Review

AI's Role in Fortifying Cyber Defenses: A 2024 Perspective on Machine and Deep Learning Applications

Md. Badiuzzaman Biplob *, Mahmuda Samia Konika, Kazi Mohammad Moinul Ahsan, Tasnia Zannat, Arif Ahmed

Posted Date: 9 September 2024

doi: 10.20944/preprints202409.0550.v1

Keywords: artificial intelligence; AI security; cyber security; modern security; machine learning; deep learning; cyber-attack

 doi:10.20944/preprints202409.0550.v1

Review

AI's Role in Fortifying Cyber Defenses: A 2024 Perspective on Machine and Deep Learning Applications

Md. Badiuzzaman Biplob [1,*], Mahmuda Samia Konika [2], Kazi Mohammad Moinul Ahsan [2], Tasnia Zannat [2] and Arif Ahmed [2]

[1] Computer Science and Engineering Department, Chittagong University of Engineering and Technology, Bangladesh
[2] Computer Science and Engineering Department, Daffodil Institute of IT, Bangladesh
* Correspondence: biplob.cse45@gmail.com

Abstract. By 2024, artificial intelligence (AI) will have had a revolutionary impact on cyber security, putting the sector at a critical turning point. This article explores the significant influence AI has had on cyber security procedures, outlining the progress made as well as the difficulties faced. artificial intelligence (AI) has transformed threat detection and response systems, allowing for proactive security tactics against a constantly changing array of cyber threats. By utilizing neural networks and machine learning algorithms, artificial intelligence (AI) systems can predict possible security breaches, detect unusual trends, and automatically reduce risks in real-time. These capabilities are unparalleled. Nevertheless, despite these impressive advancements, worries about data privacy, adversarial attacks, and ethical ramifications remain significant. Moreover, the never-ending game of cat and mouse between cyber attackers and defenders continues, requiring constant innovation and adaptability in cyber security strategies driven by Artificial Intelligence. In addition to providing insights into its implications for protecting digital assets and bolstering resilience against cyber threats in the changing cyber security scenario of 2024, this paper summarizes the current state of the artificial intelligence revolution in cyber security.

Keywords: artificial intelligence; AI security; cyber security; modern security; machine learning; deep learning; cyber-attack

I. Introduction

Artificial intelligence (AI) has advanced quickly, permeating daily life and having an impact on cyber security. The old reactive defensive approach has changed as a result of Artificial Intelligence's rapid growth. AI systems are now capable of evaluating massive volumes of data and foreseeing attacks before they happen. Additionally, AI may be customized to address personal vulnerabilities, creating a unique security layer. There are drawbacks to AI as well. Attackers are taking advantage of AI's ability to produce more intricate threats that can get past even the most advanced security-measures.

Cyber security will be completely transformed by the AI revolution by 2024, impacting both attackers and defenders. While attackers use AI to develop crafty tactics like phishing emails, defenders use it to create sophisticated and proactive defenses. Malware can potentially develop into self-learning programs that can elude detection methods thanks to AI. Hackers are also using AI to automate hacking processes, resulting in large-scale operations with little labor.

This study aims to propose strategies for leveraging AI to create a more secure digital future by examining how attackers and defenders employ it in numerous ways. By doing so, it will help readers comprehend the promise and problems presented by AI.

 doi:10.20944/preprints202409.0550.v1

II. The Evolution of AI in Cybersecurity

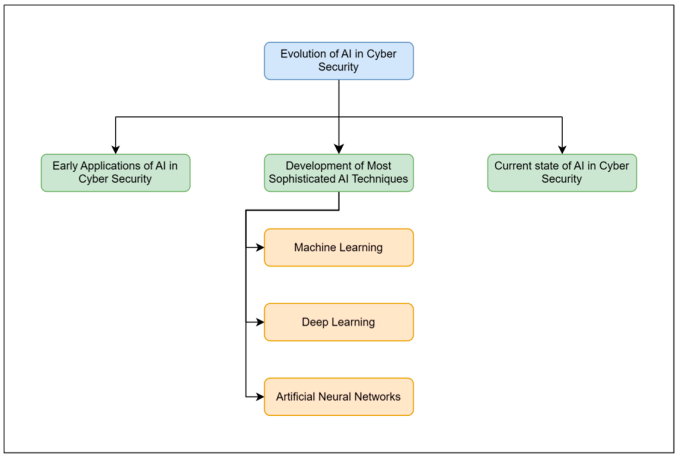


Figure 1. The AI Evolution in Cybersecurity.

A. Early Applications of AI in Cyber Security

The union of cyber security with artificial intelligence is not new. The first uses of this strong alliance went far further back in time, setting the groundwork for the more advanced instruments we use today.

Expert systems were the first iteration of AI [1]. They served as virtual security guards, continuously keeping an eye on user behavior, system activity, and network traffic. They contrasted this data with a predetermined set of patterns linked to well-known risks. Consider them as a more straightforward type of cyber security bouncer, verifying identification and sounding an alert if anything unusual is observed.

Anomaly detection was another early use. Researchers used AI to spot anomalous activities by analyzing enormous volumes of data. Imagine a system that could identify even the smallest anomaly in a sea of ordinary network data as possibly being a sign of an attempted security breach. This pioneering kind of anomaly detection made possible the increasingly complex AI-powered threat detection techniques in use today.

The most significant contribution of AI was to the automation of threat analysis using signature-based threat detection [2]. AI-assisted in the creation of digital signatures, which are distinctive identifiers used to identify known infections and malware. The ability of security systems to automatically detect and stop known dangerous software was a major advancement.

These early applications had limitations, even if they were an important place to start. Expert systems were not flexible enough to respond to emerging threats, anomaly detection might produce false positives, and attackers with malware modification skills could readily circumvent signature-based techniques. However, these initial endeavors laid the groundwork for the development of more sophisticated AI applications that are expected to revolutionize cyber security by 2024.

B. The development of More Sophisticated AI Techniques

Though revolutionary at the time, the early uses of AI in cyber security had drawbacks. They served as the technological equivalent of training wheels. More advanced AI techniques developed in tandem with the growing demand for stronger defenses. The application of AI in cyber security is changing as follows:

- Machine Learning: Without explicit programming, artificial intelligence (AI) systems can learn and advance thanks to machine learning (ML) [3], a potent technique. Imagine a security system that learns to recognize risks as it examines more data. Massive volumes of network traffic and user activity may be analyzed by ML algorithms, which can then be used to spot patterns that point to possible attacks—even brand-new ones that haven't been observed before.

 doi:10.20944/preprints202409.0550.v1

- Deep Learning: Deep learning [4] is a subset of machine learning, inspired by the structure and functioning of the human brain. These sophisticated algorithms excel at processing complicated data, including text, photos, and even malicious code. Malware can exhibit tiny alterations that can be identified by deep learning, making it more difficult for attackers to avoid detection.
- Artificial Neural Networks (ANNs): Artificial Neural Networks [5] (ANNs) are networks of algorithms that can learn and process information similarly to the linked neurons in the human brain. Artificial neural networks (ANNs) can discover anomalies and potential threats with remarkable accuracy in cyber security by analyzing network traffic and user behavior in real time.

AI is now capable of more than just pattern matching and anomaly detection thanks to these sophisticated algorithms. They make it possible for AI to continuously learn and adapt, making it a more potent foe of ever-changing cyber threats. The AI revolution in cyber security will have such a significant influence in 2024 in large part because of this growth of AI techniques.

C. The Current State of AI in Cyber Security

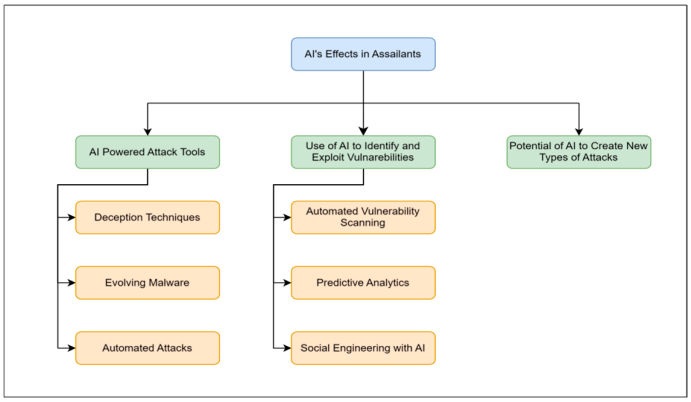
By 2024, the field of artificial intelligence in cyber security will have changed significantly and quickly. We have come a long way from those initial, basic uses that set the foundation. Attackers as well as defenders nowadays employ AI as a potent tool, making the game of cat and mouse more dangerous.

AI is being used to build a more proactive and knowledgeable security posture on the defense [6]. The workhorses are machine learning algorithms, which continuously scan through massive amounts of data to find patterns and foresee potential attacks. Imagine them as super security analysts who are always sorting through data and sounding the alert when they see something fishy. Another important component is deep learning, which is very good at identifying minute differences in malware, making it far more difficult for attackers to go unnoticed. Inspired by the human brain, artificial neural networks are ever-learning and adapting systems that can detect anomalies and possible threats in real-time with remarkable precision.

Still, the field of play isn't level. AI is being used by attackers as well [7], resulting in a new breed of complex attacks. They are utilizing AI to create self-learning malware that can avoid detection by conventional means and write deceptive phishing emails that can fool even the most cautious user. Furthermore, hackers can automate hacking procedures thanks to AI, which might lead to the initiation of massive attacks with little effort.

AI in cyber security is a two-edged sword at the moment. It gives defenders strong tools, but it also gives attackers more power. This means that to combat the constantly changing dangers from attackers who are also utilizing this potent technology, there must be a constant push to remain ahead of the curve by creating new AI-powered protections. To build a more secure digital environment, our capacity to use AI responsibly and successfully will determine the state of cyber security in 2024 and beyond.

III. AI's Effect on Attackers



 doi:10.20944/preprints202409.0550.v1

Figure 2. The Impact of AI on Attackers.

A. AI-Powered Attack Tools

The AI revolution isn't only helping defenses; attackers are also seizing the opportunity to employ this potent technology. A new generation of assault tools, intended to be more complex, deceitful, and effective, has resulted from this [8]. Here's a look at the attacker's AI-driven toolkit:

- Deception Techniques [9]: Envision an artificial intelligence that can create tailored phishing emails that exactly imitate your boss's writing style, making it nearly hard to tell them apart from real correspondence. This is the capability of assaults produced by AI. Attackers are using artificial intelligence (AI) to produce social engineering techniques, extremely convincing content, and even deepfakes to get beyond conventional security measures and deceive victims into disclosing critical information.
- Evolving Malware [10]: Static signatures were used by traditional malware, which made it simpler to identify. Now AI is altering the rules of the game. These days, attackers are creating self-learning malware that can modify its behavior and coding to avoid detection. Imagine a virus that can continuously alter its shape, making it harder for your antivirus program to identify it. Cyber security defenses are facing a serious challenge from these AI-powered attackers.
- Automated Attacks: A lot of hacking operations are repetitive, which makes them ideal for automation. Attackers are automating these procedures with AI, which enables them to conduct massive strikes with little effort. Imagine if a single attacker had command over a horde of AI-driven bots that could simultaneously target a system's weak points. This automation greatly increases the potential impact of cyber-attacks.

The use of these AI-powered technologies poses a serious challenge to cyber security experts. AI-powered dangers are always changing, necessitating increased awareness and proactive security tactics.

B. The Use of AI to Identify and Exploit Vulnerabilities

The ability of AI to recognize and take advantage of flaws is one of the most worrying things when it comes to attackers. Imagine a relentless cyberthief equipped with an extremely powerful scanner. Attackers can effectively use AI as a sophisticated tool to identify gaps in a system's defenses.

Following are some tactics that hackers are using to find vulnerabilities using AI:

- Automated Vulnerability Scanning: AI is capable of automating the process of looking for vulnerabilities in large networks. Imagine a relentless security researcher who searches for flaws all the time but with the speed and effectiveness of a machine. Compared to conventional methods, this enables attackers to locate possible entry points considerably more quickly.
- Predictive analytics: AI can identify potential vulnerabilities by analyzing past data on successful attacks and breaches. Imagine an attacker having access to a crystal ball that indicates which systems are most vulnerable, enabling them to concentrate their efforts on the most lucrative targets.
- Social Engineering with AI: AI can be used to compile data on possible targets and create customized social engineering attacks. Imagine if a hacker could examine your social media accounts and create a customized phishing email that takes advantage of your weaknesses and interests. This greatly raises the likelihood that these dishonest strategies will succeed.

Cyber security experts are quite concerned about AI's capacity to find and exploit weaknesses. To keep ahead of attackers using these potent AI technologies, it requires a proactive approach to security, with regular patching and vulnerability monitoring being essential.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 September 2024 doi:10.20944/preprints202409.0550.v1

C. The Potential for AI to Create New Types of Attacks

The potential of AI to transform into a renegade innovator as well as a smart tool in the hands of an adversary is one of the most terrifying features of this technology [11]. Envision an exceedingly sophisticated virus that possesses the ability to not only adjust to our defenses but also uncover novel avenues of attack, vulnerabilities that we haven't ever dared to imagine. AI can unleash completely new waves of unanticipated cyber-attacks, which is the danger it poses.

Similar to gifted kids, machine learning algorithms are always picking up new skills and changing as a result of the data they are exposed to. If AI were to be misused, it might be taught a perverse curriculum and taught to exploit flaws in ways that go against what we now know about cyber threats. AI is a wild card because of its unpredictable learning curve, which can produce whole new attack vectors.

Zero-day exploits, which are undiscovered software vulnerabilities, often plague security experts. AI has the potential to become the ideal exploit hunter by using its analytical skills to find these zero-day vulnerabilities far more quickly than with more conventional techniques. Consider a cyber-criminal armed with legions of AI aides who are always scouring software codes for these obscure flaws, posing a serious and persistent security threat.

Artificial intelligence (AI) has the potential to further advance social engineering, the art of deceiving others. Imagine an attacker with the uncanny ability to precisely comprehend social dynamics and human behavior by analyzing enormous amounts of social media data. With this information, one may create highly convincing social engineering efforts that are laser-focused on vast populations. AI-powered social engineering has the potential to control entire internet communities, disseminating false information and carrying out massively coordinated cyber-attacks.

IV. The Impact of AI on Defenders

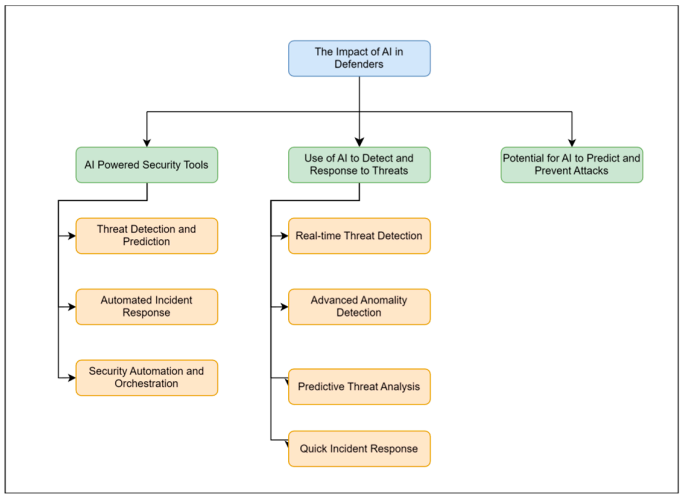


Figure 3. The Impact of AI on Defenders.

A. AI-Powered Security Tools

The AI revolution is a collaborative effort. In addition to using strong AI technologies, cyber security front-line defenders are fending against increasingly sophisticated cyber-attacks. Imagine having superpowers as a security analyst: the capacity to scan massive amounts of data, anticipate assaults before they happen, and customize defenses to target particular vulnerabilities. In 2024, AI-powered security systems should deliver on this promise.

Here's a peek at the AI toolkit that defenses are utilizing to strengthen their defenses:

- Threat Detection and Prediction: In cyber security, AI is no longer a bystander. These days, machine learning algorithms are at the forefront of threat detection [12], they detect suspicious activity by instantly evaluating user behavior and network data. Consider them as super sleuths

 doi:10.20944/preprints202409.0550.v1

who are always combing through data, sounding the alarm at the first hint of a possible attack, and sometimes even foreseeing these attacks before they happen.

- Automated Incident Response: A quicker reaction is necessary due to the growing volume and complexity of cyber-attacks. Security technologies with AI capabilities can automate incident response processes, enabling defenders to eliminate threats much more quickly [13]. Imagine if a system could automatically stop an attack to reduce damage and stop it from getting worse.
- Security Automation and Orchestration: Keeping track of a complicated network of security systems frequently leaves security staff overworked. Many of these duties can be automated by AI, freeing up security experts to concentrate on key projects. Imagine if an AI assistant handled mundane security chores, freeing up human defenders to focus on more sophisticated threats.

These AI-driven tools are revolutionary for cybersecurity defense professionals. They make it possible to analyze enormous volumes of data, spot dangers more quickly, and handle incidents with greater effectiveness.

B. The Use of AI to Detect and Respond to Threats

The conventional perception of a cyber-security defender bent over a PC, painstakingly going over records, is gradually going extinct. Defenders now have strong tools to not only identify threats but also react to them with never-before-seen accuracy and speed, all thanks to Artificial Intelligence. Let's examine in more detail how AI is changing danger detection and response:

- Real-time Threat Detection: Picture a tireless security officer who concurrently keeps an eye on every area of a digital stronghold. This is the benefit of danger detection enabled by AI. Through real-time analysis of system logs, user behavior, and network traffic, artificial intelligence (AI) can recognize suspect activities immediately. This enables defenders to thwart attackers before they have a chance to do any harm.
- Advanced Anomaly Detection: artificial intelligence is good at finding trends and abnormalities in data. This relates to cyber security as the capacity to identify minute changes in typical network traffic or user behavior that could point to a possible attack. The kind of sensitivity that AI-powered anomaly detection gives enables defenders to identify even the most cunningly camouflaged threats. Imagine a system that can identify a single drop of rain in a never-ending storm.
- Predictive threat analysis: artificial intelligence not only responds to but also anticipates potential dangers. AI systems can learn to spot patterns and anticipate potential attack sites by examining historical data on previous assaults and vulnerabilities. Envision a defense system with the ability to see into the future, exposing possible vulnerabilities so that defenders could strengthen their defenses before attackers could take advantage of them.
- Quick Incident Response: Usually there is a limited window of time in which to contain a cyberattack. The early phases of incident response can be automated by AI-powered security solutions, saving defenders a significant amount of time. Imagine a system that, in a matter of seconds, can identify a threat, instantly isolate compromised systems, stop malicious activity, and start recovery operations. This quick action can greatly reduce the harm that a cyberattack does.

AI's application in threat identification and response is revolutionizing cyber security. It enables defenders to shift from a reactive to a proactive posture, foreseeing threats and reacting to them more swiftly and accurately. This is a very important advantage in the ongoing fight against online fraudsters.

C. The Potential for AI to Predict and Prevent Attacks

AI in cyber security has true potential because it can foresee dangers rather than merely respond to them. Consider a security system that sees into the future to forecast potential assault targets and their paths, much like a digital fortune teller. In 2024, AI may be used for predictive threat assessment.

AI systems can recognize patterns and trends by examining enormous volumes of historical data on cyber-attacks, vulnerabilities, and attacker behavior. As a result, they can anticipate future attack

 doi:10.20944/preprints202409.0550.v1

targets and potential vulnerabilities with ever-greater accuracy. Consider it as an advanced risk assessment instrument that identifies weak points before they result in a significant security compromise.

Using predictive threat analysis, defenders can be more proactive when it comes to cyber security. Rather than sitting back and waiting for an attack to occur, they can concentrate on strengthening defenses in the high-risk regions that AI has identified. Consider applying security patches to vulnerabilities before they can be exploited or putting in place extra security measures around vital systems that are likely to be attacked. By being proactive, the potential damage of cyber-attacks is greatly diminished.

It's crucial to keep in mind that prediction using AI is not a perfect science. Attackers are continuously searching for new ways to get around security barriers, and cyber-attacks are no different. Although artificial intelligence (AI) can provide insightful information about possible attacks, it should be viewed as a potent tool that enhances rather than replaces existing security best practices like vulnerability management and user education.

AI's ability to anticipate and stop attacks is a big development in the war against cybercrime. It enables defenders to change their emphasis from proactive risk avoidance to reactive defense. To protect our digital environment from ever-changing cyber threats, this is an essential first step.

V. The Future of AI in Cybersecurity

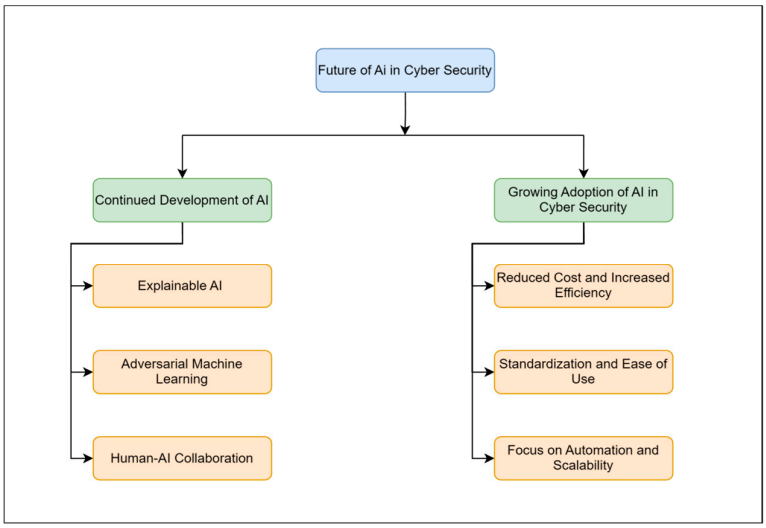


Figure 4. The Prospects of AI in Cybersecurity.

A. The Continued Development of AI Technologies

The AI revolution in cyber security is just beginning. We may anticipate more developments in AI technology as time goes on, which will change cyber threat defense even more. Here's a look at the fascinating future of cyber security enabled by AI:

- Explainable AI (XAI) [14]: One of the "black box" constraints of AI at the moment is that we don't always know how it makes its decisions. The goal of XAI is to improve the interpretability and transparency of AI's decision-making processes. This is very important in cyber security. Security experts must comprehend how AI detects risks to make sure they are not overlooking important details or responding to false positives. In the field of cyber security, the development of XAI will enable more human-AI trust and collaboration.
- Adversarial Machine Learning (AML) [15]: AI itself is a battlefield in the continuous conflict between attackers and defenders. The goal of adversarial machine learning is to provide methods for deceiving or controlling AI systems. In the context of cybersecurity, attackers can devise strategies to avoid being discovered by AI-powered security technologies. AML, however, can also be applied defensively. Defenders can create stronger security protocols by

 doi:10.20944/preprints202409.0550.v1

comprehending how attackers could attempt to control AI systems. Attackers and defenders utilizing AI are engaged in an ongoing arms race that promises to push the limits of both offensive and defensive capabilities.

- Human-AI Collaboration [16]: Building a strong partnership between humans and AI will be key to the future of cyber security, not substituting AI for human labor. While people contribute critical thinking, intuition, and the capacity to comprehend the context of danger, artificial intelligence (AI) excels in processing massive volumes of data and spotting patterns. Security teams can detect, anticipate, and respond to threats at a degree of threat detection, prediction, and reaction that is higher than either could do on its own when they combine the advantages of AI and human knowledge.

Future developments in AI technology will have a significant impact on the field of cyber security. We may anticipate seeing even more advanced defenses emerge as a result of developments in XAI, AML, and the emphasis on human-AI collaboration. This will enable us to remain ahead of the always-changing threats that lie in the digital realm.

B. The Growing Adoption of AI in Cybersecurity

The use of AI in cyber security is no longer limited to big businesses or governmental organizations with substantial security budgets. We are seeing a major trend with the maturation and accessibility of AI technology: the increasing use of AI in various industries. The following explains why AI is being used increasingly frequently as a cyber-security defensive tool:

- Reduced Costs and Increased Efficiency**:** As AI-powered security solutions become more affordable, companies of all sizes can use them. This is because of things like the commoditization of AI technology and the growth of cloud-based AI services. Security teams may work more productively, freeing up time and resources for other crucial security efforts, when AI handles regular duties like threat detection.
- Standardization and Ease of Use: Gone are the days when implementing and maintaining AI required a group of data scientists. User-friendliness is a priority in the creation of today's AI security systems. Standardized platforms with user-friendly interfaces make it possible for non-technical people as well to apply AI for threat detection and prevention. Businesses are now able to actively engage in their own cyber security protection because of this increased accessibility.
- Focus on Automation and Scalability: Security teams have a constant challenge in the ever-expanding digital ecosystem due to the overwhelming amount of data and potential threats. Security technologies with AI capabilities provide an automated solution. Artificial intelligence frees up security experts to focus on strategic objectives and complicated security issues by automating mundane duties like threat detection and incident response. Furthermore, AI solutions are naturally scalable, meaning they may expand to meet a company's expanding needs without requiring a substantial increase in resources.

Positive developments have been seen in the increasing use of AI in cyber security. It makes strong security tools more accessible to all companies, enabling them to strengthen their defenses against cyber-attacks. This broad adoption, together with the ongoing advancements in AI technology as previously mentioned, bodes well for the future of cyber security - a future in which AI and humans work together to build a more secure digital environment.

Figure 5 provides a visual representation of the complex procedure that was followed in order to compose this research paper, highlighting the meticulous steps that involved. In the meantime, Figure 6 reveals the extensive contents that are contained within this academic work, providing a glimpse into the structured depth and breadth of the work.

 doi:10.20944/preprints202409.0550.v1

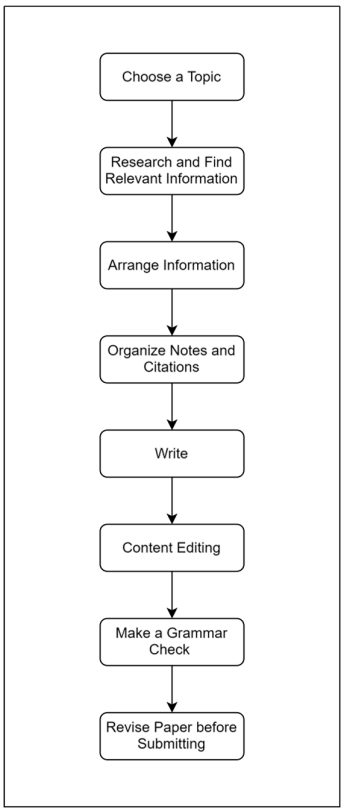


Figure 5. Process of creating this research paper.

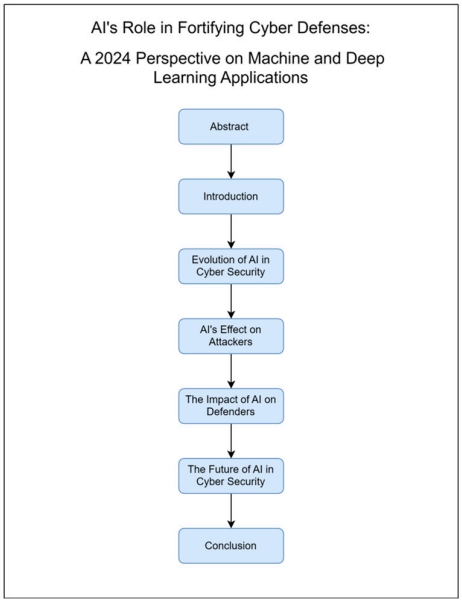


Figure 6. Contents of this paper.

VI. Conclusions

The AI revolution is set to revolutionize cyber security in 2024, introducing powerful tools for both attackers and defenders. Defenders are using AI to anticipate attacks, spot vulnerabilities, and automate incident response, while attackers are developing self-learning malware and deceitful

 doi:10.20944/preprints202409.0550.v1

strategies. The AI revolution has shifted the focus from preventive and proactive measures to reactive ones, necessitating a new strategy that recognizes the power of AI in both attackers and defenders.

Continuous research and development are crucial for AI cyber security. Defenders must innovate to keep up with attackers, while AI security solutions must be flexible and adaptable to new threats. Human-AI cooperation is also crucial, with explainable AI (XAI) enabling security experts to understand AI systems' decision-making processes.

To prepare for the future of cyber security, adopt a proactive mentality, investing in AI-powered security solutions that can analyze data, forecast attacks, and identify weaknesses. By investing in R&D, upskilling the workforce, adopting a proactive strategy, and planning for this future, we can harness the power of AI to create a more secure digital environment.

References

1. An Introduction to Neural Networks and a Comparison with Artificial Intelligence and Expert Systems. Interfaces - Zahedi, F. (1991, April 1). https://doi.org/10.1287/inte.21.2.25
2. Lee, J., Kim, J., Kim, I., & Han, K. (2019). Cyber threat detection based on artificial neural networks using event profiles. Ieee Access, 7, 165607-165626.
3. Zhu, Y. H., & Luo, Y. Z. (2019). Fast evaluation of low-thrust transfers via multilayer perceptions. Journal of Guidance, Control, and Dynamics, 42(12), 2627-2637.
4. Deep learning - LeCun, Y., Bengio, Y. & Hinton, G. Nature 521, 436–444 (28 May 2015). https://doi.org/10.1038/nature14539
5. Yegnanarayana, B. (2009). Artificial neural networks. PHI Learning Pvt. Ltd.
6. Tyugu, E. (2011, June). Artificial intelligence in cyber defense. In 2011 3rd International conference on cyber conflict (pp. 1-11). IEEE.
7. Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR), 53(1), 1-34.
8. Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. Applied Artificial Intelligence, 36(1), 2037254.
9. Zhang, L., & Thing, V. L. (2021). Three decades of deception techniques in active cyber defense-retrospect and outlook. Computers & Security, 106, 102288.
10. Sahay, S. K., Sharma, A., & Rathore, H. (2020). Evolution of malware and its detection techniques. In Information and Communication Technology for Sustainable Development: Proceedings of ICT4SD 2018 (pp. 139-150). Springer Singapore.
11. Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artificial Intelligence Review, 54(5), 3849-3886.
12. Amarasinghe, A. M. S. N., Wijesinghe, W. A. C. H., Nirmana, D. L. A., Jayakody, A., & Priyankara, A. M. S. (2019, December). AI based cyber threats and vulnerability detection, prevention and prediction system. In 2019 international conference on advancements in computing (ICAC) (pp. 363-368). IEEE.
13. Hassan, S. K., & Ibrahim, A. (2023). The role of artificial intelligence in cyber security and incident response. International Journal for Electronic Crime Investigation, 7(2).
14. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information fusion, 58, 82-115.
15. Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I., & Tygar, J. D. (2011, October). Adversarial machine learning. In Proceedings of the 4th ACM workshop on Security and artificial intelligence (pp. 43-58).
16. Wang, D., Churchill, E., Maes, P., Fan, X., Shneiderman, B., Shi, Y., & Wang, Q. (2020, April). From human-human collaboration to Human-AI collaboration: Designing AI systems that can work together with people. In Extended abstracts of the 2020 CHI conference on human factors in computing systems (pp. 1-6).