actual risks, which leaves illegal activities undiscovered. Such errors might cause pressure on security capabilities, leading to vulnerabilities. To reduce the number of false positives and false negatives, artificial intelligence models need to be improved and validated constantly; however, establishing an appropriate equilibrium can be complex [8].

### *6.2 . Lack of Human Oversight*

AI has the ability to enhance human abilities in cyber security; yet, depending just on AI systems without oversight from humans could be dangerous. While AI is intended to streamline and automate operations, it is not nearly as capable of thinking clearly as human experts and doesn't possess comparable knowledge of the context. Therefore, AI systems might make inappropriate decisions on the basis of imbalanced or inadequate data, which might result in safety breaches. Examining AI outcomes, detecting inconsistencies, and reaching sensible conclusions are all made accessible by human experts. Operative cyber security is contingent upon determining the right balance between human knowledge and artificial intelligence (AI) mechanization [9].

### *6.3. Ethical and Privacy Concerns*

Enormous amounts of data, particularly sensitive and personal data, are necessary for AI systems in cyber security to determine correlations and detect vulnerabilities. Considerations about ethics and privacy have been brought up by this dependence, specifically if the information is inappropriately archived. Privacy laws may be breached by unapproved access, breaches of data, or exploitation of personal data. It is necessary for maintaining effective information governance, encryption, and adhering to privacy principles in order to moderate these risks and keep public confidence in AI -driven cyber security resolutions [5].

### *6.4 . Evolving Threat Landscape*

A question confronting artificial intelligence-based cyber security technologies is the continuously evolving view of cyberattacks. Even though artificial intelligence algorithms are trained on past data and patterns, newer

procedures for attack or emerging risks may be recognized for the very first time. AI systems could therefore be powerless to identify and responding to threats that weren't previously unexplored. In order to remain up to date with new threats, AI models need to be constantly evaluated, updated, and trained. AI and human capability, along with current threat information, may enhance cyber threat recognition and mitigation. AI is not a comprehensive examination response, even if it could considerably enhance cyber security expertise. Adversary assaults, false positives and negatives, a non-existence of human control, moral concerns, and an evolving threat environment constitute some of the difficulties encountered by artificial intelligence-powered cyber security systems. More research, collaboration, and an extensive plan that carries concurrently the expertise of artificial intelligence with human expertise will be necessary to overcome these obstacles. By resolving these encounters, we can use the benefits of artificial intelligence while determining vigorous and reliable cyber security measures [7].

## 7. CHALLENGES WHILE IMPLEMENTING AI

The use of AI-based elucidations in the area of cyber security continues to develop, along with the increasing utilization of AI in several other domains. AI can be used to identify, stop, and react to cyberattacks. It has been shown to be an effective instrument to strengthen an organization's overall security architecture. However, while integrating artificial intelligence into cyber security, several problems need to be taken into consideration. These challenges contain a variety of challenges, such as human capability, moral encounters, and technological restrictions. In this section, we will look at the challenges accompanying with using AI for cyber security and offer sustainable solutions. Data Quality: preceding to ever contemplating incorporating artificial intelligence into cybersecurity research, the quality of data is a further problem that has to be addressed. Data quality is an additional problem that has to be addressed prior to contemplating using artificial intelligence in cybersecurity research. When collecting and analyzing data, many different kinds of errors could occur, including inaccurate information or sources that are skewed [8].

### *7.1 . Lack of Transparency in AI System*

Although being observed as a game-changer, AI in cybersecurity does not come outside its drawbacks. The lack of transparency in AI systems is one of the remarkable concerns. This is because AI systems can intermittently be thought of as "black boxes," which employ extensive mathematical computational models that are difficult for humans to understand or analyze. Due to this, it might be challenging for human experts to fully recognize the conclusions generated by these algorithms and to implement the necessary variations to improve their performance. There are several major implications for cybersecurity from the lack of transparency. unobserved threats to security could go undetected, and false positives might result in the system sounding

unnecessary warnings or cautions [9].

In additive, moral issues specifically predispositions and discrimination—are addressed by the transparency of AI algorithms. Without human operatives acknowledging it, AI systems may make racist or discriminatory choices. This could have significant concerns, mainly in law enforcement or employment operations. Researchers are examining into new methods for "explicable “AI” with the objective of addressing this task and making it possible for humans to understand the verdict-making methods of these AI systems. Among the techniques used are conversational explanations, visualization, and definitions of rules that can be easily realized by humans and that regulate the AI computer's decision-making procedure. These attempts assist individuals to identify any deficiencies as well as improve their abilities by providing them with a greater identification of how AI systems function [10].

### *7.2 . Adversarial Attacks in AI Cybersecurity*

AI cyberattacks, and countermeasures have been fascinating a lot of interest in cybersecurity research over the past few years. Many research analyses have investigated the use of AI to identify and combat adversarial aggression, but various challenges must yet be tackled before these systems can be extensively implemented. The potential of artificial intelligence-based cybersecurity attacks and defenses has been accentuated by recent research. A survey by MIT Technology Review Insights and Darktrace of more than 300 C-level executives, directors, and managers exhibited that the majority of them think artificial intelligence will become important to cybersecurity in the near future [11].

The extensive implementation of these systems remains to combat numerous difficulties, including a few studies addressing the use of artificial intelligence (AI) to identify and react to adversarial attacks. Integrating with present systems: The technique of incorporating AI systems into current environments can be confronting because of the difficulties of the technology involved. To avoid interrupting the functionality of the remaining systems, the incorporation procedure must be properly planned and conducted. This is remarkably significant because any interruption to the organization's events might have devastating effects. According to AI research in workflow management systems, the employment of AI planning attempts has the ability to address the issue of AI algorithms integrating with occurring systems. Nonetheless of the obstacles, integrating AI systems with remaining systems is vital to realizing the full promise of AI technology in many businesses. As a result, organizations must carefully plan their incorporation strategy and work together closely with their technology collaborators to ensure a successful implementation [12].

## 8. CONCLUSION

Ending on a positive note, AI is revolutionizing cybersecurity. AI simplifies actions and frees up cybersecurity professionals to deliberate on new complex duties; by 2022, 40% of these professionals will have used AI. The efficacy of threat detection and response is revealed by

applications from the industry leaders. With an estimated annual growth speed of 23.3% and attainment of $38.2 billion by 2026, the future of AI in cybersecurity seems optimistic. Ethical concerns, the delicate balance between false positives and negatives, and the adversarial security of data threats are models of challenges that need continuous consideration and model enhancement. The approach must be vigilant and systematic, with an emphasis on the incorporation of AI and human expertise. A complete fortification of security standards is guaranteed by this collaboration. If these challenges can be successfully overcome, AI will be able to recognize its full potential and play a vital role in safeguarding our digital environment from new threats.

## REFERENCES

[1] E. Benishti, "The Benefits and Risks of Using AI for Cybersecurity: A Balanced Perspective," Ironscale, 2023.

[2] World Economic Forum, "4 ways AI can help us enter a new age of cybersecurity," 2021.

[3] L. Lazic, "Benefit From AI in Cybersecurity," in The 11th International Conference on Business Information Security (BISEC-2019), Serbia, 2019.

[4] N. Papernot, P. McDaniel, A. Sinha, M. Wellman. SoK: Security and Privacy in Machine Learning. Proceedings of the IEEE Symposium on Security and Privacy, San Francisco, CA, USA. 2018.

[5] N. Carlini and D. Wagner. Towards evaluating the robustness of neural networks. In 2017 IEEE Symposium on Security and Privacy (SP). IEEE. pp. 39-57, 2017.

[6] S. Nithya. “Everyone wants to do the model work, not the data work”, Data Cascades in High-Stakes AI " proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 2021.

[7] I. Jada and T. Mayayise, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," Science Direct, vol. 100063, no. 100063, 2013.

[8] H. Nassaji. Qualitative and descriptive research: Data type versus data analysis. Language Teaching Research, vol. 19, no. 2, pp. 129-132. 2015.

[9] T. L. Lash, M. P. Fox, R. F. MacLehose, G. Maldonado, L. C. McCandless and S. Greenland, “Good practices for quantitative bias analysis”, International Journal of Epidemiology, Vol. 43, No. 6, pp. 1969-1985, 2014.

[10] M. Kearns and A. Roth. The ethical algorithm: The science of socially aware algorithm design. Oxford University Press. M. I. T. T. R. Insights, “Preparing for AI-enabled cyberattacks,” MIT Technology. 2022.

[11] A. Klubnikin, "Top 5 AI challenges &

how your company could overcome them," Ritrex, 2023.

[12] E. Anthi, L. Williams, . M. Rhode, P. Burnap and A. Wedgbury, Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems, Vol. 58, 2021.