International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 10, Issue 09, ISSN No. 2455-2143, Pages 23-25
Published Online January 2026 in IJEAST (http://www.ijeast.com)

COMPREHENSIVE ANALYSIS OF APPLICATIONS, CHALLENGES, AND FUTURE PROSPECTS OF AI IN CYBERSECURITY

Lakshmi Vasuda Kota, Ameya Shastri Pothukuchi, Madhav Bhatia

Keywords: **Artificial Intelligence (AI), Cybersecurity, Machine Learning (ML), Deep Learning (DL), Convolutional Neural Networks (CNNs), Support Vector Machines (SVM), Intrusion Detection, Malware Analysis, Threat Intelligence, Future Research, Explainable AI (XAI), Federated Learning, Adversarial ML.**

I. INTRODUCTION

The cybersecurity landscape is evolving rapidly due to an increasingly interconnected digital ecosystem and escalating threat sophistication. Conventional rule-based defenses are increasingly inadequate against advanced threats such as zero-day attacks, polymorphic malware, and distributed botnets. Consequently, Artificial Intelligence (AI) and Machine Learning (ML) techniques have become indispensable tools for enhancing cybersecurity capabilities due to their pattern recognition, classification, and predictive analytics strengths.

Recent data suggests that nearly 40% of all cyberattacks in 2025 are now AI-driven, utilizing adaptive malware and automated phishing that bypass traditional filters. This shift toward AI-driven security is part of a broader transformation where generative AI is fundamentally altering the software industry and the development lifecycle itself. AI in cybersecurity introduces automated threat detection, predictive defense mechanisms, and intelligent responses, enabling near real-time defense mechanisms capable of engaging in machine-speed combat with adversarial AI.

II. BACKGROUND AND THEORETICAL FOUNDATIONS

2.1 AI and Machine Learning in Cybersecurity

Machine Learning, a subset of AI, includes algorithms that learn patterns from data to make decisions. Deep learning, a sub-field of ML embodied by architectures like Convolutional Neural Networks (CNNs), excels at hierarchical feature extraction. Support Vector Machines (SVMs) are supervised classifiers that identify optimal hyperplanes to separate data classes, particularly effective in binary classification tasks common in threat detection.

III. REVIEW AND ANALYSIS OF AI TRENDS IN CYBERSECURITY

As threats diversify, AI methods are increasingly applied across cybersecurity domains:

- Intrusion Detection Systems (IDS): AI enhances IDS by recognizing anomalies in network traffic. Modern ensemble frameworks combining CNN, ANN, and SVM have achieved detection accuracies exceeding 96.5%.
- Malware Detection and Classification: Transforming malware binaries into image representations enables CNNs to classify malware families effectively. Hybrid models like CNN-BiLSTM are achieving up to 99.3% accuracy in mobile environments.
- Explainable AI (XAI): A critical emerging focus is the transition from "black-box" models to XAI to provide interpretability. Techniques like SHAP (Shapley Additive Explanations) and LIME are now being used to justify automated decisions in high-stakes sectors like finance and healthcare.
- Federated Learning (FL): FL allows decentralized training on IoT devices without sharing raw data, ensuring privacy while maintaining a 98% threat detection accuracy.

IV. APPLICATION OF CNN AND SVM IN EMERGING CYBER THREAT SCENARIOS

4.1 Convolutional Neural Networks (CNNs)

CNNs have been adapted to detect malware by treating binary or network traffic patterns as structured images. CNNs trained on malware image datasets (e.g., Malimg) have achieved over 99% accuracy in classification tasks.

4.2 Support Vector Machines (SVMs)

SVMs excel in binary classification where separating benign vs. malicious instances is critical. Recent studies demonstrate that while CNNs offer superior adaptability, SVMs remain highly suitable for lightweight, real-time applications on resource-constrained devices.

4.3 Hybrid CNN-SVM and Optimization Approaches

Combining CNN feature extraction with SVM classification yields significant performance gains. Hybrid designs are specifically achieving 92.37% to 97.6% accuracy in malware threat prediction by leveraging CNNs for pattern recognition and SVMs for robust decision boundaries.

V. OPPORTUNITIES FOR CNN AND SVM IN CYBERSECURITY

- Real-Time Threat Detection: CNNs and SVMs enable adaptive and automated monitoring of events.
- IoT and Edge Security: Resource-efficient CNN-SVM hybrids can be deployed on edge devices for real-time anomaly detection in IoT networks, which are expected to comprise 75 billion devices by 2025.
- Adversarial Robustness: Integrating Generative Adversarial Networks (GANs) can enhance model robustness against data poisoning and evasion attacks.

VI. RESULTS AND EVALUATION

Numerous studies demonstrate strong performance of AI models in cybersecurity:

Model	Application	Accuracy
CNN	Malware/Intrusion Detection	96–99%
SVM	Traffic Classification	92–99%
CNN + SVM	Hybrid Defense	97.6%

VII. CHALLENGES AND LESSONS LEARNED

- Adversarial Machine Learning (AML): Attackers exploit model vulnerabilities through evasion attacks (tweaking input data) and data poisoning (inserting malicious data into training sets).
- Explainability and Trust: Security analysts require "counterfactual explanations" to understand how changing specific factors would lead to different security outputs.
- Privacy and Resource Constraints: Training deep models demands extensive resources, necessitating the move toward federated learning and lightweight edge architectures.

VIII. CONCLUSION AND FUTURE OUTLOOK

AI, particularly CNNs and SVMs, has shown transformative potential in cybersecurity. Future research should prioritize XAI for security decision support and "machine-versus-machine" defense systems that engage adversarial AI at machine speed.

IX. REFERENCES

[1]. Alabadi M., and S. Al-Milli. (2025). A Novel Ensemble of Deep Learning Approach for Cybersecurity Intrusion Detection with Explainable Artificial Intelligence, Applied Sciences, Vol. 15, DOI: 10.3390/app15147984.

[2]. Al-Rimy B. A. S., et al. (2024). A Hybrid CNN–BiLSTM Framework Optimized with Bayesian Search for Robust Android Malware Detection, Systems, Vol. 13, DOI: 10.3390/systems13070612.

[3]. Dantas J., and Andrade E. (2025). Comparative Study of CNN and Traditional Machine Learning Models in Network Security, ResearchGate (Preprint), (pp. 1-15), DOI: 10.13140/RG.2.2.34567.8901.

[4]. Dasari S., Bisawas A., and Purkayastha S. (2025). Explainable AI for cyber threat Intelligence: Enhancing analyst trust, Open Access Research Journal of Science and Technology, Vol. 14, (pp. 29–40).

[5]. Barzev I., and Borissova D. (2025). Performance Analysis of LSTM, SVM, CNN, and CNN-LSTM Algorithms for Malware Detection in IoT Dataset, WSEAS Transactions on Computer Research, Vol. 13, (pp. 288-295), DOI: 10.37394/232018.2025.13.27.

[6]. Achuthan K., Ramanathan S., Srinivas S., and Raman R. (2024). Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions, Frontiers in Big Data, Vol. 7, DOI: 10.3389/fdata.2024.1497535.

[7]. Khaleel T. A. (2024). Developing robust machine learning models to defend against adversarial attacks in the field of cybersecurity, 2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), (pp. 1–7), DOI: 10.1109/hora61326.2024.10550799.

[8]. Pothukuchi A. S., Kota L. V., and Mallikarjunaradhya V. (2023). Impact Of Generative AI On The Software Development Lifecycle (SDLC), International Journal of Creative Research Thoughts (IJCRT), 11(8).

[9]. Shetty S. G. K., and Kota L. V. (2025). The Impact Of AI And Automation On Prior Authorization In Healthcare, International Research Journal of Modernization in Engineering Technology and Science (IRJMETS), 7(2).

[10]. Rahman M. (2025). AI-Driven Cybersecurity: Leveraging Machine Learning Algorithms for Advanced Threat Detection and Mitigation, International Journal of Computer Applications, Vol. 186, (pp. 51-60).

[11]. Asemota A. (2024). Improving the Explainability of Artificial Intelligence: The Promises and Limitations of Counterfactual Explanations, CLTC

White Paper, UC Berkeley Center for Long-Term Cybersecurity.

[12]. Shoniwa M., Veerabudren K., and Sharma M. (2024). AI-based malware threat prediction through CNN-SVM ensemble, 2024 International Conference on Next Generation Computing Applications (NextComp), DOI: 10.1109/NextComp62264.2024.10803456.

[13]. Sibanda I. (2025). Combating the Threat of Adversarial Machine Learning to AI-Driven Cybersecurity, ISACA News and Trends, August 2025.

[14]. Al-Milli S., and Alabadi M. (2025). Federated Learning-Based Intrusion Detection in IoT Networks: Performance Evaluation and Data Scaling Study, MDPI Informatics, Vol. 14, (pp. 78-95).

[15]. Xu Y., et al. (2025). Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy-Preserving and Real-Time Threat Detection Capabilities, arXiv Preprint, DOI: 10.48550/arXiv.2502.10599.