International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Artificial Intelligence in Cyber Security: Review Paper on Current Challenges Faced by the Industry

Tarun Grover[1], Dr. Harmeet Malhotra[2]

Abstract: ***In the dynamic realm of cyber security, artificial intelligence (AI) has emerged as a potent tool for safeguarding systems and data from ever - evolving threats. The rapid evolution of artificial intelligence (AI) has revolutionized various industries, and cybersecurity is no exception. The ever - evolving landscape of cyber threats necessitates the adoption of sophisticated defense mechanisms. AI's ability to analyse vast amounts of data, identify patterns, and adapt to evolving threats offers immense potential to enhance cybersecurity measures. However, the integration of AI into cybersecurity practices is not without its challenges. This paper provides a concise overview of role of Artificial Intelligence (AI) in cybersecurity, addressing current challenges and proposing future directions for enhancing the effectiveness of AI in protecting digital assets. The paper examines the application of AI in - depth, discusses its pivotal role in cyber security, analyses existing challenges faced by AI - powered cybersecurity systems, and outlines potential future directions for research and development.***

Keywords: Cyber security, Artificial Intelligence, Natural Language Processing, Artificial Intelligence

1. Introduction

In the ever - evolving landscape of cybersecurity, the threat landscape is constantly shifting, with new attack vectors and techniques emerging daily. The sheer volume and complexity of data generated by modern computing systems further complicate the task of securing networks and protecting sensitive information. To combat these challenges, the cybersecurity industry is turning to artificial intelligence (AI) as a powerful tool to enhance threat detection, prevention, and response capabilities. AI encompasses a broad range of technologies, including machine learning (ML), natural language processing (NLP), and deep learning (DL). These technologies enable computers to learn from data, identify patterns, and make predictions without explicit programming. AI algorithms can analyse vast amounts of data, including network traffic, user behavior, and security logs, to identify anomalies and suspicious patterns that may indicate cyberattacks. This ability to analyse large datasets and extract meaningful insights is crucial for detecting threats that would otherwise go unnoticed.

AI - powered systems can proactively block or mitigate attacks by analysing network traffic, user behavior, and other risk indicators. For instance, AI's sharp eye can identify and block suspicious traffic, preventing unauthorized access attempts and skillfully detecting and classifying phishing emails, ensuring system security. In the event of a security breach, AI can assist in incident response by accelerating the investigation and remediation process. AI algorithms can analyse vast amounts of data to identify the root cause of an attack, isolate affected systems, and prioritize remediation efforts. Real - time insights and automated tasks drastically cut response times and minimize breach impact. By leveraging real - time insights and automation, incident response speeds up dramatically, reducing the damage caused by breaches. While AI holds immense promise for revolutionizing cybersecurity, its adoption faces several challenges. One of the primary concerns is data privacy or it is complex and opaque, making it difficult to understand their decision - making processes.

AI is poised to play an increasingly important role in cybersecurity. As AI technologies continue to evolve, their potential to enhance threat detection, prevention, and response capabilities will only grow. By addressing the current challenges of data privacy, explain ability, and adversarial AI attacks, we can harness the power of AI to create a more secure and resilient digital world.

2. Research Methodology

This research adopts a comprehensive methodology, involving a thorough literature review of academic papers, industry reports, and expert opinions. The review focuses on identifying the current applications, challenges, and future directions of cyber security in AI.

In this a comprehensive search of academic databases, including Scopus, Web of Science, and Google Scholar, was conducted to identify relevant academic papers. The search keywords included "artificial intelligence, " "cybersecurity, " "machine learning, " "deep learning, " and "threat detection. "

In addition to peer - reviewed academic papers, the literature review also included industry reports and expert opinions.

3. Literature Review

Industry reports provide valuable insights into the current state of AI adoption in cybersecurity, while expert opinions offer perspectives on the future directions of AI in this domain. Few of them are as:

Federated Learning with Multi - Objective Evolutionary Algorithm for Privacy - Preserving and Communication - Efficient Neural Networks (2020)
It's a multi - objective evolutionary algorithm for designing neural networks for federated learning. Federated learning allows training models on distributed data without revealing the underlying data, protecting privacy. This algorithm optimizes neural network structure to minimize both communication costs and error rates.

Licensed Under Creative Commons Attribution CC BY

Secure Federated Learning with Double - Trapdoor Encryption (2021)
It introduces a secure federated learning approach using double - trapdoor encryption. This scheme utilizes multiple keys and decrypts information in stages, enhancing security. It allows safe training of models across distributed datasets without compromising privacy.

Operating Encrypted Deterministic Finite Automata in the Cloud (2019)
It's a method for operating encrypted deterministic finite automata in the cloud. It allows processing complex Boolean formulas while keeping the data encrypted. This approach integrates data security measures with cloud computing, allowing for secure analysis and confident decision - making.

TrustAccess: A Blockchain - Based Ciphertext - Policy Attribute - Based Encryption Scheme for Secure and Reliable Attribute Hiding Access Control (2020)
This presents TrustAccess, a secure attribute - based encryption scheme for access control. It utilizes blockchain technology to ensure reliable and secure attribute hiding. TrustAccess allows fine - grained access control based on user attributes while maintaining privacy.

RBAC with Two Rules for Secure and Efficient Access Control (2018)
It follows two rules for enhancing the security and efficiency of Role - Based Access Control (RBAC). These rules restrict role - task and permission - task relationships to prevent unauthorized access. They also ensure efficient access control by assigning roles and permissions based on specific tasks

Content Analysis
The collected literature was analysed to identify key themes and patterns. This analysis centered around the extraction of information pertaining to the applications of AI in cybersecurity, the current challenges associated with its adoption, and promising future directions for AI - powered solutions in the cybersecurity domain.

4. Synthesis and Discussion

The findings from the literature review were synthesized to provide a comprehensive overview of AI in cybersecurity. The discussion explores how AI can revolutionize threat detection, prevention, and response across the cybersecurity landscape, but also recognizes the critical challenges that must be overcome for full potentialization.

AI in depth
Artificial intelligence (AI) has been around since the early days of computing. Initially, it was thought that machines could never be as intelligent as humans. However, as AI technology has advanced, machines have been able to beat humans at complex tasks such as chess and Go. This progress is due to three main factors:

- Increased computational power: Computers have become much more powerful in recent years, allowing AI algorithms to process more data and perform more complex calculations.
- Development of powerful search algorithms: AI researchers have developed new search algorithms that allow machines to explore complex problems more efficiently.
- Well - structured knowledge sets: AI algorithms can be trained on large datasets of information, which allows them to learn and perform tasks effectively.

Artificial intelligence (AI) is experiencing widespread adoption across various fields, with cyber defense being no exception. AI - powered systems boast exceptional capabilities in real - time detection and response to cyber threats. Furthermore, their ability to analyze large amounts of data empowers the identification of patterns and trends potentially indicative of cyberattack.

AI's power, however, has its limitations. Susceptibility to attacker manipulation and potential errors necessitate its utilization in conjunction with other security measures like firewalls and intrusion detection systems.

AI Based Threat Detection
In today's digital world, the need to safeguard networks, systems, and data from diverse threats, such as malware, phishing, and ransom ware, has never been more urgent. A promising approach to address these challenges lies in the field of artificial intelligence (AI), which is revolutionizing threat detection and defence in several ways:

1) Proactive Threat Detection
AI's real - time analysis of vast data volumes allows for high - accuracy detection of anomalies and potential threats. One example is its ability to identify suspicious network traffic patterns, such as a spike in connections from a single IP address. . AI can analyse data from IoT devices to detect unusual activity, such as a sudden change in temperature or humidity.

AI can analyse social media feeds to identifying the potential threats, such as mentions of a company's vulnerabilities.

2) Automated Incident Response
AI's ability to automate incident handling minimizes damage and enables swift recovery. AI achieves this by promptly identifying and responding to threats, eliminating the need for human involvement. For instance, AI can automatically quarantine infected devices or roll back changes made by malicious actors. Additionally, it can isolate compromised systems to prevent malware propagation and patch vulnerabilities to hinder attackers' exploitation attempts.

3) Behavioral Analysis and User Monitoring
Leveraging its capacity to learn and analyze user behavior, AI plays a crucial role in deterring insider threats by identifying deviations from established patterns.

This includes detecting unauthorized attempts to access sensitive data, download large data amounts potentially indicative of exfiltration, and access the network from unusual locations or times.

Licensed Under Creative Commons Attribution CC BY

4) Threat Intelligence and Prediction

Utilizing artificial intelligence (AI) to analyze and process threat intelligence data empowers proactive threat prediction and prevention. Through its learning capabilities, AI acquires knowledge of known threats and their patterns, enabling the identification of potential threats that may not be yet recognized. This allows for the anticipation and pre - emption of cyberattacks, enhancing overall cybersecurity posture.

5) Anomaly - Based Intrusion Detection

AI excels at detecting anomalies in system behavior, potentially revealing zero - day attacks. By analyzing and learning normal behavior patterns, AI can identify deviations that signal potential threats. These deviations can include:

Abnormal system behavior: AI can flag activity that deviates from established baselines, suggesting a possible attack.

Communication with unknown servers: AI can identify unexpected communication with unfamiliar or unauthorized servers, indicating potential malicious activity.

Unapproved code execution: AI can detect the execution of unauthorized or unexpected code, often a telltale sign of an attack.

These capabilities allow AI to play a crucial role in proactive threat detection and prevention, especially against zero - day attacks that exploit unknown vulnerabilities

6) Enhanced Phishing Detection

Artificial intelligence (AI) offers a significant advantage in the fight against phishing by utilizing its analytical prowess to examine emails and URLs, effectively distinguishing fraudulent attempts from legitimate communications.

This ability stems from AI's capacity to learn and identify the characteristics of phishing emails and URLs, enabling it to detect suspicious senders, malicious URLs, the presence of phishing - related keywords like "urgent" or "password", and links leading to harmful websites.

Machine Learning and Predictive Analytics:

The evolving landscape of cyber security threats, characterized by increased sophistication and widespread dissemination, poses a significant challenge to security personnel, exceeding their capacity to adequately respond.

An alarming trend of escalating complexity and pervasiveness of cyber threats poses a critical challenge to the capabilities of security personnel, potentially jeopardizing cyber security posture. Traditional defense measures are not always effective, and many detection approaches rely on manual investigation, which can be slow and inaccurate. Machine learning can automate many cybersecurity tasks, such as threat detection, prevention, and response.

Machine learning has the power to revolution the cybersecurity by providing intelligent decision - making that can automatically possess the agility and adaptability to effectively counter evolving threat environments. Machine learning will be used to predict the cyberattacks, identify malicious behaviour, and prevent damage to systems.

Machine learning falls under the umbrella of artificial intelligence (AI). AI is the ability of machines to simulate human intelligence, while machine learning is a method of learning from data to improve performance. Deep learning is a subset of machine learning that uses artificial neural networks to learn from data.

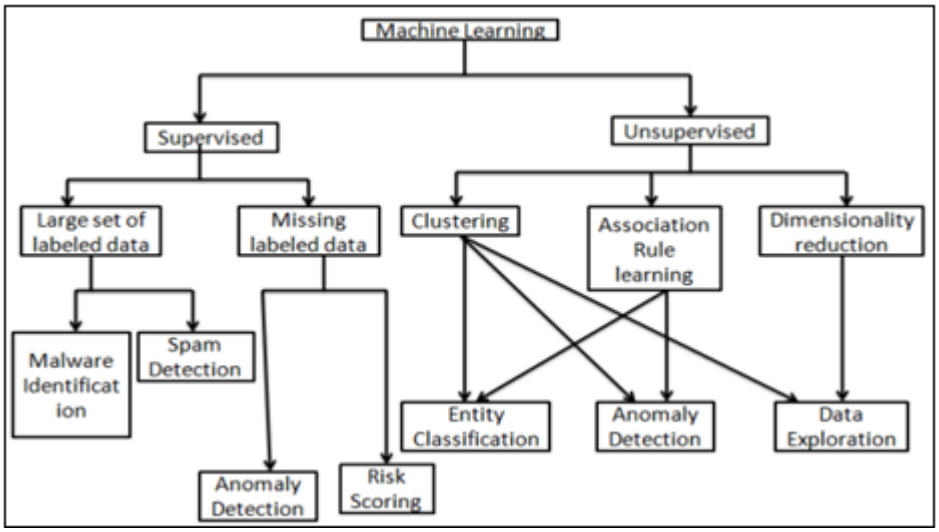
Machine learning techniques can effectively monitor and analyse large amounts of data, including network traffic, emails, and user activity logs. This allows for the detection of anomalies and suspicious patterns, potentially indicative of cyberattacks. By automating this process, machine learning significantly reduces the burden on security personnel, focuses on more complex tasks.

In addition to threat detection, machine learning can also play a crucial role in incident response and vulnerability management. Automating tasks like device quarantine and malicious traffic blocking, machine learning helps organizations minimize cyberattack impact and expedite recovery. Additionally, by utilizing machine learning algorithms, vulnerabilities within systems and software can be prioritized based on their severity and exploitability, enabling proactive patching and mitigating the risk of attacker exploitation.

The integration of machine learning into cybersecurity strategies has proven to be highly effective in combating the evolving threat landscape. By automating routine tasks, enhancing threat detection capabilities, and streamlining incident response, machine learning empowers organizations to protect their valuable assets and maintain a strong cybersecurity posture.

Studies have demonstrated the effectiveness of machine learning in various cybersecurity applications, including intrusion detection, spam filtering, and malware analysis. However, the implementation of machine learning in cybersecurity is not without its challenges. This study delves into the effectiveness and potential drawbacks of machine learning approaches for cybersecurity applications.

Licensed Under Creative Commons Attribution CC BY

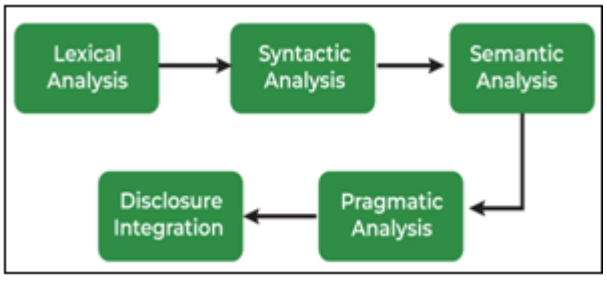


Natural Language Processing (NLP) in Cybersecurity:
Natural Language Processing is a branch of Artificial Intelligence (AI) that integrates the principles and techniques of linguistics, computer science, and AI to enable machines to understand and interpret human language. NLP has traditionally been used to simplify machine - to - human communication, such as chatbots and predictive text. However, NLP is now being applied to cybersecurity to enhance breach protection, identification, and scale and scope analysis.

Phishing Detection
NLP can be used to detect phishing attempts by understanding the bot or spam behavior in email text. It can also be used to identify patterns of spammers and the types of messages they send.

Log Parsi
NLP can be used to parse logs more effectively than traditional rules - based methods. This is because NLP can generalize beyond the logs it was exposed to during training, creating methods to transform raw data into rich content ready for an analyst.

Phases of NLP are as:



NLP is a powerful tool that can be used to improve cybersecurity. By automating tasks, enhancing threat detection capabilities, and streamlining incident response, NLP can help organizations to protect their valuable assets and maintain a strong cybersecurity posture.

Deep Learning in Cyber Security:
Deep learning (DL) is a subset of machine learning that has emerged as a powerful tool for cybersecurity. Deep learning analyzes vast security data to uncover patterns and anomalies suggestive of cyberattacks, leading to improved intrusion detection, malware analysis, and other cybersecurity tasks.

There are three main types of DL algorithms: supervised learning, unsupervised learning, and hybrid learning. Supervised learning algorithms learn from labelled data, while unsupervised learning algorithms learn from unlabelled data. Hybrid learning algorithms combine supervised and unsupervised learning techniques.

DL algorithms have been shown to be more effective than traditional machine learning algorithms for many cybersecurity tasks. This is because DL algorithms can learn more complex patterns from data.

Here are some specific examples of how DL is being can be used for cyber security:

Intrusion detection: DL algorithms can be used to analyse network traffic and identify patterns that may indicate intrusions.

Malware analysis: Deep learning algorithms have emerged as powerful tools for analyzing malware samples and accurately classifying them as benign or malicious. This is achieved by leveraging the algorithms' ability to learn complex patterns and relationships within large datasets of malware and safe software.

Phishing detection: DL algorithms can be used to detect phishing emails and websites.

Botnet detection: Deep learning (DL) algorithms present a valuable tool for the identification of botnets, networks of infected computers susceptible to exploitation for malicious purposes.

Overall, DL possesses significant promise for revolutionizing the area of cybersecurity, and as DL algorithms undergo further development, their role in protecting organizations against cyberattacks is likely to grow increasingly crucial

Licensed Under Creative Commons Attribution CC BY

The Role of AI in Cyber Security

The increasing focus on AI within the computer security community reflects its transformative potential. AI's ability to analyze massive datasets and identify patterns suggestive of cyberattacks allows for real - time threat detection, empowering organizations to prevent breaches and protect sensitive information. Additionally, AI automates routine tasks like security patching and vulnerability scanning, enabling IT personnel to devote their time to complex security challenges and implement advanced solutions, thereby creating a more secure environment.

In addition, Develop new security tools and techniques by the help of AI. The usage of AI facilitates the creation of virtual honeypots, which function as decoys to attract and deceive cybercriminals, thereby enabling the acquisition of valuable information about their methods and activities.

While AI offers promising solutions for cybersecurity, its adoption is not without challenges. One challenge is that AI systems can be complex and opaque, making it difficult to understand how they work. This can make it difficult to trust AI systems and to ensure that they are not making mistakes. Another challenge is that AI systems can be vulnerable to attack. Cybercriminals can exploit vulnerabilities to launch attacks or to manipulate the results of AI - powered security tools.

Implementing artificial intelligence (AI) technologies into existing cybersecurity frameworks requires careful planning, training, and resource allocation. AI has the power to significantly enhance cybersecurity operations by providing features such as:

Precision biometric password authentication: AI is used to develop more secure and user - friendly password authentication methods, such as facial recognition or voice recognition.

Predictive risk analysis: Through the analysis of vast quantities of data, AI algorithms have the capability to identify patterns and anomalies that are indicative of potential cyber attacks. This facilitates proactive threat detection and prevention measures.

Natural language processing (NLP): NLP can be used to improve the effectiveness of cybersecurity tools by enabling them to understand and respond to natural language commands.

Enhanced identity and access management: AI can be used to strengthen identity and access management systems by verifying user identities more accurately and preventing unauthorized access.

However, integrating AI into cybersecurity systems also presents challenges. One of the primary concerns is the cost of AI technologies, which can be prohibitively expensive for some organizations. Additionally, AI systems require extensive training and configuration to be effective, which can be time - consuming and resource - intensive.

Despite these challenges, the potential benefits of AI in cybersecurity are significant. The integration of AI into organizational cybersecurity frameworks allows for the optimization of cyberattack detection and prevention procedures, the bolstering of cyber resilience, and the streamlining of cybersecurity operations. As AI technologies continue to develop and mature, their adoption in cybersecurity is expected to increase.

5. Challenges & Risks

The advancement of AI in cybersecurity brings both immediate and long - term challenges. While AI techniques can be rapidly deployed to address urgent cybersecurity challenges, a smarter approach is required. Current AI applications offer promising solutions, but the ultimate goal is to develop entirely new information processing concepts for future situation management and decision - making. Knowledge management for network centric warfare is a demanding field that requires efficient information management systems to enable superior situational awareness for leaders and policymakers.

Given the potential horizon of AI development, we should not solely rely on Narrow AI for the foreseeable future. Some experts believe that the ultimate goal of AI, artificial general intelligence (AGI), could be achieved by the mid - 21st century. In 2008, the first AGI meeting took place at Memphis University. The Singularity Institute for Artificial Intelligence (SIAI), founded in 2000, warns researchers about the potential risks of increasingly accelerated intelligence growth in machines. This could lead to the Singularity, defined as the point at which machine intelligence surpasses human intelligence. Artificial intelligence is currently the most commonly discussed path to the Singularity, but other breakthroughs in various fields could also contribute to the development of super intelligent machines.

Few current challenges of using artificial intelligence (AI) in cyber security:

Data privacy: AI algorithms rely on large datasets of sensitive information, raising concerns about the potential for misuse and privacy violations. It is crucial to develop robust data governance practices and implement stringent privacy measures to protect user data.

Explainability: AI models can be complex and opaque, making it difficult to understand their decision - making processes. This lack of transparency hinders trust and accountability in AI - powered cybersecurity solutions. Developing more transparent and explainable AI models is essential for building trust and ensuring responsible AI usage.

Adversarial AI: Cyber attackers may exploit vulnerabilities in AI models to launch adversarial attacks, manipulating the models to produce erroneous outputs or bypass security measures. Enhancing the resilience of AI models against adversarial attacks is crucial for ensuring their effectiveness in real - world cyber security scenarios.

Licensed Under Creative Commons Attribution CC BY

Bias: The potential for AI algorithms to replicate biases from their training data poses a significant challenge to the development of fair and equitable cyber security solutions. Implementing effective bias detection and mitigation strategies is essential to address this issue and ensure the responsible use of AI in this domain.

Integration challenges: The integration of artificial intelligence (AI) into existing cybersecurity infrastructure presents significant complexities and necessitates considerable specialized expertise. Organizations need to address issues of compatibility, resource limitations, and the need for ongoing retraining as AI technologies evolve.

Skill shortages: There is a growing demand for cybersecurity professionals with expertise in AI. Organizations need to invest in training and development programs to equip their workforce with the necessary skills to effectively utilize AI in cyber security.

Addressing these challenges is crucial to ensure the responsible and effective utilization of AI in cybersecurity. As AI continues its rapid advancement, its impact on cybersecurity will only grow, shaping a future where AI is the cornerstone of digital protection.

Regulatory and Ethical Considerations

The rapid advancement of cybersecurity technologies and the increasing reliance on digital systems have led to a growing body of cybersecurity regulations. These regulations are designed to protect individuals and organizations from cyberattacks and to ensure that cybersecurity practices are aligned with ethical principles.

Some of the specific cyber security regulations include:

The Data Protection Act, 2022 (DPA): The DPA establishes a comprehensive framework for the protection of personal data in India.

The General Data Protection Regulation (GDPR): The GDPR is a European Union regulation that sets out rules for the processing of personal data. It requires organizations to take appropriate measures to protect personal data from unauthorized access, use, disclosure, alteration, or destruction.

The Health Insurance Portability and Accountability Act (HIPAA): HIPAA is a United States law that sets out rules for the protection of health information. It requires organizations to take appropriate measures to protect health information from unauthorized access, use, disclosure, alteration, or destruction.

The Cyber Security Information Sharing Act (CISA): CISA is a law that encourages the sharing of cybersecurity information between the government and the private sector. It also establishes a voluntary framework for the development and implementation of cyber security standards. There are a number of sector - specific regulations that apply to cyber security, such as the Reserve Bank of India's Guidelines on Information Security for Banks and the Securities and Exchange Board of India's (SEBI) Guidelines on Cyber Security for the Securities Market.

In addition to these specific regulations, there are also a number of general data privacy laws and regulations that apply to cybersecurity. These laws and regulations typically require organizations to collect, use, and disclose personal data in a responsible and ethical manner.

Policy Management and Security Awareness

Strong security policies and robust security awareness programs are key to establishing a culture of security within an organization. This culture goes beyond mere compliance; it fosters a sense of shared responsibility and empowers employees to make informed decisions around cyber Security.

Leadership Commitment: Leaders set the example by actively promoting security through their actions and decisions. They integrate security into business strategies, champion initiatives, and recognize employees who uphold security standards.

Communication and Transparency: Open communication builds trust and ensures everyone understands the organization's security policies and practices. Regular updates, clear explanations, and open dialogue create a culture of awareness and collaboration.

Culture of Reporting: Creating a secure environment means encouraging employees to report potential threats and incidents without fear of repercussions. Building a culture of transparency and trust empowers individuals to contribute to the organization's overall security posture.

Inclusiveness: Security awareness and policy updates must reach all levels of the organization, from entry - level employees to top management. This ensures everyone understands their role in upholding security standards and contributes to a collective responsibility for a secure environment.

6. Conclusion

Artificial intelligence (AI) has emerged as a significant instrument in the battle against the escalating sophistication of cyber threats. AI can analyse vast amounts of data to identify anomalies and suspicious patterns that may indicate cyberattacks. The proactive identification and mitigation of cybersecurity threats are achieved through the analysis of network traffic data, user behavior patterns, and other indicators of potential risk.

Additionally, AI can help in incident response by accelerating the investigation and remediation process.

Despite its immense potential, AI adoption in cybersecurity faces several challenges. One of the primary concerns is data privacy. AI algorithms rely on large datasets, raising concerns about the potential for misuse of sensitive information. Another challenge is explainability. AI models can be complex and opaque, making it difficult to understand their decision - making processes. This lack of transparency can hinder trust and accountability in AI - powered cybersecurity solutions. AI, despite its potential, is not immune to cyberattacks. Cyber attackers may exploit AI

Licensed Under Creative Commons Attribution CC BY

vulnerabilities to launch adversarial attacks, manipulating AI models to produce erroneous outputs or bypass security measures.

Despite these challenges, AI is poised to play an increasingly important role in cybersecurity. As AI technologies continue to evolve, their potential to enhance threat detection, prevention, and response capabilities will only grow. By addressing the current challenges of data privacy, explainability, and adversarial AI attacks, the harnessing of AI's power presents a compelling opportunity to create a more secure and resilient digital landscape.

The power of AI unlocks new avenues for improved cybersecurity. By addressing these challenges of data privacy, explainability, and adversarial AI attacks, AI can help to create a more secure and resilient digital world.

References

[1] Tyugu, E. (2011). Artificial intelligence in cyber defense.2011 3rd International Conference on Cyber Conflict, ICCC 2011 - Proceedings, 95–105.
[2] https: //www.researchgate. net/publication/333477899_Use_of_Artificial_Intelligence_Techniques_Applications_in_Cyber_Defense
[3] Artificial Intelligence for Cyber Security: A Comprehensive Review" by S. Jha and D. S. Upadhyaya
[4] "Machine Learning in Cyber Security: A Survey" by I. Goodfellow, I. Bengio, and Y. Bengio
[5] "Adversarial Machine Learning in Cyber Security" by I. Goodfellow, N. Papernot, Y. Bengio, I. J. Goodfellow, and F. D. dos Santos
[6] "Explainable Artificial Intelligence in Cybersecurity" by L. A. de Moraes, S. A. de Aguiar, and K. M. de Souza
[7] "Human - AI Collaboration in Cybersecurity" by S. J. Hyrum, A. R. Simon, and L. E. Grew (2020)
[8] Communication Systems, pp.1 - 4, 2017. Qiang Liu, Pan Li, Wentao Zhao, Wei Cai, Shui Yu, Victor C. M. Leung, “A Survey on security threats and defensive techniques of machine learning: A data driven view”, IEEE Access, pp.12103 - 12117, 2018.
[9] "The 2023 State of AI in Cybersecurity" by Gartner
[10] "The AI Revolution in Cybersecurity" by McKinsey & Company
[11] "The Future of AI in Cybersecurity" by Forrester Research
[12] "AI's Role in Cybersecurity: A 2023 Update" by PwC
[13] "AI in Cybersecurity: Opportunities and Challenges" by Accenture
[14] "The Future of AI in Cybersecurity" by Andrew Ng, Co - founder of Coursera and Landing AI
[15] "AI and the Future of Cybersecurity" by Marcus Ranum, Chief Security Officer at Tenable Network Security
[16] "AI in Cybersecurity: Opportunities and Challenges" by Brenda Longino, Chief Information Security Officer at Hewlett - Packard
[17] https: //link. springer. com/article/10.1007/s40745 - 022 - 00444 - 2
[18] https: //www.crowdstrike. com/cybersecurity - 101/machine - learning - cybersecurity/
[19] https: //www.kroll. com/en/insights/publications/cyber/case - studies
[20] https: //www.metacompliance. com/blog/policy - management/policy - management

Licensed Under Creative Commons Attribution CC BY