An Impact on Artificial Intelligence in Cyber Security system with its Limitations

Arun Kumar Tyagi[1], Dr. Ravindra Kumar Vishwakarma[2]

[1]Research Scholar, Department of FOCSIT, Motherhood University Roorkee, Haridwar, India
[2]Research Guide, Department of FOCSIT, Motherhood University Roorkee, Haridwar, India

Abstract:
Artificial intelligence (AI) is transforming the way value is created across enterprises, industries, communities, and society at large. As a rapidly evolving technology, AI has proven to be highly relevant in numerous global sectors. This widespread applicability has led to its integration into various business operations and industrial systems. Among its many applications, AI has shown significant promise in the field of cyber security. Cyber security itself has emerged as a critical concern in the tech-driven world, particularly as more companies adopt advanced information technologies in their operations. With the increasing reliance on digital infrastructure, there is a growing need for robust security frameworks to protect sensitive data and systems from cyber threats. This necessity has spurred a parallel rise in cyber security initiatives, with AI playing a vital role in enhancing their effectiveness. In recent years, machine learning—a subset of AI—has become a fundamental component of modern cyber security tools, offering the ability to detect, analyze, and respond to threats with speed and precision. This paper explores the intersection of AI and cyber security through a comprehensive review, aiming to assess the impact of AI technologies on securing digital environments.

Keywords: Artificial Intelligence, Cyber security, Cyber Threats, Data Protection, Vulnerability Management, AI-Driven Solutions, Information Security

Artificial Intelligence (AI) traces its origins back to the 20th century, born out of the ambition to develop systems capable of functioning independently of human cognitive input. This aspiration sparked a wave of research aimed at creating intelligent machines and robotic systems that could replicate human behavior while reducing reliance on human intervention [1]. Early developments focused on designing entities that mimicked human reasoning and decision-making processes.

Mathematics played a pivotal role in the early stages of AI, as researchers and mathematicians worked to formulate the equations and models necessary for building intelligent systems. Substantial funding from both public and private institutions accelerated these research efforts, highlighting the importance and potential of AI from its infancy. The historical progression of AI reveals a steady and impressive advancement, culminating in powerful platforms that support the development, deployment, and management of machine learning and deep learning models at scale. These platforms simplify tasks such as data processing and software deployment, making AI more accessible and cost-effective [2].

In parallel with the rise of AI, the threat landscape in cyberspace has also expanded. As cyber risks intensify, AI is increasingly leveraged as a critical tool in detecting, preventing, and mitigating cybercrime activities. The evolution of computing power and processing capabilities significantly contributed to AI's continuous advancement. As depicted in the referenced graph, public interest and technological adoption of AI steadily increased over time[3]. Even in its early stages, AI captured the attention of visionaries who foresaw its transformative potential. The development of more advanced algorithms alongside successive generations of computers fueled further innovation. Global competition among nations to achieve technological superiority drove accelerated investment and development in AI technologies. By the end of the 20th century, AI had achieved widespread recognition for its capabilities and strategic importance[4]. Continued research has since expanded AI's practical applications across multiple sectors. Figure below illustrates a detailed overview of the AI lifecycle, highlighting the iterative stages involved in building effective AI systems.

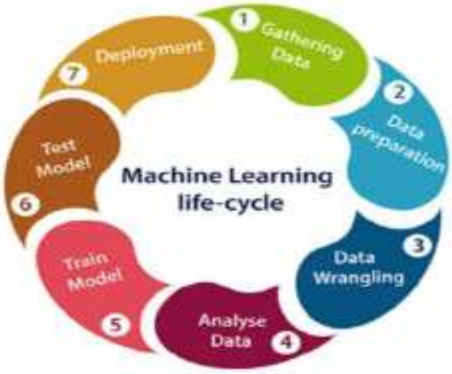


Fig. Graphical life-cycle of AI

In the present day, it is evident that artificial intelligence has experienced remarkable growth and integration across various sectors. Over time, extensive data collection and analysis have enabled AI systems to deliver highly accurate insights and predictions, making them invaluable tools for organizations and industries alike[5]. These advancements have significantly expanded the scope of AI applications. AI has been particularly transformative in fields such as banking, marketing, healthcare, and entertainment. The ability of machines to simulate human behavior and cognitive processes has led to the development of intelligent systems capable of interacting naturally with users. Robotic systems and software that emulate human actions have become increasingly sophisticated, pushing the boundaries of what machines can achieve.

One of the most notable areas of AI integration is in personal assistant technologies. Voice-activated systems such as Amazon's Alexa, Apple's Siri, and Google Assistant have revolutionized user interaction with devices, offering convenience, efficiency, and automation in daily tasks. These systems rely on natural language processing and machine learning to provide personalized assistance and enhance user experience. Figure below illustrates a range of AI applications and highlights the widespread impact of artificial intelligence across modern technologies and industries.

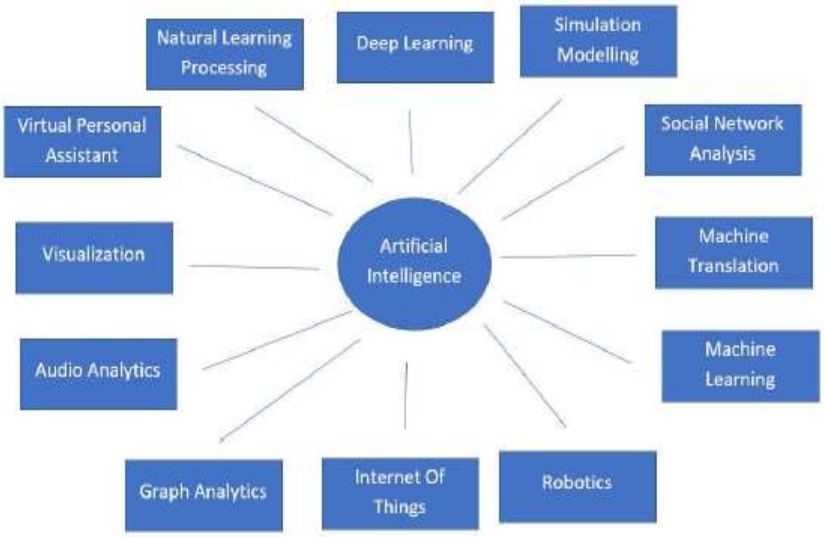


Fig . Possible Applications of Artificial Intelligence.

As previously discussed, artificial intelligence (AI) has found widespread application across various sectors and industries. Among the areas experiencing significant benefits from AI integration is cyber security. This growing intersection between AI and cyber security has brought about both notable advantages and emerging challenges, which this study aims to explore.

Cyber security refers to the practice of safeguarding computers, networks, and digital systems from unauthorized access, attacks, and damage—most of which occur via the internet [6, 7]. These attacks often result in severe financial and operational losses for organizations. Stevens [8] warns that cyber-attacks are increasingly being recognized as potential forms of digital terrorism, posing serious threats to national security and economic stability. Recent technological advancements have made businesses more vulnerable, where a single successful cyber-attack can cripple operations or compromise critical data. Trappe and Straub[9] define cyber security as the proactive protection of computing systems against threats originating from cyberspace. In this evolving threat landscape, organizations must adopt comprehensive security strategies to safeguard their digital assets. Cyber-attacks may even be instigated by competitors seeking to undermine or exploit rival companies. Therefore, implementing strong cyber security frameworks is not just a technical requirement but a strategic necessity. Protecting confidential and sensitive data has become a top priority, emphasizing the importance of cyber security measures in ensuring both organizational resilience and public trust. AI contributes significantly to these efforts by enhancing the ability to detect, prevent, and respond to cyber threats in real time, helping secure digital infrastructures more effectively than traditional methods.

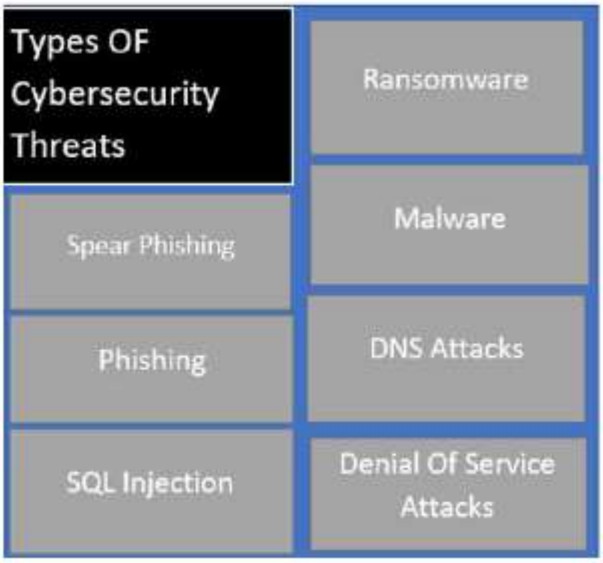


Fig. : Types of Cybersecurity Threats

Cyber security encompasses several distinct domains, each playing a vital role in ensuring the protection of digital assets for both individuals and organizations[10]. These core areas include application security, network security, information security, and operational security. When effectively implemented, these components work together to preserve privacy, uphold data integrity, and secure systems against potential threats. Achieving robust protection across these domains is essential for ensuring business continuity and sustainable growth. Figure below illustrates the various types of cyber threats that currently challenge digital security systems. As highlighted in earlier discussions, safeguarding personal and organizational information has become increasingly important. Numerous methods have been developed to counter cyber threats, and these strategies are constantly evolving to keep pace with the changing threat landscape.

Artificial intelligence has emerged as a transformative tool in this regard, offering advanced capabilities for strengthening cyber security defenses. According to Stoianov and Ivanovo[11], recent advances in AI have led to significant improvements in managing and analyzing large datasets for threat detection and prevention. By leveraging machine learning, organizations can proactively identify vulnerabilities, detect anomalies, and respond to attacks with greater speed and accuracy. AI has become a crucial enabler of modern cyber security, significantly enhancing data protection and reducing the risk of breaches. The sections below outline additional ways AI continues to reshape and reinforce cyber security practices across various industries.

Artificial intelligence (AI) has created a profound impact on the cyber security landscape. Its integration into digital systems has introduced both positive advancements and notable challenges. AI has catalyzed significant transformation across industries, and cyber security has been one of the primary beneficiaries of this technological evolution [12]. Perols and Murthy [13] emphasize that AI has reshaped the way businesses and organizations approach cyber security, although the effects are not without complexity—offering both benefits and potential risks.

Cyber-attacks have grown in sophistication, with perpetrators developing advanced methods to exploit system vulnerabilities. However, AI-driven automation, particularly through machine learning algorithms, has outpaced traditional security approaches. These algorithms adapt and respond faster than human-operated systems, preventing repeated exploitation through learned behaviors. The implementation of AI in cyber security also helps minimize human error, one of the major causes of security breaches. AI technologies fulfill diverse roles in defending digital environments [14, 15]. Ongoing research seeks to improve their efficiency in threat detection, risk analysis, and response. In today's data-centric world, safeguarding confidential information is paramount. AI enables organizations to enforce stronger protections around their data. Looking ahead, AI is expected to become even more embedded in organizational security infrastructures, advancing toward self-defending systems capable of detecting and neutralizing threats autonomously.

A defining feature of AI in cyber security is its ability to learn from experience—an essential capability that enhances resilience. By recognizing past threats, AI systems can proactively adapt to prevent future attacks. This continuous learning loop makes AI an indispensable tool in the fight against cybercrime. Scholars have described AI as a "rescue technology" in cyber security, with its predictive abilities and rapid response mechanisms offering unmatched protection [16, 17].

Modern AI systems can analyze vast data streams, detect system malfunctions, and monitor in real-time—far surpassing human monitoring capabilities [18]. These systems are capable of identifying unauthorized access attempts or anomalies and responding before any damage occurs. The capacity for real-time traffic monitoring allows AI to take preventive action, ensuring systems remain uncompromised and that sensitive data is protected. Data protection is a critical concern for businesses, and AI significantly strengthens encryption protocols. The application of complex data encryption techniques ensures the integrity and confidentiality of information [19, 20]. However, this technological progress comes with trade-offs. The efficiency of AI has, in some cases, reduced the demand for certain cyber security roles. As machines become more capable, reliance on human specialists diminishes, leading to potential job displacement in some areas of the industry [10]. Moreover, AI reduces the need for constant manual system maintenance, as it can autonomously identify and resolve issues. According to Mengidis et al. [21], machine learning-driven cyber security systems can dynamically adjust defenses based on previous attacks. These systems evolve by learning from the behaviors of attackers, making it increasingly difficult for intruders to exploit vulnerabilities. This adaptability is one of the major strengths that makes AI so effective in maintaining secure environments.

AI-Based Techniques in Cyber security Signature-Based Techniques

One of the foundational techniques by which AI enhances cyber security is signature-based detection. This method involves identifying cyber threats and malware through unique code patterns or "signatures" [28]. AI systems utilize these patterns to detect and respond to known threats by referencing databases of previously cataloged attacks [21]. These databases—often referred to as blacklists—enable quick matching of incoming code with recognized malicious signatures, allowing for rapid threat mitigation. The faster the match is made, the quicker the response, minimizing potential damage [29]. Before the adoption of AI, such detection methods were time-intensive and less efficient, often leading to significant system failures and data breaches. Signature patterns represent a form of machine learning, where the AI system continuously refines its detection criteria based on observed attack behavior [30]. However, one notable limitation of this approach is its ineffectiveness against new, previously unseen threats. If a malware's signature does not exist in the database, the system may fail to detect it. To circumvent detection, attackers often modify their tactics by altering code patterns, thereby bypassing signature-based filters [10].

Despite this limitation, signature-based AI techniques have been instrumental in preventing a significant number of cyber-attacks. Continuous refinement and the integration of hybrid approaches are improving their effectiveness. As illustrated in Figure 4, various applications of AI continue to shape and enhance cyber security frameworks, making systems more robust and less prone to compromise.

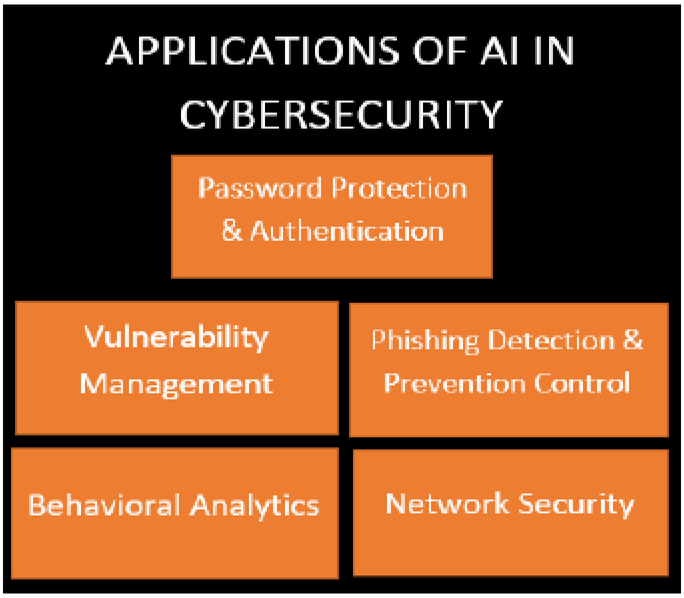

APPLICATIONS OF AI IN CYBERSECURITY
Password Protection & Authentication
Vulnerability Management
Phishing Detection & Prevention Control
Behavioral Analytics
Network Security

Fig. Application of AI in Cybersecurity

Machine Learning in Cyber security

Machine learning (ML), a subset of artificial intelligence, has significantly advanced the field of cyber security. According to Mengidis[22], human analysts are prone to errors when processing and interpreting vast datasets. AI-powered systems, by contrast, are less likely to overlook critical details or anomalies within logs and data streams. Utilizing AI for analyzing network logs and packet data has proven instrumental in identifying threats early [11]. AI systems are equipped to review large volumes of data quickly and accurately—tasks that are time-consuming and error-prone for human analysts. These systems can process and evaluate real-time data logs to detect inconsistencies or potential breaches. This analytical capability enables system administrators to promptly address and correct vulnerabilities, limiting damage or data loss. Because of this, AI is increasingly seen as a potential supplement—or even alternative—to human cyber analysts. Another advantages of AI in this context is its capacity to manage and assess vast datasets without compromising accuracy. When combined with human expertise, AI becomes even more powerful. Analysts can guide AI operations while allowing the system to perform the heavy-lifting of data processing, ensuring a comprehensive and efficient security posture[23]. Machine learning techniques such as **classification** and **clustering** help detect and identify malware. Classification compares incoming data with known benign and malicious records to identify discrepancies. Clustering, on the other hand, groups similar data and flags anomalies, which may indicate an intrusion or system compromise. These techniques have demonstrated effectiveness far beyond what is possible through manual analysis alone.

Network Intrusion Detection

Network-based attacks remain a dominant threat in the cyber security domain. Attackers often exploit vulnerabilities through networks to gain unauthorized access to sensitive information. As such, detecting and mitigating these threats at the network level is critical. AI has made significant strides in enhancing **Network Intrusion Detection Systems (NIDS)**, transforming how organizations defend their network infrastructure. By integrating AI into firewalls and other network security layers, access without proper credentials has become increasingly difficult. AI-driven firewalls can identify unusual patterns, block malicious traffic in real time, and adapt to new forms of intrusion. This proactive approach helps in stopping threats before they penetrate deeper into the system. AI's ability to gather, process, and interpret large-scale network data allows for efficient threat detection and response [23]. The presence of AI ensures a real-time security perimeter that can preemptively address potential breaches. This intelligence-driven method of defense enhances the likelihood of preventing unauthorized access and reinforces the overall resilience of an organization's digital ecosystem. As networks remain the frontline of cyber security, AI technologies continue to evolve to ensure no potential attack vector goes unnoticed. The self-learning nature of AI means these systems improve continuously, learning new patterns and methods of defense from every attempted breach [24, 25].

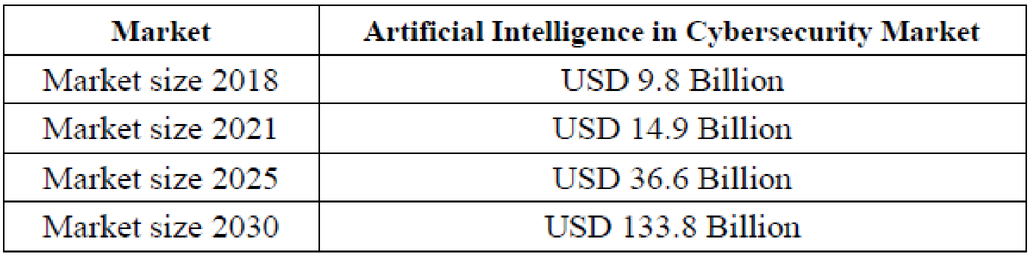
Vulnerability Management

Another critical area where AI is proving invaluable is in vulnerability management. With thousands of new vulnerabilities being discovered annually, managing and responding to them has become overwhelming for cyber security teams. In 2019 alone, approximately 20,362 vulnerabilities were reported—a staggering 18% increase from the previous year. This exponential growth in threats has necessitated the adoption of AI systems capable of identifying, prioritizing, and responding to system vulnerabilities at scale. AI tools can automate the detection of exposure points in software and hardware, helping organizations shore up their defenses before an attack occurs. This capability significantly reduces the window of opportunity for hackers to exploit system weaknesses.

IBM's research on AI-driven cyber security strategies confirms that even during global disruptions like the COVID-19 pandemic, organizations have continued to increase their investment in AI-based protection solutions [26]. The growing reliance on digital systems underscores the need for efficient, automated vulnerability management systems that can stay ahead of emerging threats.

AI enhances vulnerability management by monitoring systems continuously, scanning for weak points, and recommending actionable steps to eliminate them. This results in more secure infrastructures and reduced risk exposure for enterprises across industries.

Table . Artificial Intelligence Valuation in Cybersecurity market prediction



Market	Artificial Intelligence in Cybersecurity Market
Market size 2018	USD 9.8 Billion
Market size 2021	USD 14.9 Billion
Market size 2025	USD 36.6 Billion
Market size 2030	USD 133.8 Billion

Securing Data Centers with AI

Data centers are integral components of modern organizations, housing sensitive and critical data that must be safeguarded against cyber threats. Artificial intelligence has become increasingly essential in enhancing the security of these environments [28]. One of the main advantages of AI in this context is its ability to automate operational processes, such as controlling power usage, bandwidth allocation, and temperature regulation. These aspects are crucial for maintaining optimal performance and preventing system failures or breaches. Human error has historically been a major challenge in managing data centers. AI technologies reduce this risk by providing consistent, real-time monitoring and response. Moreover, AI enhances the cost-efficiency of managing these centers by reducing hardware maintenance costs and predicting equipment failures before they occur. These predictive capabilities contribute to more stable and secure infrastructures. AI also plays a vital role in protecting data centers from environmental and operational risks, further ensuring the security of the valuable data they house. Given these advantages, many companies have integrated AI into their data center operations to improve performance, minimize downtime, and bolster overall cyber security [23]. Furthermore, AI's role in vulnerability detection extends to internal systems. Machine learning algorithms can identify anomalies in user accounts, flagging potentially malicious behavior from within the organization.

Limitations of AI in Cyber security

While artificial intelligence offers transformative benefits in cyber security, it is not without limitations. A historical perspective highlights humanity's persistent drive to control and optimize the environment for survival and progress. From Darwin's concept of evolution to the industrial era, humans have developed machines to improve productivity and replace manual labor. With the rise of computers and AI, this ambition has extended into the digital realm, where machines now play a significant role in managing and securing data [31]. AI has undeniably enhanced operational efficiency, but its increasing reliance presents some drawbacks. For one, systems powered by AI still require substantial oversight, updates, and ethical governance. Since these systems operate based on algorithms and historical data, they can become vulnerable if attackers learn to manipulate these models.

Moreover, modern computer technologies now support essential infrastructures such as finance, healthcare, and national defense. This interdependence creates a single point of failure: a sophisticated breach or AI system manipulation could result in catastrophic consequences. Therefore, while AI strengthens digital defenses, it also demands stronger fail-safes and backup protocols to mitigate its potential failures [31]. One of the critical ways cyber security has attempted to overcome vulnerabilities is through data encryption. Encryption ensures that even if data is intercepted, unauthorized users cannot decipher it without the appropriate decryption key. As the demand for secure communication and transactions has grown, encryption standards have evolved significantly [32]. However, attackers have also become more adept at deciphering these methods, requiring ongoing advancement in encryption techniques [33]. AI can assist in this by identifying encryption weaknesses or anomalies, but integrating AI with advanced encryption protocols remains technically and ethically complex. In addition, businesses often face barriers in leveraging AI fully, particularly concerning data privacy regulations and the computational costs involved. In this *Figure* show the role of data encryption and organizational barriers in limiting the universal adoption of AI for resolving cyber security threats and enhancing business value.

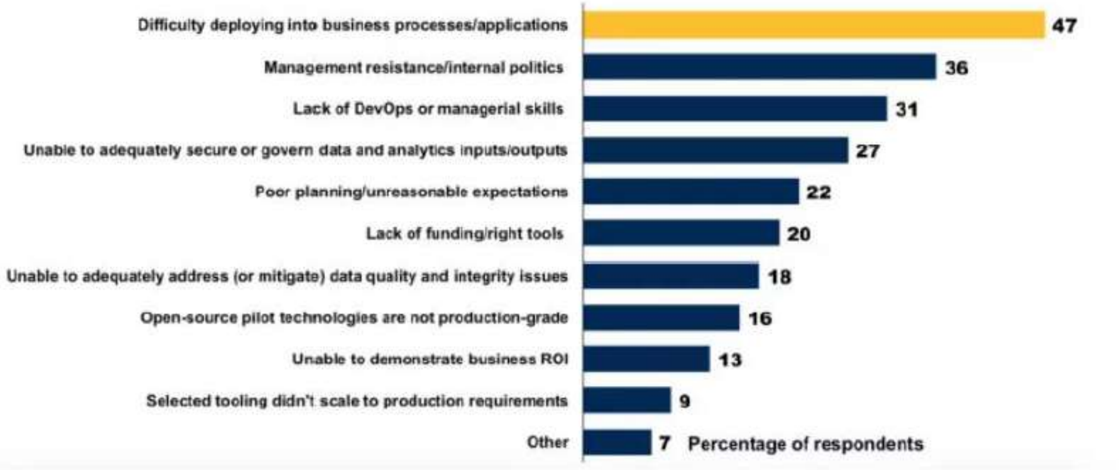


Fig. Barriers to implementing AI against cyber threats on delivering business value

Encryption and Security Limitations of AI in Cyber security

As data breaches become more common, the demand for advanced data encryption protocols has increased dramatically. With sensitive information often described as being “in hot soup” due to its vulnerability [34], computer scientists have responded by designing more complex methods of data encryption. The goal has consistently been to secure information and prevent unauthorized access. Given that machines can outperform humans in tasks they are programmed for, it is logical that AI would excel in implementing and managing these security protocols [35]. AI systems have significantly enhanced data security by automating encryption processes, optimizing protection mechanisms, and responding to threats in real time. By integrating multiple encryption strategies, AI can generate unique and complex protocols that are difficult to decrypt without authorized access. This advancement has been particularly beneficial for large organizations and network providers, where the scale and speed of data processing demand robust security solutions.

However, while AI provides many advantages, its origins as human-developed software expose it to inherent vulnerabilities. Since humans created AI, they also possess the potential to reverse engineer it, understand its architecture, and manipulate it for malicious purposes [35]. Even though AI can be self-learning and adaptive, its core remains programmable, and with minimal code alterations, it could be transformed from a security tool into a cyber-weapon. This susceptibility highlights a major limitation of AI: it is ultimately a product of its programming. Any entity with the right expertise could exploit or reprogram an AI system, using it against the very networks it was designed to protect [26]. This dual-use risk necessitates greater caution from developers and cyber security professionals. While AI is proficient at detecting threats and malware, it still requires human oversight. AI systems may fail to identify sophisticated or subtle attacks, especially when malicious content closely resembles legitimate activity. Additionally, as cyber threats evolve, so must AI models. This constant race demands continuous training and updating of AI systems, without which they may become ineffective [9]. Another critical concern is the potential for AI to be used not only defensively but offensively. Malicious actors can harness AI to create highly intelligent and adaptive malware. This means AI could be used to develop viruses capable of bypassing traditional security measures, exploiting systems faster than they can be patched. In such scenarios, AI shifts from being a safeguard to a cyber-security threat itself. The complexity of AI technology poses an additional barrier. Its implementation and management require advanced knowledge, limiting access for smaller organizations or those lacking technical expertise. Misuse or misconfiguration of AI systems could create vulnerabilities instead of closing them. Moreover, the cost of AI adoption is significant [34]. High development, integration, and maintenance expenses restrict its use to well-funded entities, leaving smaller institutions exposed to cyber risks they cannot afford to counter with AI solutions.

Conclusion

AI has brought transformative benefits to cyber security, offering increased detection speed, data analysis capability, and automated defense mechanisms. However, its limitations must not be overlooked. From being vulnerable to manipulation, to requiring constant updates, high implementation costs, and human oversight, AI is not a flawless solution. Nonetheless, the overall impact of AI on cyber security remains overwhelmingly positive. While challenges exist, they can be mitigated through responsible development, ethical governance, and continuous innovation. Moving forward, it is imperative for researchers, developers, and organizations to focus on reinforcing AI systems against misuse, lowering adoption costs, and making them more accessible.

The future of cyber security lies in the synergy between human expertise and artificial intelligence. Strengthening this alliance will ensure more resilient, adaptive, and secure systems, protecting digital infrastructures from an increasingly sophisticated landscape of cyber threats.

REFERENCES

1. Blake, C. (2020). Artificial Intelligence and Advances. Advances In Machine Learning & Artificial Intelligence, 1(1). https://doi.org/10.33140/amlai.01.01.03
2. Dash, B., & Sharma, P. (2022). Role of artificial intelligence in smart cities for information gathering and dissemination (a review). Academic Journal of Research and Scientific Publishing, 4(39), 58–75. https://doi.org/10.52132/ajrsp.e.2022.39.4
3. Chen, Z., & Liu, B. (2016). Lifelong Machine Learning. Synthesis Lectures On Artificial Intelligence And Machine Learning, 10(3), 1-145. https://doi.org/10.2200/s00737ed1v01y201610aim033
4. Vorobeychik, Y., & Kantarcioglu, M. (2018). Adversarial Machine Learning. Synthesis Lectures On Artificial Intelligence And Machine Learning, 12(3), 1-169. https://doi.org/10.2200/s00861ed1v01y201806aim039
5. Dilmegani, C. (2022, September 12). AI platforms: Guide to ML Life Cycle Support Tools. AIMultiple. Retrieved September 26, 2022, from https://research.aimultiple.com/ai-platform/
6. Chen, Z., & Liu, B. (2018). Lifelong Machine Learning, Second Edition. Synthesis Lectures On Artificial Intelligence And Machine Learning, 12(3), 1-207. https://doi.org/10.2200/s00832ed1v01y201802aim037
7. Heldah, C. (2021). How Artificial Intelligence (AI) is Transforming Cybersecurity. Plug and Play Tech Center. Retrieved 1 September 2021, from https://www.plugandplaytechcenter.com/resources/how-artificial-intelligencetransforming-cybersecurity/.
8. Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of phishing attacks using AI-based Cybersecurity
9. Awareness Training. International Journal of Smart Sensor and Adhoc Network., 61–72. https://doi.org/10.47893/ijssan.2022.1221
10. Stevens, T. (2020). Knowledge in the grey zone: AI and cybersecurity. Digital War, 1(1-3), 164-170.

11. https://doi.org/10.1057/s42984-020-00007-w
12. Trappe, W., & Straub, J. (2018). Cybersecurity: A New Open Access Journal. Cybersecurity, 1(1), 1.
13. https://doi.org/10.3390/cybersecurity1010001
14. Catherine. (2021). Artificial Intelligence in Cyber Security - Impacts & Advancements. Intellipaat Blog. Retrieved 1 September 2021, from https://intellipaat.com/blog/artificial-intelligence-in-cyber-security/.
15. Stoianov, N., & Ivanov, A. (2020). Public Key Generation Principles Impact Cybersecurity. Information & Security: An International Journal, 47(2), 249-260. https://doi.org/10.11610/isij.4717
16. Vlassis, N. (2007). A Concise Introduction to Multiagent Systems and Distributed Artificial Intelligence. Synthesis Lectures On Artificial Intelligence And Machine Learning, 1(1), 1-71. https://doi.org/10.2200/s00091ed1v01y200705aim002
17. Perols, R., & Murthy, U. (2018). The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3112872
18. Hamilton, W. (2020). Graph Representation Learning. Synthesis Lectures On Artificial Intelligence And Machine Learning, 14(3), 1-159. https://doi.org/10.2200/s01045ed1v01y202009aim046
19. Keen, E. (2021). The benefits and limitations of AI in cybersecurity - Help Net Security. Help Net Security. Retrieved 1 September 2021, from https://www.helpnetsecurity.com/2018/12/20/ai-cybersecurity-benefits-limitations/.
20. Raedt, L., Kersting, K., Natarajan, S., & Poole, D. (2016). Statistical Relational Artificial Intelligence: Logic, Probability, and Computation. Synthesis Lectures On Artificial Intelligence And Machine Learning, 10(2), 1-189.
21. https://doi.org/10.2200/s00692ed1v01y201601aim032
22. Mengidis, N., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2019). Blockchain and AI for the Next Generation Energy Grids: Cybersecurity Challenges and Opportunities. Information & Security: An International Journal, 43(1),21-33. https://doi.org/10.11610/isij.4302
23. Daily, J., & Gardiner, B. (2018). Cybersecurity Considerations for Heavy Vehicle Event Data Recorders. SAE International Journal Of Transportation Cybersecurity And Privacy, 1(2), 113-143. https://doi.org/10.4271/11-01-02-0006
24. Vostoupal, J. (2021). The Cybersecurity Qualifications as the Prerequisite for the Cybersecurity Certification of Entities. Jusletter-IT, (27-Mai-2021). https://doi.org/10.38023/2029e2f5-bd30-4757-aef5-01b27ae61962
25. Vermesan, O., & Bacquest, J. Next Generation Internet of Things.
26. Johnson, R. (2022, July 18). Artificial Intelligence in cybersecurity market size to reach USD 133.8 billion by 2030 driven by growing number of cyber attacks. Yahoo! Finance. Retrieved September 26, 2022, from https://finance.yahoo.com/news/artificial-intelligence-cybersecurity-market-size-070000706.html
27. Rada, R. (2014). Artificial intelligence. Artificial Intelligence, 28(1), 119-121. https://doi.org/10.1016/0004-3702(86)90034-2
28. Kravets, V. (2019). Comparative Analysis of the Cybersecurity Indices and Their Applications. Theoretical And Applied Cybersecurity, 1(1). https://doi.org/10.20535/tacs.2664-29132019.1.169090
29. Chung, S. (2021). AI-Based CYBERSECURITY: Benefits and Limitations. 1-2. https://doi.org/10.22471/ai.2021.6.1.18

30. Computer.org. (2021). The Impact of AI on Cybersecurity | IEEE Computer Society. Computer.org. Retrieved 1 September 2021, from https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity/.
31. Creese, S., Dutton, W., Esteve-Gonzalez, P., & Shillair, R. (2020). Cybersecurity Capacity Building: Cross-National Benefits and International Divides. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3658350
32. Raghavan, V., Venkat N. Gudivada, & Venu Govindaraju. (2016). Cognitive Computing: Theory and Applications. Elsevier Science.
33. Here, P., Look, E., & Data, B. (2021). Impact of AI-Driven Cybersecurity in Fighting Data-Driven Cyberattacks. SmartData Collective. Retrieved 1 September 2021, from https://www.smartdatacollective.com/how-ai-drivencybersecurity- drastically-impacts-our-lives/.
34. upGrad. (2021). Artificial Intelligence in Cyber Security: Role, Impact, Applications & List of Companies | upGrad blog. upGrad blog. Retrieved 1 September 2021, from https://www.upgrad.com/blog/artificial-intelligence-in-cybersecurity/.
35. John, N. (2021). The Impact of AI and Machine Learning on CyberSecurity. Globaltechcouncil.org. Retrieved 1 September 2021, from https://www.globaltechcouncil.org/cyber-security/the-impact-of-ai-and-machine-learningon- cybersecurity/.
36. Dubber, M., Pasquale, F., & Das, S. (2020). The Oxford Handbook of Ethics of AI. Oxford University Press, Incorporated.
37. Thomas, B. (2021). Artificial Intelligence in Cyber Security: Role, Impact, Applications & List of Companies |upGrad blog. upGrad