Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140
Volume 14 Issue 01, 2025

The Role of Artificial Intelligence in Cyber Security

Noorsaba L. Siddiqui[1], Shivani,V. Bramhankar[2], Surekha V. Poharkar[3], Swati G. Thote[4], Mr. Rupesh Bangre [5]

[1-5]MCA Department Suryodaya College of Engineering & Technology,Nagpur.
noorsabasiddiqui57@gmail.com[1],shivanibramhankar101@gmail.com[2],surekhapoharkar20@gmail.com[3], swatithote59@gmail.com[4],rupesh.rpb@gmail.com[5]

Peer Review Information

Submission: 11 Feb 2025
Revision: 20 Mar 2025
Acceptance: 22 April 2025

Keywords

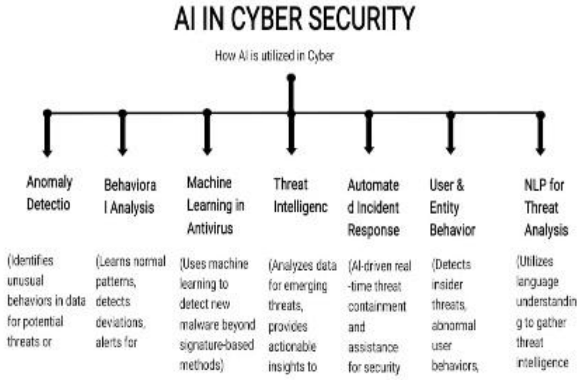
Artificial Intelligence
Cyber security
Machine Learning
Vulnerability Management

Abstract

The advent of advanced cyber-attacks, artificial intelligence (AI) is positioned to transform cyber security. AI in cyber security utilizes intelligent algorithms and machine learning to enhance threat detection, prevention, and response so that systems can process data, identify patterns, and make decisions at volumes and speeds above human capabilities. This paper examines how AI enhances threat detection, incident response automation, and responsive security defence architecture. It examines different types of AI automation techniques, such as intrusion detection systems, malware detection and analysis, vulnerability scanning, and prevention from phishing attacks. These case studies will demonstrate how the integration of AI into cyber security systems is helpful and challenging at the same time. Lastly, the paper tackles serious issues like data bias problems and adversarial Artificial Intelligence, as well as ethical issues, and provides recommendations on how AI can be utilized responsibly in computer system protection.

INTRODUCTION

In the contemporary digital world, cyber security threats are changing at a rate that has never been seen before. Because traditional rule-based security solutions often fail to keep up with the complexity and speed of contemporary attacks, it is imperative to adopt a more proactive and dynamic response. Artificial intelligence (AI) has become a key instrument in this dynamic environment that can transform cyber security practices and improve an organization's overall security posture. Artificial intelligence (AI) in cyber security uses machine learning (ML) methods and clever algorithms to analyse data, spot trends, and perform tasks automatically at a rate and volume significantly higher than that of humans. This facilitates faster incident response, more effective and efficient threat detection, and the development of more robust security architectures. The potential of artificial intelligence (AI) in cyber security is examined in this article, along with its applications in various contexts, disadvantages, and ethical quandaries [1].


AI IN CYBER SECURITY
How AI is utilized in Cyber
Anomaly Detectio
Behaviora l Analysis
Machine Learning in Antivirus
Threat Intelligenc
Automate d Incident Response
User & Entity Behavior
NLP for Threat Analysis
(Identifies unusual behaviors in data for potential threats or
(Learns normal patterns, detects deviations, alerts for
(Uses machine learning to detect new malware beyond signature-based methods)
(Analyzes data for emerging threats, provides actionable insights to
(AI-driven real -time threat containment and assistance for security
(Detects insider threats, abnormal user behaviors,
(Utilizes language understandin g to gather threat intelligence

AI-DRIVEN IMPROVEMENTS IN CYBER SECURITY

Threat Detection:

Traditional signature-based intrusion detection systems (IDS) are usually not effective against zero-day attacks and polymorphic malware. AI-based intrusion detection systems (IDS) utilize machine learning algorithms to detect normal network patterns and find anomalies that could be indicators of malicious behaviour. Through detection of deviations from learned patterns, the systems can identify previously unknown threats and offer a more proactive and robust defence.

For example, network traffic can employ machine learning techniques like clustering and anomaly detection to findoutliers that may lead to a data breach or an attack through DDoS.

Incident Response Automation:

It may require a lot of time and effort to respond manually to security incidents. There are many areas of incident response that can be automated through AI, including: Priority of Alerts: In order to allow security teams to concentrate on the most critical threats, machine learning can analyse security alerts and prioritize them according to their severity and possible impact. Automated Remediation: AI systems can automatically fix vulnerabilities, segregate infected systems, and quarantine malicious traffic, making it possible to keep the attacker off the system for most of the attack duration. Threat Intelligence Enrichment: AI can enrich security alerts by automatically appending contextual data from different threat intelligence feeds, enhancing the visibility of the threat environment for security analysts [2].

AI METHODS IN SPECIAL CYBER SECURITY FUNCTIONS

- **Intrusion Detection Systems (IDS):** Machine learning techniques such as Support Vector Machines (SVM), Random Forests, and Neural Networks are used by AI-driven intrusion detection systems (IDSs) to detect malicious network behavior. To detect anomalies and possible intrusions, they can analyze user behavior, system logs, and network traffic. Problem: Excessive false positives can saturate security staff. False alarms need to be minimized through appropriate algorithm tuning and training.

- **Malware Detection and Analysis:** Through monitoring file behavior and attributes, artificial intelligence (AI) is able to substantially improve malware detection by detecting malicious code. Dynamic analysis may be able to monitor for malware activity in a sandbox environment, while machine learning-based static analysis may detect suspicious patterns in the composition of the code. Large datasets of malware samples, for example, can be employed to train deep learning algorithms to detect emerging threats and their variants.

- **Vulnerability Scanning:** By prioritizing vulnerabilities based on their potential impact and exploitability, AI can automate vulnerability scanning and also make it more accurate. Security teams would be able to focus on patching the most critical systems by employing machine learning to determine which vulnerabilities are most likely to be attacked.

- **Challenge:** It requires ongoing effort and access to reliable threat intelligence to keep vulnerability databases up to date and ensure accurate prediction models [3].

- **Case Studies (Examples - Need to be researched and referenced further):**

Darktrace: Darktrace applies artificial intelligence (AI) to automatically detect and respond to network cyberthreats. Its system learns an organization's normal "pattern of life" and subsequently detects and eliminates non-matching patterns.

Cylance: Cylance extends beyond traditional signature-based solutions by employing AI-driven prevention to predict and stop malware execution.

IBM QRadar Advisor with Watson: This Watson-based tool offers security analysts suggestions and insight for threat analysis and incident response.

The possible advantages of incorporating AI into cyber security systems, including enhanced rates of threat detection, faster incident response times, and less dependence on manual processes, are illustrated by these case studies. They also highlight the importance of meticulous preparation, implementation, and continuous monitoring to ensure that these systems are not only effective but also trustworthy [4].

CHALLENGES AND ETHICAL CONSIDERATIONS

Ai poses some challenges and
ethical concerns even though it has a lot to offer cyber security:

- **Data Bias:** Data is employed for training machine learning algorithms; if the data is prejudiced, the AI system will also be prejudiced. This will result in false threat identification and unjustified repercussions. For example, an AI-powered intrusion detection system that was trained mostly on data about a particular industry or geographic area may be not so effective a t detecting threats in other industries or areas.

- **Adversarial Artificial Intelligence:** Attackers may utilize AI to create advanced attacks that are engineered to bypass detection by AI-driven security systems. Since both the attackers and the defenders are attempting to outsmart each other, this forms an "arms race." For example, adversarial attacks can be employed to alter input data so that AI systems incorrectly label malicious files as benign.

- **Ethical Concerns:** There are a few ethical concerns involved in using AI in cyber security, such as:

- **Privacy:** Since AI systems often gather and process enormous amounts of data, privacy can be a potential issue.

- **Transparency:** AI systems are not transparent and accountable as it becomes hard to understand their decision-making processes.

- **Job Displacement:** AI automation could lead to job loss in the cyber security sector [5].

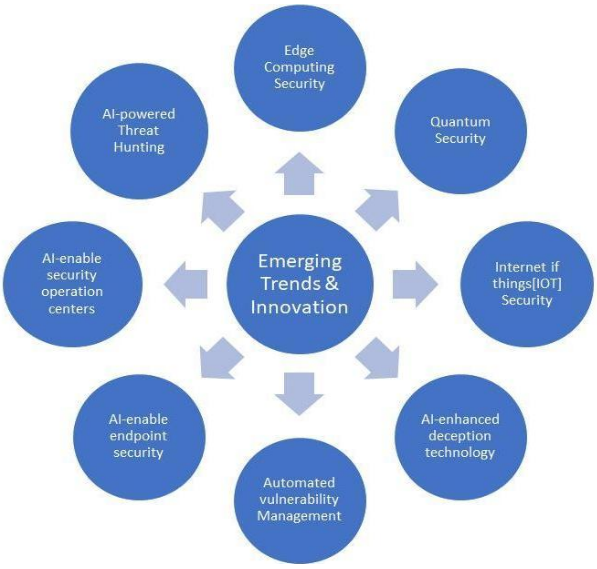
Recommendations for Responsible AI Use in Cyber security

- The following are a few suggestions to make the best out of AI in cyber security and reduce the associated risks and ethical challenges:
- Data Quality and Diversity: In order to minimize bias, utilize high-quality, representative, and diverse training data.
- The aim of explainable AI (XAI) is to maximize transparency and interpretability of AI decision-making through the development and application of XAI methods.
- Adversarial Training: Exposing AI systems to different attack environments can help train them to resist adversarial attacks.
- Human-in-the-Loop Approach: Keep human control over AI systems to enable morally and responsibly sound decision-making.
- Ethical Frameworks and Guidelines: Develop and follow ethical frameworks and guidelines for developing and AI development and implementation for cyber security [6].

FUTURE DIRECTIONS

Future studies need to look into:

- Developing more secure and understandable AI algorithms for cyber security.
- Developing automated methods for the detection and prevention of adversarial AI attacks.
- Developing frameworks and ethical guidelines for AI use in cyber security.
- Drawing on the potential role of AI in new cyber security domains, including cloud and Internet of Things security.
- Examine how the AI is influencing the cyber security profession and determining how to reskill and up skill experts


Edge Computing Security
Quantum Security
Internet if things[IOT] Security
AI-enhanced deception technology
Automated vulnerability Management
AI-enable endpoint security
AI-enable security operation centers
AI-powered Threat Hunting
Emerging Trends & Innovation

CONCLUSION

By improving threat detection, incident response automation, and the creation of dynamic and adaptive security architecture, artificial intelligence can transform cyber security. But to achieve this potential, there is a need for meticulous preparation, implementation, and continuous monitoring. To make sure that AI is utilized reasonably and effectively in computer defence, it is necessary to solve the issues of data bias, malicious AI, and ethics. Organizations can unlock AI's potential to build a safer and more resilient digital future by adopting a holistic strategy that intersects technological innovation with moral reasoning and human expertise [7].

References

Buczak, A. L., & Guven, E. (2016). A survey of machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153-1176. (Good for a broad overview of ML techniques used.)

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, 305-316. (A classic paper highlighting challenges and limitations.)

ENISA Threat Landscape Report. (European Union Agency for Cyber security). (Regularly updated reports that often discuss the role of AI in both attack and defense.) Search the ENSA website.

World Economic Forum. (2023). *The Global Cyber security Outlook 2023*. (Examines cyber security trends and the impact of emerging technologies, including AI.)

MITRE ATT&CK Framework. (While not specifically about AI, it's a crucial resource for understanding attack tactics and techniques, which AI-powered security tools aim to detect and prevent. Refer to the official MITRE website.)

Various cyber security vendor reports (e.g., CrowdStrike, Palo Alto Networks, FireEye/Mandiant, Microsoft). These companies regularly publish reports on threat intelligence and the use of AI in their products. Search their websites for "threat report" or "cyber security forecast."

Ahmed, M., Nanda, P., Hassan, M., and Islam, R. (2016). Anomaly based intrusion detection system using support vector machine. *2016 International Conference on Information and Communication Technology Research (ICTRC)*, 23-26. (Example of a specific ML technique applied.)