STM JOURNALS

International Journal of
Information Security Engineering

ISSN: 3049-1150
Volume 3, Issue 1, 2025
January–June
DOI (Journal): 10.37591/IJISE

https://journals.stmjournals.com/ijise

Review IJISE

Ramifications of Artificial Intelligence and Cyber Security

V. Basil Hans*

Abstract

Artificial intelligence (AI) has pros and cons for cyber security: AI can improve network security, anti-malware, and fraud detection. AI can simulate cyberattacks, automate responses, and analyse enormous databases. AI-powered phishing and deepfakes are cyber risks. AI can potentially be attacked and become a liability for corporations. AI has transformed cyber security, bringing both new opportunities and challenges. AI-powered tools discover abnormalities faster, automate threat responses, and improve threat detection accuracy. As AI systems improve, fraudsters use them to launch complex attacks like AI-generated phishing schemes, deepfakes, and adaptive malware. Defenders must innovate to outperform hostile actors in this cyber arms race due to AI's dual usage. This article discusses how AI integration in cyber security might minimize or increase cyber threats and the ethical and regulatory frameworks needed to handle this changing situation. AI algorithms can find software trends and spot basic infections and ransomware before they infect computers. AI can boost capabilities and protect data by reviewing articles, news updates, and cyber risk research using natural language processing.

Keywords: Artificial intelligence (AI), cyber security, threat detection, AI-driven attacks, automation, ethics

INTRODUCTION

The biggest concern about artificial intelligence (AI) is its impact on jobs. There are immediate issues with AI where attention is needed. Hackers are becoming more dangerous to enterprises, and perimeter and endpoint security are not enough. We know hackers are good, learning like we are, and not bound by their employers to read hundreds of pages of security policy manuals. The rise of business-critical Internet-based services makes it impossible to raise the drawbridge and trust firewalls and antivirus software, yet the industry does. Better to confront reality. The cyber security function must close the rising gap between its security and criminal threat. The main point is that automation is so crucial that a good model requires artificial intelligence. To prepare for field AI application, an initial state is supplied. Soon, the ramifications stretch beyond AI's necessity. Besides having a huge range of empirical instruments, a successful cyber security model will help the function determine future service developments.

AI solutions may identify shadow data, monitor data access irregularities, and notify cyber security professionals to potential dangers from malicious actors accessing sensitive data, saving time in real-time detection and remediation. Through AI-powered risk analysis, high-fidelity alert summaries and automated responses can speed up investigations and triage by an average of 55%.

AI helps detect threat landscape flaws and defend against cybercriminals. AI models may balance security and user experience by monitoring login attempts, validating people using behavioral data,

***Author for Correspondence**
V. Basil Hans
E-mail: vhans2011@gmail.com

Research Professor, Department of Management & Commerce, Srinivas University, Mangaluru, Karnataka, India

Received Date: October 07, 2024
Accepted Date: January 15, 2025
Published Date: February 12, 2025

Citation: V. Basil Hans. Ramifications of Artificial Intelligence and Cyber Security. International Journal of Information Security Engineering. 2025; 3(1): 40–45p.

simplifying access, and decreasing fraud costs by up to 90%. AI systems also avoid phishing, malware, and other threats, improving security [1].

INTERSECTION OF ARTIFICIAL INTELLIGENCE AND CYBER SECURITY

AI and cyber security are two of the most innovative tech fields. These fields are destined to dominate future national defense procedures. They have both sparked a heated discussion regarding their misuse and altering power relations by its owners in the name of global security. It is intriguing to witness how these wide, qualitative talks affect the study process. We shall cover the intersecting field of these two issues by discussing the technical aspects of how they converge in this paper.

Cyber security defends systems, networks, and programs from cyberattacks. Cyberattacks try to access, alter, or delete sensitive data, take money from users via ransomware, or disrupt company activities. Today, there are more devices than people and attackers are more creative, making cyber security difficult [2].

Cyber security and AI have several interdisciplinary overlaps, according to Li [3]. AI technology like deep learning can be used in cyber security to build smart models for malware categorization, intrusion detection, and threat intelligence sensing. However, cyberattacks will disrupt AI models' sample, learning, and choices. Thus, AI models need cyber security defense and protection systems to defend against adversarial machine learning, safeguard privacy, secure federated learning, etc. The aforementioned two aspects inform our analysis of AI and cyber security. First, we review AI research on cyber assaults, including classical machine learning and deep learning. We then examine AI counterattacks, identify their defenses, and study their properties. We conclude by discussing how to design a secure AI system using encrypted neural networks and secure federated deep learning.

Thakur et al. [4] say cyber security and information security are used interchangeably, but the latter recognizes the involvement of humans in the security process, while the former see this as an additional dimension and a potential target. However, cyber security discussions focus on society's ethics, which is crucial. Many frameworks and models address cyber security. Cyber security, its framework, workforces, and computer data protection are also covered.

Ghelani (2022) [5] states, “Academic and practitioner literature provides a wealth of information security guidance. Most security threat research focuses on technology countermeasures, but deterrence, deception, detection, and reaction are also feasible. This article presents the results of a Korean qualitative study on how organizations secure their information systems. The results demonstrate a strongly established preventative mindset motivated by a desire to assure technology and service availability and a widespread lack of business security understanding. Preventative tactics were also present. The paper proposes research on combining, balancing, and optimizing systems for enterprise-wide strategy deployment. This investigation covered information security and military sources where security strategy is discussed. Nine security strategies exist. A qualitative focus group examines how firms use various security techniques. Eight security administrators discussed their firms' security practices in focus groups. According to the research, many firms avert technology service disruptions. Other methods supported the preventative strategy operationally.”

Cyber security requires AI and machine learning. They enable predicting and preventing new threats. Automatic AI-based tools are already fighting high-level cyberattacks. Such systems began with the next generation. Several systems employ machine learning to predict and prevent cyberattacks. These tools make standard computer security event detection methods less effective and provide less protection than needed. Predefined patterns for detecting security incidents in traditional signature-based access control can only identify a small portion of cyberattacks, leaving a plausible scenario for high impact.

ADVANCED ARTIFICIAL INTELLIGENCE FOR CYBER SECURITY

AI developments from cyber security and the two disciplines' distinct strengths will be explored. Technology like AI and machine learning has changed cyber security from detection to prediction. Compared to humans, AI can detect threats and secure networks. Networks are monitored at a granular level to ensure proper operation. AIOps alerts network operators to behavior changes and provides the required skills to respond to threats. Correlations or causations can also be used to find new escape routes or focus on human verification. AI cyber security uses threat analysis and intelligence, autonomous reaction, and trustworthy alerts. The trustworthy alerts turbocharging teams help them respond faster and make better threat-stopping decisions.

Cyber security is a major social concern in the digital age that requires inventive, cutting-edge solutions. To meet this need, AI has revolutionized cyber security. AI's ability to process and evaluate massive amounts of heterogeneous cyber security data helps it complete important tasks efficiently. Threat identification, asset prioritization, and vulnerability management are conducted faster and more accurately than humans, changing cyber security. This document comprehensively analyzes AI's substantial impact on cyber security and how AI tools augment and often surpass human-mediated procedures. By exploring the complexity of AI implementation in cyber security, we show that AI can foresee, identify, and preempt cyber dangers, enabling enterprises to take a proactive approach to digital safety. Despite these advances, AI's limits must be considered. To achieve proportionate and effective cyber security, we emphasize ongoing human oversight and action. We address ethical issues and stress the importance of strong governance mechanisms for responsible and transparent cyber security using artificial intelligence. This study explains how AI is changing cyber security techniques, making the digital future safer. It lays the framework for ongoing research and discussion on AI in cyber security, which is becoming increasingly crucial as we progress deeper into the digital age [6].

With faster processing power and danger prediction, AI and machine learning are giving companies and governments a competitive edge. Defense using AI lets firms improve, modify, and implement security measures using prediction data. Machine learning helps firms identify current and future threats so they can make smart improvements. Cloud technology has enabled hundreds of open-source algorithms and access to innovative solution specialists for machine learning. It provides dense Ethernet cables for ultra-high-speed networks and supercomputers that are unattainable locally. Threat intelligence, threat analytics, vulnerability management, and security awareness initiatives are finally supported by these technologies. Knowing things are changing, specific upgrades, and where teams need to adapt might help.

CHALLENGES AND ETHICS

The rapid development of machine learning and 'deep learning' tools for cyber security and cyber defense has raised many critical issues that must be addressed to promote their responsible use by those who benefit from them and those who may be harmed by their misuse. These topics explore artificial intelligence ethics, however few outcomes are unique to AI in cyber security operations. To yet, none have been solely based on thorough scientific studies based on field experience. Cyber security applications are also suitable for debate.

Nair et al. [7] argue AI has modernized and increased productivity in industries and society. The internet of things (IoT) lets us perceive and transport data between devices and perform activities quickly. AI is now used in numerous fields, from agriculture to weather prediction. AI can help improve soil quality, crop growing, crop cutting, and weather forecast, decreasing causalities. Note that IoT/smart devices benefit more from AI. IoT reduces cyberattacks and vulnerabilities in various areas worldwide, which addresses system failure prevention, detection, and recovery. Cyberattacks must be identified immediately, yet trained professionals require a long time to track and recover. We expect that AI will assist professionals track cyberattacks and avoid large losses in the near future. Identifying spam, trash, etc. is machine learning. Because every industry/business needs cyber security, especially

crucial ones like healthcare, cyber security is essential. We hope to mitigate such assaults or weaknesses on public networks/infrastructure using artificial intelligence. We examine AI's strengths, drawbacks, and future uses in intrusion/vulnerability detection.

According to Chaudhary et al. [8], cyber security utilizing AI can improve security but also open the door to new attacks on AI. Machine Learning algorithms can detect zero-day attacks and unexpected system behavior that may suggest an attack or infection. This research examined security risks, defense methods, and cyber security issues for intrusion detection, malware detection, and network anomaly detection utilizing machine learning and deep learning algorithms. The majority of approaches used supervised models. The maximum accuracy for intrusion detection was 99.90% with RBF-SVM (radial basis function–support vector machine), while malware detection was 97.79% with deep neural network (DNN). DNN models identified pirated software with 96% accuracy. Network anomaly detection was better with Seq2Seq (Sequence-to-Sequence) model at 99.90%. DBN (deep belief network) models detect anomalies with 69.77% accuracy. This study concludes by discussing 5G security, cyberattacks, and the critical significance of the above growing sectors in cyber security.

The AI security sector has evolved and grown. The annual revenue will rise to about $100 billion by 2025. Depending on the AI architecture, cyber security controls for deep learning must be implemented. AI advancement in cyber security creates ethical and moral issues. Controlling model formation and development is critical if threat actors can exploit automated learning AI to create biased and incorrect models that can give malevolent advice. Due to this technology, cyber security risks such AI vulnerabilities, hackers' deceptive instructions to launch cyber assaults, and automated attacks must be reduced. Companies need preparation and incident response to combat AI misuse. The issue is about making the correct choices to protect yourself and do the right thing.

FUTURE TRENDS AND ADVICE

AI will continue to impact cyber security and the public realm. AI will organize data to disclose context, meaning, and value and guide decisions as data quantity and quality rise. To fundamentally modify behavior, education must emphasize the dangers of reckless behavior and be backed by consequences. AI-powered software must be transparent, explainable, and trustworthy to promote accountability and build confidence. Beyond that, AI will be used for personalized propaganda, fake news, misinformation, distributed manipulation, skewed search ranks, weaponized social influence, and other tools that could kill people and devastate communities beyond emotional pain. Technology, business, politics, government, and education must work together to combat these trends. Business and regulatory laws must hold corporations accountable for data damage and control large-scale AI products that influence public opinion. National security posture should rely more on analytics, explanation systems, and multi-organizational and international collaboration than secrecy and the military complex. AI will eventually become a helpful, leading, and rational instrument to prevent and reduce damage. It will combine logic, explanation, and interaction well.

As we pursue AI in cyber security, opportunities and threats increase. AI will be crucial in cyber security as it examines big data volumes and detects new attack fronts [9].

ARTIFICIAL INTELLIGENCE IN INDIA

India has achieved significant AI advances, especially in startups. Its research positioning could be improved by addressing previously mentioned issues. The findings illuminate India's AI environment. Though progress has been made, education, infrastructure, and legislation still need improvement to support future growth. By solving these issues, India could benefit economically from AI. This is a theoretical discussion, not research. Any significant "Results and Discussion" section must be based on carefully collected and examined data. In conclusion, India is at a vital technological juncture, seeking to use AI's transformative potential to serve its vast and diverse population. This study revealed the country's complex and diverse artificial intelligence landscape, including its opportunities and challenges. The burgeoning AI startup ecosystem and significant investments from local and foreign

entities bode well for AI in India. As shown by its AI research and innovative startups, the country can become a global leader in AI. However, the expedition faces challenges. Educational accomplishment infrastructure readiness and regulatory structures were found to be lacking. The focused spread of AI in urban areas, while helpful for cities, may increase the divide between urban and rural areas, leaving a large percentage of the population without AI benefits. While India has a large talent pool and a strong legacy in mathematics and technology, it must adapt its educational system to meet the rapidly growing AI industry needs. Infrastructure issues, especially outside major cities, may limit grassroots inventions and research. A strong, adaptable, and flexible regulatory structure is needed to ensure that AI proliferation follows ethical principles, promotes diversity, and corresponds with national socio-cultural norms. India's socioeconomic landscape can be transformed by AI. However, a thorough and multidimensional plan is needed to maximize AI's potential and distribute its benefits. India can develop a future where AI offers progress and wealth to everyone while being globally competitive and locally relevant by investing in education, infrastructure, and governance [10].

CONCLUSION

AI in cyber security both benefits and drawbacks. On one side, AI-powered systems can detect and respond to cyber threats in real time, providing a proactive protection against emerging cyberattacks. Unlike traditional methods, machine learning algorithms are capable of identifying anomalies, forecasting breaches, and mitigating risks. This has changed cyber security techniques from reactive to proactive, making systems more resilient.

However, AI creates new weaknesses. Cybercriminals can use AI to create more complex phishing, malware, and deepfakes. If not adequately educated, maintained, or managed, AI systems used for essential security functions pose hazards. The threat of adversarial assaults, where hackers persuade AI models to behave unintentionally, is growing.

AI's privacy and data security effects must also be considered. AI systems rely on vast amounts of data, which may lead to privacy concerns and the potential misuse of sensitive information.

In conclusion, AI has immense potential to improve cyber security, but it also poses complicated threats that must be addressed. The future of cyber security depends on balancing AI defense with risk mitigation. A secure digital future requires strong governance, ethical considerations, and AI and cyber security innovation.

REFERENCES

1. IBM. Artificial Intelligence (AI) Solutions. [Online]. Ibm.com. 2024. Available at https://www.ibm.com/artificial-intelligence?utm_content=SRCWW&p1=Search&p4=43700077827237093&p5=p&p9=58700008530962751&gad_source=1&gclid=Cj0KCQiAy8K8BhCZARIsAKJ8sfS_cicDte_OeloA-K7ABS75t4yF3ZqPLAc2MAfD77qZx9KbWqLno2MaArlmEALw_wcB&gclsrc=aw.ds
2. Cisco. Cloud Security. [Online]. Cisco. 2024. Available at https://www.cisco.com/c/en_in/products/security/what-is-cybersecurity.html
3. Li JH. Cyber security meets artificial intelligence: a survey. Front Inform Technol Electron Eng. 2018; 19 (12): 1462–1474.
4. Thakur K, Qiu M, Gai K, Ali ML. An investigation on cyber security threats and security models. In: 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, USA, November 3–5, 2015. pp. 307–311.
5. Ghelani D. Cyber security, cyber threats, implications and future perspectives: a review. Authorea Preprints. September 22, 2022. Available From: https://www.authorea.com/users/506161/articles/587239-cyber-security-cyber-threats-implications-and-future-perspectives-a-review
6. Kumar S, Gupta U, Singh AK, Singh AK. Artificial intelligence: revolutionizing cyber security in the digital era. J Computers Mech Manage. 2023; 2 (3): 31–42.

7. Nair MM, Deshmukh A, Tyagi AK. Artificial intelligence for cyber security: current trends and future challenges. Automat Secure Comput Next-Gen Syst. 2024; May 3: 83–114.
8. Chaudhary H, Detroja A, Prajapati P, Shah P. A review of various challenges in cybersecurity using artificial intelligence. In: 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Toothukudi, India, December 3–5, 2020. pp. 829–836.
9. Morel B. Artificial intelligence and the future of cybersecurity. In: Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence, Chicago, IL, USA, October 21, 2011. pp. 93–98.
10. Hans V. B. An examination of artificial intelligence in India. Int J Enhanced Res Manage Computer Appl. 2023; 12 (10): 1–7.

