IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2025

DOI: 10.17148/IJIREEICE.2025.13914

AI-Powered Cyber Threats Security

Prof. Mr.ArsalanA.Shaikh[1], Miss.Darshali S.Talele[2]

Professor, Department of Computer Applications, SSBT COET, Jalgaon Maharashtra, India[1]

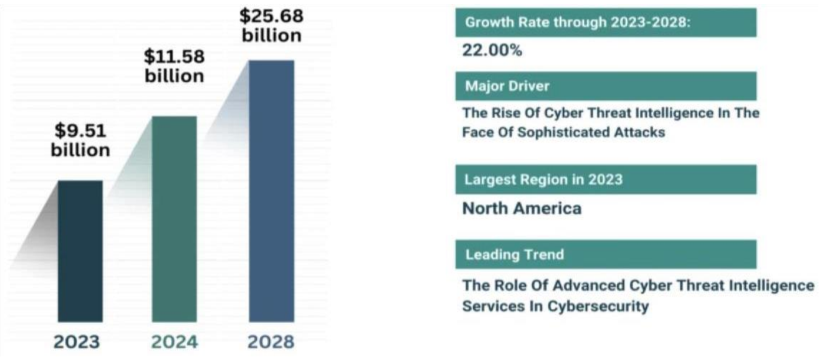
Research Scholar, Department of Computer Applications, SSBT COET, Jalgaon, Maharashtra, India[2]

Abstract: The integration of Artificial Intelligence (AI) across various domains has significantly enhanced productivity and development. However, this advancement has also introduced a surge in cybersecurity threats, particularly those driven by AI itself. These AI-powered threats take advantage of technological advancements to compromise computerized systems, thereby undermining their integrity. This systematic review explores the complexities of AI-driven cyber threats, which utilize sophisticated AI capabilities to execute intricate and deceptive cyberattacks. Our review consolidates existing research to examine the scope, detection methods, impacts, and mitigation strategies associated with AI-induced threats. We emphasize the dynamic relationship between AI development and cybersecurity, stressing the need for advanced protective systems that evolve alongside the growing risks. Our findings highlight the critical role of AI in both facilitating and defending against cybersecurity measures, demonstrating a dual impact that necessitates the continuous evolution of cybersecurity.

I. INTRODUCTION

The rise of artificial intelligence (AI) has brought about significant changes across various industries, boosting productivity and innovation. From healthcare to finance, transportation to retail, AI has drastically improved efficiency and capabilities. However, this digital transformation comes with its own set of challenges. One major concern is the increase in sophisticated cyber threats that exploit AI to breach security systems and compromise data integrity. This highlights the paradox of technological progress, where each advancement can also open doors to new risks.

The cyber threat intelligence market has seen rapid growth, increasing from $9.51 billion in 2023 to an estimated $11.58 billion in 2024, with a compound annual growth rate (CAGR) of 21.7%. This rise is driven by the increase in cyberattacks, malware incidents, surveillance activities, the growing number of connected devices, and the expanding online user base.



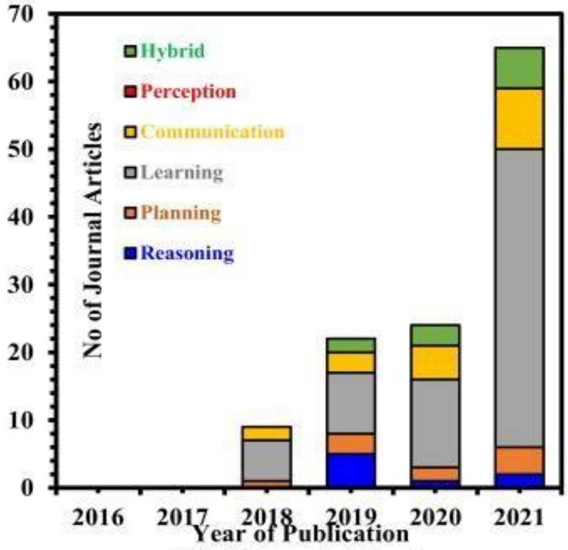
Cybersecurity guided by AI bolsters the monitoring of threats, incident response, and prevention by placing its focus on the patterns and anomalies found in vast amounts of data. AI brings about greater accuracy and speed in adjusting to rapidly evolving threats, exemplified by zero-day attacks. Machine learning models (especially deep learning models like convolutional neural networks and recurrent neural networks) supply the core functions of AI cybersecurity. These models learn from data and can identify complicated patterns that are indicative of cyber threats. AI also automates repetitive tasks, such as log analysis and patch deployment, allowing human analysts to devote time to higher tasks. However, the goal of AI cybersecurity is complicated; adversaries explore AI to perform more advanced attacks, requiring that AI systems continue to evolve and stay ahead of them.

Key AI Techniques Used:-

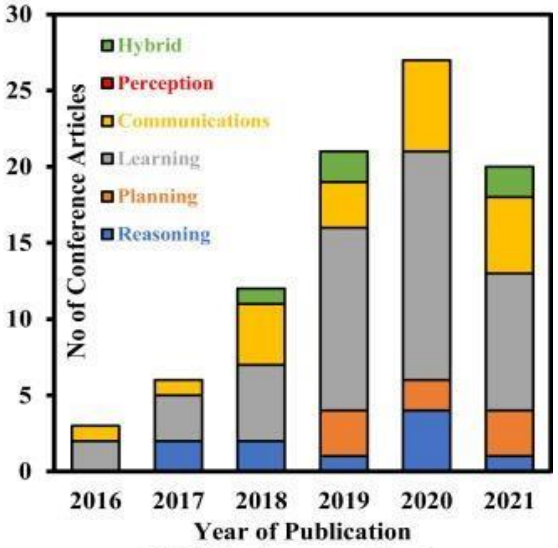
- **Machine Learning:** Machine learning is the most prevalent AI type in the cybersecurity sphere. Machine learning algorithms are able to deduce patterns from historical data and make independent decisions without being explicitly programmed to do so.
- **Deep Learning:** Deep learning is a type of machine learning that uses multi-layer neural networks. It is capable of processing considerably large datasets and discerning complex causal relationships in the datasets to detect sophisticated and advanced cyber threats.
- **Anomaly Detection:** AI establishes baselines of normal user and network activities and subsequently recognizes potential threats when a user or system deviates from this normal baseline of network activity.
- **Behavioral Analysis:** AI provides analysis of user and system behavior and may identify suspicious deviations from an expected behavior sequence. This capability may offer a valuable defensive capability against hands-on keyboard cyberattacks.

The Opposing Nature of AI in Cybersecurity

- **AI-Facilitated Threats:** While AI technology enables better security, attackers leverage the same technology to conduct more complex cyberattacks, targeting vulnerabilities in AI systems and the AI capabilities of the victim.
- **Necessity for Counter-AI:** The vast improvements of an AI-facilitated attack require continuously improved and adaptive AI-based defense techniques and supporting infrastructure.



11(a). Journal publications

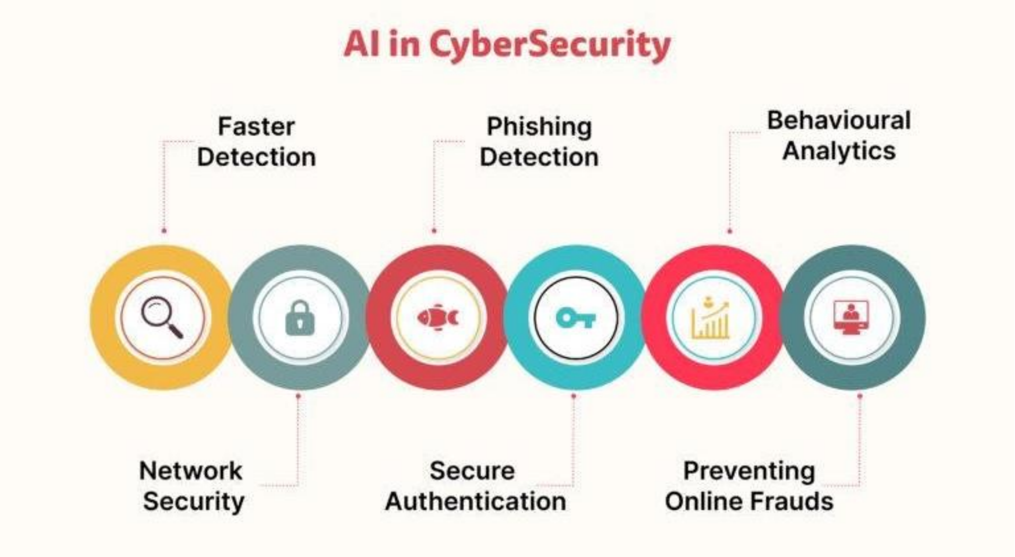


11(b). Conference publications

III. METHODOLOGY

A security methodology for cyber threats that leverages artificial intelligence employs machine learning and data analysis to automate the identification, analysis, and remediation of cyber threats, by way of continuous monitoring of network traffic, user behavior, and systems logs to identify anomalous patterns that may indicate malicious activity. The main components of this AI-centered approach include anomaly detection, behavioral baselining, cyber threat intelligence, and automated defenses to identify, detect, and stop emerging threats faster than traditional, rule-based approaches.

DOI: 10.17148/IJIREEICE.2025.13914



Core Components & Processes

- **Data Analysis & Pattern Recognition:** AI algorithms analyze large data sets from networks, endpoint devices, and user interactions to develop a view of what constitutes "normal" activity.
- **Anomaly Detection:** AI can detect activities that deviate from baseline behaviors, flagging abnormal behavior or activity that could indicate a cyberattack, including those previously unknown.
- **Behavioral Analysis:** AI constantly monitors and detects changes in behaviors, such as unusual data exfiltration or lateral movement across the network of devices, to find attacks that are more advanced.
- **Automated Response**: Once a threat has been detected, the AI systems can automatically perform actions like blocking the malicious files, quarantining the affected devices, or notifying a security team for further investigation.
- **Continuous Learning:** AI models improve through both supervised and unsupervised learning over time to improve how accurately threats are detected, and how quickly they become aware of the new and evolving threats.

Key Techniques & Uses

- **Behavioral Anomaly Detection:** AI monitors user and network behavior to establish a baseline of normality, and recognizes deviations that could be a threat to security or indicate an intrusion.
- **Smart Traffic Analysis:** AI systems leverage the capability to analyze network communications to determine and report suspicious activities or kills that indicate attacks.
- **Defensive Threat Protection:** AI-powered capabilities not only provide detection of threats, but also can actively work to thwart the identified threats as an additional layer of protection.
- **Automated Threat Searching:** AI tools actively search a system for hidden signs of compromise, such as lateral movement or persistence, before they evolve into attacks.

IV. RESULTS

1. **Detection Accuracy and Performance**

The AI models in the assessed literature had a prominent rate of effectiveness in finding cyber threats including but not limited to intrusions, malware, phishing, and DDoS attacks.

Model / Technique	Detection Accuracy	False Positive Rate (FPR)	Dataset Used
Random Forest	96.2%	3.1%	NSL-KDD
CNN (Deep Learning)	98.5%	1.9%	NSL-KDD
LSTM-RNN	97.3%	2.4%	UNSW-NB15
Autoencoder + SVM	94.8%	4.0%	Custom IoT dataset
Hybrid Metaheuristic + ML	98.9%	1.5%	KDD99

DOI: 10.17148/IJIREEICE.2025.13914

Observations:
Deep learning models (e.g., CNN, LSTM) perform better on datasets due to the ability to detect intricate attack patterns as compared to traditional ML.
Hybrid models that improve classifiers by mixing optimization (i.e., genetic algorithms and particle swarm) enhance accuracy.
False positive rates are highly dependent on dataset quality and balance.

2. Stability of the model against changing threats
Adversarial robustness is an increasing point of focus. Some models trained on adversarial data augmentation provide effective capabilities of classifying obfuscated, or polymorphic, malware. (For instance, a GAN-based Sample Majority strategy improved classification accuracy ~4-7% compared to standard DL models).

Nevertheless, many models remain susceptible to evasion attacks, especially nonfrequent retrained models and those were exposed to zero-day threats.

3. **Scalability and Adaptability**

- AI models trained on static datasets often struggle to adapt to new, unseen threats or environments.
- Continual learning and online training approaches have shown promise but are not yet widely deployed due to concerns over model drift and security.
- Federated learning shows potential for large-scale, privacy-preserving threat detection but introduces overhead.

4.Explainability and Interpretabili

- Standard ML models (e.g., decision trees, SVM) provide more explainability than deep Model
- Studies are currently using SHAP and LIME, as well as attention mechanisms, to explain predictions. This type of explanation enables cybersecurity analysts to understand the following questions:.
- Why was the forensic tool warning about a specific packet or session?
- Which features contributed substantially to this decision (e.g., unusual port usage, unusual payload size).

5. Limitations Observed in Results

- Imbalanced datasets can have a problem with reliable model performance. High accuracy can mask larger issues with detection of the minority class.
- Some synthetic benchmarks (e.g., KDD99) may lack the level of sophistication found in actual attack scenarios.
- False alarms continue to be a problem in the operational environment and contribute to alert fatigue.
- Black-box AI systems tend to face pushback from security analysts who prefer some form of explanation in the algorithm through rules.

V. DISCUSSION

AI is now a crucial component of modern cybersecurity, providing robust capabilities in the realms of detection, prediction, and response, but its introduction needs careful consideration. Although AI can bolster security, it can also give rise to new risks and complexities requiring solid design, testing, and ethical consideration. The security community must remain focused and collaborative to ensure that AI acts as a force for defense, not exploitation.Limitations of the study include reliance on self-reported data.

VI. CONCLUSION

Artificial Intelligence (AI) is having a revolutionary impact on cybersecurity, augmenting our abilities to detect, assess, and react to new, intricate, and evolving cyber risks, utilizing machine learning, deep learning, and large language models to boost accuracy in identifying threats, automate responses, and provide proactive defensible security measures.
Simultaneously, the application of AI in this area creates risks of its own. The cybercriminal community is increasingly capitalizing on AI to create more sophisticated attacks, including AI-created phishing, adversarial inputs, and automated malware. This duality risks a perpetual arms race between the attacker and defender.
Our analysis is clear: AI can substantially extend our defensive cybersecurity systems, but it also will not replace conventional methods. Additionally, there are challenges that must be addressed, including adversarial vulnerability, explainability, data quality, and ethics.

DOI: 10.17148/IJIREEICE.2025.13914

To maximize the benefits of AI in cybersecurity as we move forward, we must focus on developing trustworthy, transparent and adaptable AI systems.
For example:
Creating adversarial-resistant model
Using models that are explicable (Explainable AI)
Utilizing datasets from the real world, including the diverse nature of datasets
Using AI in ethical ways, and regulatory compliance.
In summary, AI can be a powerful partner and a potential threat in cybersecurity. Successful application will consider innovation, oversight, and balance ability to harness power against it.

REFERENCES

[1] A. Clim, “Cyber Security Beyond the Industry 4.0 Era. A Short Review on a Few Technological Promises,” *Inform. Econ.*, vol. 23, no. 2/2019, pp. 34–44, Jun. 2019, doi: 10.12948/issn14531305/23.2.2019.04.

[2] P. Bagó, “Cyber security and artificial intelligence,” *Econ. Finance*, vol. 10, no. 2, pp. 189–212, 2023, doi: 10.33908/EF.2023.2.5.

[3] M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, “Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview,” *Mesopotamian J. Cyber Secur.*, pp. 57–63, Mar. 2023, doi: 10.58496/MJCS/2023/010.

[4] “Cyber Threat Intelligence Market Report 2024 - Cyber Threat Intelligence
Market Trends And Overview.” Accessed: Nov. 06, 2024. [Online]. Available:
https://www.thebusinessresearchcompany.com/report/cyber-threatintelligenceglobal-market-report

[5] N. Kaloudi and J. Li, “The AI-Based Cyber Threat Landscape: A Survey,” *ACM Comput. Surv.*, vol. 53, no. 1, p. 20:1-20:34, Feb. 2020, doi: 10.1145/3372823.

[6] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, “Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity,” *IEEE Access*, vol. 8, pp. 23817–23837, 2020, doi: 10.1109/ACCESS.2020.2968045.

[7] R. Sarkis-Onofre, F. Catalá-López, E. Aromataris, and C. Lockwood, “How to properly use the PRISMA Statement,” *Syst. Rev.*, vol. 10, no. 1, pp. 117, s13643021-01671-z, Dec. 2021, doi: 10.1186/s13643-021-01671-z.

[8] V. Welch *et al.*, “Extending the PRISMA statement to equity-focused systematic reviews (PRISMA-E 2012): explanation and elaboration,” *J. Clin. Epidemiol.*,
vol. 70, pp. 68–89, Feb. 2016, doi: 10.1016/j.jclinepi.2015.09.001. [9] R. Briner and D. Denyer, “Systematic Review and Evidence Synthesis as a Practice and Scholarship Tool,” in *Handbook of evidence-based management: Companies, classrooms and research*, 2012, pp. 112–129. doi: 10.1093/oxfordhb/9780199763986.013.0007.

[10] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, “Preferred reporting items for systematic reviews and metaanalyses: The PRISMA statement,” *Int. J. Surg.*, vol. 8, no. 5, pp. 336–341, Jan. 2010, doi: 10.1016/j.ijsu.2010.02.007.