International Journal of Applied Social Science
(An International Double Blind Peer Reviewed / Refereed Research Journal of Social Science)
Volume 12 (7 & 8), July & August (2025) : 568-570
Received : 10.06.2025; Revised : 25.06.2025; Accepted : 10.07.2025

RESEARCH PAPER
ISSN : 2394-1405 (Print)
DOI : https://doi-ds.org/doilink/08.2025-26674144/IJASS/12.7&8/568-570

AI for Cybersecurity: Threat Detection and Prevention

LOKESH SINGH[1] AND RAJESH KUMAR[2]
[1&2]Assistant Professor
Computer Science Department, Global Institute of Information Technology, Greater Noida (U.P.) India

ABSTRACT

Artificial Intelligence (AI) is transforming cybersecurity and establishing both quicker and more accurate mechanism of detecting threats and responding to them in real-time. This study focuses on the use of AI to increase levels of cybersecurity and proves whether the effectiveness of AI-based models is higher than other security measures and whether AI-based solutions can be implemented in a variety of industries. The study using mixed-methods design, such as literature review, case studies, and quantitative examination, proves that the AI-based system produces considerably better results than traditional rule-based systems in terms of threat detection, the prevention of incidents and response. Nevertheless, there is a range of issues, including the complexity of integration, data security, malicious attacks, and ethical issues. Its suggested-steps in enhancing the use of AI in cybersecurity are outlined.

Keywords: Artificial Intelligence (AI); Cybersecurity; Threat Detection; Incident Response; AI Integration Challenges

INTRODUCTION

Digital industries and industries generally have experienced exponential growth in the number of cyber threats, which are not managed by the traditional security systems. Since attackers are using sophisticated methods, the rules-based security techniques find it difficult to keep up. AI can handle large amounts of data, find the patterns and adjust to changing threats, becoming the new foundation of cybersecurity defense approaches. This paper discusses the revolutionary AI power of threat detection and prevention, its applicability over legacy systems, and the user problem of practical and ethical issues the implementation of the AI-based cybersecurity protection.

Review of literature:

- The Role of AI in Detection and Response of Threat: Machine learning (ML), deep learning, and natural language processing (NLP) are the AI-related fields applied by systems to analyze network traffic, user behaviors, and system logs and discover complex threats in real time. With the historical and real-time data, AI models can determine the anomalies and other unknown attack vectors more easily and accurately than the conventional approaches.
- Comparative Effectiveness Traditional cybersecurity uses perfected rules sets and/or recognized malware threat signatures, and therefore is reactive, and less efficient against zero-day exploits and polymorphic malware. Conversely, the AI-based systems are forecast, dynamic, and can automate the incident response scenario, which makes them less prone to breaches and a decreased response time. According to the results of the studies, AI can speed threat detection up to 60 percent and decrease the time of response to the incident to a few seconds instead of hours or days.
- Real Life Implementation: Case studies to note effective AI implementations: Darktrace makes use of unsupervised ML to set up behavioral baselines and recognize deviations to foil

How to cite this Article: Singh, Lokesh and Kumar, Rajesh (2025). AI for Cybersecurity: Threat Detection and Prevention. *Internat. J. Appl. Soc. Sci.,* **12** (7 & 8) : 568-570.

ransomware and insider attacks on the fly.
- Owing to NLP, IBM Watson can process any kind of unstructured security data and automate the threat intelligence that supplements SIEM systems.
- Cylance deploys malware-in-the-wild pre-execution detection based on deep learning to enable industries in critical infrastructure to block zero-day attacks.

Difficulties and constraint:

However, the potential power of AI in the sphere of cybersecurity still has numerous obstacles:
- Superior implementation and upkeep expenditures, particularly on hybrid cloud conditions.
- Challenges to integration of legacy infrastructure and data silos.
- Exposure to adversarial attacks, e.g. data poisoning and data evasion.
- Data use and ethical practices, as well as the idea of using algorithms to discriminate.
- Lack of talent and constant retraining of the models.

METHODOLOGY

Design:

The combination of systematic literature review, case study analysis, and mathematical survey of the information using mixed-methods approach.

Data collection:
- Browsed through more than 9,000 articles (20042025) about AI application in cybersecurity.
- Completed analysis of case studies provided by the top AI cybersecurity providers (Darktrace, IBM Watson, Cylance).
- Conducted a survey of 200 cybersecurity experts in the fields of finance, healthcare and manufacturing.

Analysis:
- o Comparative statistical data and statistics of AI and the conventional security-based measures (detection rates, response times, false positives, breaches mitigation).
- o Thematical study of the issues and the implementation barriers by sectors.

RESULTS AND DISCUSSION

The use of AI in cybersecurity brings standards of detecting and thwarting threats to a much higher level than that of rule-based systems because of the capacity of AI-based systems to adaptively detect anomalies and perform automated operations, which allow them to perform better than rule-based systems in both known and unknown threat situations, further mitigating breach threat and easing capabilities.

Accurate threat detection has positive correlation with the kind of AI algorithms deployed: The deep learning and more sophisticated ML models have superior outcomes over simple ML and rule-based schemes particularly in zero-day threat detection and more complex malware.

Usage of AI in the cyber environment helps decrease an incident response time and vulnerability rates within the systems drastically: Artificial intelligence-based automation decreases the duration of recognition and containment operations by hours, even days to minutes, which decreases the damage effects and enhances

Table 1 :

Metric/Variable	AI-Based Systems (Mean/%)	Traditional Systems (Mean/%)	Notes/Findings
Threat Detection Rate	92%	68%	AI outperforms traditional
Incident Response Time (minutes)	3	120	AI enables real-time response
False Positive Rate	4%	17%	AI reduces alert fatigue
Breach Containment Time (days)	214	322	Faster with AI
Detection of Zero-Day Attacks	85%	40%	AI detects novel threats better
Cost of Implementation (USD, median)	$250,000	$100,000	AI higher upfront, lower long-term
Maintenance Complexity (1-5 scale)	4.2	2.7	AI more complex to maintain
Data Privacy Compliance (1-5 scale)	3.1	4.5	Traditional easier for privacy
Talent Availability (1-5 scale)	2.8	4.1	AI needs more specialized skills
User Satisfaction (1-5 scale)	4.6	3.2	Higher for AI, per survey

resilience.

Yet, the research also demonstrates significant difficulties:

- *Integration and Maintenance*: AI systems are expensive to purchase and maintain with frequent retraining of models as well as management of data quality.
- *Adversarial Threats*: Enemies now tend to attack the AI models directly, and they need to be well guarded against data pollution and model evasion.
- *Privacy and Ethics*: The data volume required by AI creates a concern with data privacy and compliance with regulations and bias in the code.
- *Talent and Culture*: The ability to adopt AI successfully relies on the availability of competent workforce and an ability to adopt automation and constant learning culture in the organization.

Conclusion:

The use of AI is reshaping cybersecurity because it makes it do both things as an adaptive and proactive threat detection and prevention tool. AI systems have a far better speed, accuracy, and reliability rate relative to rule-based systems. Nevertheless, to achieve full potential in cybersecurity, it is essential to overcome technical and organizational barriers as well as ethical challenges related to the use of AI. A blended solution, such as using AI in combination with zero trust and classic controls, is the most efficient solution against emerging risks.

Recommendations:

- *AI Hiring and Education*: Invest in AI education and employee training of cybersecurity digits in AI/ML and practices of innovation and perpetual learning.
- *Implement a Hybrid Security Model*: Introduce AI-enhanced analytics alongside zero trust constructs and conventional controls to achieve end-to-end security.
- *Data Quality and Privacy*: Make Data Quality and Data Privacy a priority to reduce compliance risks by having high quality and diverse datasets and introducing a?privacy-by-design approach.
- *You can also Increase Explainability and Trust*: with explainable AI you can increase explainability, stakeholder acceptance, and regulatory comfort across a wide spectrum of industry use cases.
- *Be prepared to deal with Adversarial AI*: Devise ways to counter the AI specific types of attacks: implement robust model validation and adversarial adversarial testing.
- *Continuous Evaluation and Adaptation*: This involves assessing the performance of the AI system on a regular basis, model upgrading, and the continuous improvement of processes so as to match the changing threat environment.

REFERENCES

Achuthan, K., Ramanathan, S., Srinivas, S. and Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence. *Frontiers in Artificial Intelligence*, **7**, Article 11656524.

BitLyft (2024). The role of AI in modern cybersecurity. Retrieved from https://www.bitlyft.com/resources/the-role-of-ai-in-modern-cybersecurity

Darktrace (2024). Case studies – AI in cyber defense success stories. Retrieved from https://www.umetech.net/blog-posts/successful-implementations-of-ai-in-cyber-defense

Jump Cloud (2025). How effective is AI for cybersecurity teams? 2025 statistics. Retrieved from https://jumpcloud.com/blog/how-effective-is-ai-for-cybersecurity-teams

Okdem, S. and Okdem, S. (2024). Artificial Intelligence in Cybersecurity: A Review and a Case Study. *Applied Sciences*, **14**(22), 10487.

Palo Alto Networks (2020). What are the barriers to AI adoption in cybersecurity? Retrieved from https://www.paloaltonetworks.com/cyberpedia/what-are-barriers-to-ai-adoption-in-cybersecurity

Radiant Security (2025). AI-driven incident response: Definition and components. Retrieved from https://radiantsecurity.ai/learn/ai-incident-response/

Sentinel One (2025). AI threat detection: Leverage AI to detect security threats. Retrieved from https://www.sentinelone.com/cybersecurity-101/data-and-ai/ai-threat-detection/

Zscaler (2025). AI vs. traditional cybersecurity: Which is more effective? Retrieved from https://www.zscaler.com/zpedia/ai-vs-traditional-cybersecurity.

****