



# The Role of Artificial Intelligence in Modern Cyber Security: Challenges and Future Prospects

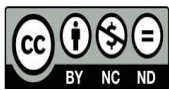
Sufyan Salim Mahmood AL-Dabbagh<sup>1\*</sup>, Sura Sabah Ibrahim<sup>2</sup>, Alyaa Ghanim Sulaiman<sup>3</sup>, Mustafa Ali Abuzaraida<sup>4</sup>

<sup>1,2</sup>Department of Cyber Security, College of Computer Science and Mathematics, University of Mosul Mosul, Iraq.

<sup>3</sup>Department of Software, College of Computer Science and Mathematics, University of Mosul Mosul, Iraq.

<sup>4</sup>Libyan Authority for Scientific Research, Tripoli, Libya.

**To Cite this Article:** Sufyan Salim Mahmood AL-Dabbagh<sup>1\*</sup>, Sura Sabah Ibrahim<sup>2</sup>, Alyaa Ghanim Sulaiman<sup>3</sup>, Mustafa Ali Abuzaraida<sup>4</sup>, "The Role of Artificial Intelligence in Modern Cyber Security: Challenges and Future Prospects", Indian Journal of Computer Science and Technology, Volume 05, Issue 03 (September-December 2026), PP: 08-11.



Copyright: ©2026 This is an open access journal, and articles are distributed under the terms of the [Creative Commons Attribution License](#); Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

**Abstract:** The pace at which digitization is increasing in today's world has also raised the level of cyber threat intensity in terms of size as well as complexity. While traditional approaches to cybersecurity continue to hold equal importance, they appear to be less efficient in dealing with complex approaches to cyber-attacks in the present scenario. Artificial Intelligence (AI) has turned out to be a revolutionary trend in cybersecurity, which is able to efficiently identify cyber-threats, create predictive systems for defensive purposes, as well as deal with cyber-attacks in an adaptive manner, apart from a range of other capabilities. In this research paper, Artificial Intelligence as a trend in present-day cybersecurity, challenges in AI, as well as opportunities in the future for AI in cybersecurity, shall also be discussed.

**Key Word:** cyber security, AI, IDS.

## I. INTRODUCTION

The 21st century has also observed a level of connectivity in the cyber world that is unprecedented in itself, as it is primarily marked by billions of devices being connected to Internet of Things, clouds, as well as 5G networks, even as this connectivity, apart from innumerable benefits of efficiencies, innovations, etc., also marks an undefined threat level to cyber criminals in itself [1].

Artificial Intelligence is noticed to be a very useful resource in dealing with such cybersecurity problems. Having capabilities to process large quantities of data, identify anomalies, as well as learn from an ever-changing environment, Artificial Intelligence is known to be a dynamic, response-based solution for cybersecurity problems [2]. Machine Learning, Deep Learning, as well as Natural Language Processing methods, have also been increasing in their use in cybersecurity applications in order to identify malicious activities, in addition to dealing with them automatically [3].

However, what is important to highlight is that in spite of such immense potential for transformation, it is also imperative to discuss another set of risks/challenges pertaining to this latest advancement in computer science, which is AI itself in this case. Data bias, adversarial attacks, interpretability, as well as dual use of AI technologies, have produced complex challenges for those engaged in this domain of science as well as for practitioners [3]. This paper shall endeavor to discuss how AI is also a potential source of cyber-security risk, as well as serving as a protective mechanism against it.

## II. ARTIFICIAL INTELLIGENCE IN CYBERSECURITY APPLICATIONS

AI is a critical part of different industries in cyber operation cases. Mentioned below are a few of them in the following subsections [4], [5], [6], [7]:

### A. Threat Detection and Anomaly Identification

The machine learning algorithms function effectively in identifying malicious patterns as well as malicious actions of users in a computer network. Unlike previous systems, machine learning algorithms possess capabilities in identifying unknown malicious patterns, which include zero-day attacks as well as malicious polymorphic malware patterns. The clustering algorithms, as well as deep learning, function effectively in real-time detection, as well as adapting to new data sets.

### B. Intrusion Detection and Prevention Systems

Artificial intelligence-based IDPS systems utilize both supervised as well as unsupervised learning processes to analyze system processes, identify intrusions, as well as protect systems from unauthorized access. These systems learn from data present in computer networks, resulting in minimized false alarms, as well as increased detection capabilities of potential threats.

### C. Phishing and Fraud Detection

Natural Processing of Language (NLP) algorithms have also increasingly been used for testing texts, emails, as well as

URLs for phishing attacks as well as social engineering attacks. Artificial intelligence is also applied in systems that detect unusual transaction patterns, which outline cyber-related fraud in the financial industry.

### D. Automation of Security Orchestration

Artificial intelligence technologies aid in automating incident response in Security Operation Centers (SOCs). Artificial intelligence also helps in prioritizing actions for response as well as response actions, which is efficient in securing threats as it reduces work for analysts. Platforms for Security Orchestration, Automation, and Response (SOAR) combine multiple modules of artificial intelligence for this purpose.

### E. Predictive Threat Intelligence

Predictive analytics leverages past threat intelligence to give projections of future attacks. Artificial intelligence systems have the capability to review threat feeds, Dark-Web postings, as well as open-source intelligence to give predictive analysis of potential attack vectors, thus presenting an opportunity for proactive defensive measures to be taken.

### F. Enhancing Zero Trust and Cloud Security

Artificial intelligence systems also facilitate having a Zero Trust infrastructure by checking the credentials of individuals as well as devices for integrity at all times. Artificial intelligence systems also facilitate access control, vulnerabilities, as well as anomaly detection in a cloud infrastructure.

Fig. 1 summarizes these points in visual style.



Fig. 1 AI in Cybersecurity Applications (Generated by Gmini).

## III. CHALLENGES OF USING AI IN CYBERSECURITY

Although it has many benefits, several challenges also exist in applying AI for cybersecurity purposes. These challenges include the following categories [6], [8], [9]:

### A. Data Availability and Quality

However, at present, machine learning algorithms require data of high quality for efficient functioning, even if finding different types of cybersecurity data is quite challenging owing to data sensitivity in regard to cyber-attacks. In this case, poor data quality may result in poor models as well as high false positives.

### B. Adversarial Machine Learning

Machine learning is a field of vast potential, but potential, human learning is another. Nowadays, cyber attackers have also attacked AI models as part of a regular process. Adversarial techniques have been employed by them to train data so that they could manipulate AI models, for example, by creating malware that is close to real applications.

### C. Lack of Explain Ability

A lot of types of AIs, for example, deep learning AI, tend to be "black box" systems which aren't interpretable either. In cybersecurity, having an understanding of how an AI system makes decisions to determine which malicious activity is malicious is of paramount importance.

#### D. Ethical & Privacy Issues

Artificial intelligence systems deal mostly with confidential information. Additionally, even in cases where they are not protected, they generally compromise confidentiality most of the time because they mishandle people's information. Moreover, they also discriminate based on data bias.

#### E. Skills & Integration Gap

There is also the need for qualified staff in implementing AI-assisted cybersecurity systems, who should understand AI as well as cybersecurity topics. The limitation of qualified personnel is a significant hindrance in this case. The integration of AI in legacy systems is characterized by complexity as well as costs.

#### F. Resource Demand & Resource Demand

The training, as well as the infrastructure costs, of the models may also prove to be costly, especially for small organizations. Furthermore, for AI models, regular checkups are needed in order to prevent what is referred to as model drift. Fig.2 illustrates these points in visual style.



Fig. 1 Some Challenges in applying AI for cybersecurity purposes (Generated by Gmini).

### IV.CASE STUDIES AND REAL-WORLD IMPLEMENTATIONS

Some of the organizations that have incorporated AI into cybersecurity tools include [10]:

- IBM Watson for Cyber Security utilizes cognitive computing to analyze threat feeds as well as cyber security blogs to provide insights to cyber security experts.
- Darktrace Enterprise Immune System employs unsupervised learning features to detect insider threats as well as unusual events in cyber environments.
- Google's Chronicle solution utilizes Artificial Intelligence in scanning for large-scale threats in international infrastructure systems.

These examples highlight potential benefits in detection as well as in response times, but they also present challenges in maintaining awareness of context in order to avoid false alarms.

### V.FUTURE PROSPECTS OF AI IN CYBERSECURITY

The future of AI in cybersecurity is promising but complex. Key research and development directions include [10]:

#### A. Neuro-Symbolic and Explainable AI

Today, the trend in AI is to combine hybrid models of intelligence, which involve symbolic processing together with neuronal networks in order for computers to reason about relationships between cause-and-effect.

#### B. Autonomous Security Operations Centers

A fully automated SOC, which is capable of real-time detection, analysis, and response to attacks, is in development stages. Technologies for reinforcement learning, multi-agent systems, and coordination would be an integral part of this development process.

### C. Integration of Quantum and Post-Quantum Security

Applications in the field of artificial intelligence might include algorithm development in a world of post-quantum computers, as well as methods to find quantum computer-based attacks.

### D. AI in Offensive Cyber Operations

While being quite disputable from an ethical point of view, employing AI in cyber-attacks, for instance, in searching for vulnerabilities in an adversary's systems, is of interest to several nation-states as well.

### E. Governance & Regulation of AI in Security

The future framework must include responsible usage of Artificial Intelligence, which involves transparency, accountability, as well as compliance with data protection regulations, including GDPR and AI Act regulations. Ethical standards would also play a critical part in instilling trust in AI-based defensive systems.

## VI.DISCUSSION

The integration of AI in cyber protection systems marks the beginning of a paradigm shift from reactive to proactive systems. Though completely dependent upon automatic systems, however, complacency as well as vulnerabilities in critical systems might be a possibility. That is, human intervention is an imperative in understanding the result of AI as well as understanding complex scenarios, which otherwise would remain unclear to AI systems. Furthermore, it is even more imperative to have collective efforts between people who deal in Artificial Intelligence, cybersecurity experts, ethicists, as well as policymakers. This is because this collective effort is going to result in much better standards of AI audits, bias, as well as explainability.

## VII.CONCLUSION

Artificial Intelligence is changing the paradigms of cybersecurity by providing intelligent, scalable, as well as adaptive defensive systems to deal with cyber-attacks effectively. Even if taking into consideration issues in relation to adversarial samples, ethics, as well as usability, it would be difficult to overlook the advantages of combining Artificial Intelligence in cybersecurity systems. As the level of complexity of cyber-attacks keeps increasing day by day, technologies related to Explainable Artificial Intelligence, Neuro-symbolic Reasoning, as well as Ethical Governance have immense potential in developing a stable cyber world in the coming future. The future of Artificial Intelligence in cybersecurity is full of challenges, opportunities, as well as promises, which require innovations, awareness, as well as collective actions from people around the globe.

## REFERENCES

1. S. N. Vulpe, R. Rughiniş, D. Ţurcanu, and D. Rosner, "AI and cybersecurity: a risk society perspective," *frontiersin.org*, vol. 6, 2024, doi: 10.3389/FCOMP.2024.1462250/FULL.
2. P. Tripathi, "AI and Cybersecurity in 2024: Navigating New Threats and Unseen Opportunities," *International Journal of Computer Trends and Technology*, vol. 72, no. 8, pp. 26–32, Aug. 2024, doi: 10.14445/22312803/IJCTT-V72I8P105.
3. A. Habbal, M. K. Ali, and M. A. Abuzaraida, "Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions," *Expert Syst Appl*, vol. 240, Apr. 2024, doi: 10.1016/j.eswa.2023.122442.
4. A. Critch and S. Russell, "TASRA: a Taxonomy and Analysis of Societal-Scale Risks from AI," Jun. 2023, doi: <https://doi.org/10.48550/arXiv.2306.06924>.
5. H. Chaudhary, A. Detroja, P. Prajapati, and P. Shah, "A review of various challenges in cybersecurity using artificial intelligence," *Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020*, pp. 829–836, Dec. 2020, doi: 10.1109/ICISS49785.2020.9316003.
6. P. Pavan Kumar, M. Satish, B. Sunitha Devi, A. Prakash, K. P. Reddy, and S. Malli Babu, "The Future of AI in Predicting Cybersecurity Threats," *Lecture Notes in Electrical Engineering*, vol. 1274 LNEE, pp. 1382–1395, 2025, doi: 10.1007/978-981-97-8043-3\_197.
7. N. Wirkuttis and H. Klein, "Artificial Intelligence in Cybersecurity," *inss.org.il*, vol. 1, no. 1, p. 103, 2017, Accessed: Dec. 20, 2025. [Online]. Available: <https://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/Artificial%20Intelligence%20in%20Cybersecurity.pdf>
8. L. X. Ying, A. H. Mohd Aman, M. S. Jalil, T. Mohd Omar, Z. S. Attarbashi, and M. A. Abuzaraida, "Malaysia Cyber Fraud Prevention Application : Features And Functions," *Asia-Pacific Journal of Information Technology and Multimedia*, vol. 12, no. 02, pp. 312–327, Dec. 2023, doi: 10.17576/apjitm-2023-1202-10.
9. S. N. Vulpe, R. Rughiniş, D. Ţurcanu, and D. Rosner, "AI and cybersecurity: a risk society perspective," *frontiersin.org* SN Vulpe, R Rughiniş, D Ţurcanu, D Rosner *Frontiers in Computer Science*, 2024•frontiersin.org, vol. 6, 2024, doi: 10.3389/FCOMP.2024.1462250/FULL.
10. E. Hashmi, M. M. Yamin, and S. Y. Yayilgan, "Securing tomorrow: a comprehensive survey on the synergy of Artificial Intelligence and information security," *AI and Ethics*, vol. 5, no. 3, pp. 1911–1929, Jun. 2025, doi: 10.1007/s43681-024-00529-z.