AI-Driven Advancements in Cybersecurity

Conference: 13th AICLST, Kolkata, 6–8 March 2026

Paper reference: TA-12/P

Printed pages: 309–314

Source: *Leather 2050: Challenges & Opportunities*, ILTA (2026)

AI-Driven Advancements in Cybersecurity

1, 2 Department of Computer science & Engineering, 3,4 Department of Information Technology, 5Department of Electronics and Communication, Government College of Engineering & Leather Technology Kolkata-700106, India

Ref. No. TA-12/P

Falguni Sinhababu1

, Brijesh Kumar Sriwastava2, Kalyan Mahata3, Srirupa Dasgupta4, Ipsita Sengupta5

Abstract

Artificial Intelligence (AI) is transforming cybersecurity by enhancing threat detection, incident response, and risk mitigation. Leveraging techniques such as machine learning, deep learning, and neural networks, AI enables systems to identify patterns, detect anomalies, and predict potential attacks with high accuracy. It supports automated, real-time decision-making, reducing reliance on human operators and improving response efficiency. By analyzing vast and heterogeneous datasets, AI uncovers sophisticated attack vectors and hidden vulnerabilities across complex digital environments. Additionally, AI augments human cybersecurity expertise by providing actionable insights, optimizing resource allocation, and enhancing threat intelligence. While challenges remain, AI integration marks a shift toward proactive, resilient cybersecurity, empowering organizations to defend against increasingly advanced adversaries effectively. The leather industry’s increasing use of automation, IoT, and global supply chains heightens cybersecurity risks. Attacks can disrupt production, cause financial loss, and expose data, making robust security essential.

Keywords — Machine Learning (ML), Deep Learning (DL), Artificial Intelligence (AI), Cyber Security.

1. Introduction

The integration of Artificial Intelligence (AI) has profoundly transformed cybersecurity, enhancing the

Corresponding author email: fsinha@gmail.com

ability to detect, predict, and mitigate digital threats. Machine Learning (ML) and AI algorithms improve applications such as fraud detection and spam filtering by analyzing historical datasets to identify anomalies and forecast potential attacks. These systems surpass human capabilities in processing large volumes of data, uncovering complex patterns that might go unnoticed manually, while also reducing false positives associated with traditional methods.

As cyberattacks grow increasingly sophisticated and frequent, conventional security frameworks struggle to keep pace. AI emerges as a transformative solution, redefining defense strategies by enabling real-time threat detection, predictive analytics, and adaptive response mechanisms. It supports cybersecurity professionals by providing actionable insights, optimizing resource allocation, and enhancing threat intelligence, creating a powerful human–machine partnership.

This paper examines the expanding role of AI in fortifying digital ecosystems, emphasizing its contributions across threat detection, incident response, and proactive defense. By leveraging a range of AI methodologies—from ML models to neural networks—security systems can analyze extensive datasets, uncover hidden patterns, and anticipate potential threats with high precision. The synergistic integration of AI and human expertise establishes a resilient cybersecurity framework capable of addressing a diverse and evolving spectrum of cyber risks.

2. Liturature Overview

The impact of a successful cyberattack can be severe, affecting individuals and organizations alike. With vast amounts of personal, financial, and operational data at risk,

breaches can cause financial loss, reputational damage, and operational disruption. Cyber adversaries often target the weakest link—human users and their devices. Artificial Intelligence (AI), powered by machine learning, is increasingly deployed to enhance cybersecurity defenses by detecting anomalies, predicting threats,

and enabling rapid response [5].

Despite technological progress, human involvement remains crucial, as traditional security operations still rely on manual decision-making. Human error, particularly in

Table 1: Review of AI-based Cyber Security Techniques

Author Techniques Used Features / Contributions

Al-Yaseen et al. [1] Deep Learning (DL), AI Integration Presents best practices in cybersecurity using advanced AI techniques, particularly Deep Learning.

Achi Unimke Aaron et al. [2]

Defensive Security Policies, Risk Assessment

Examines the influence of cyber threats on emerging technologies and business environments.

R. Banu et al. [3] Multi-Agent Systems, Recurrent Neural Networks

Highlights the effective utilization of agent-based systems for securing network devices.

Shruthi Kohli [4] Supervised Machine Learning, Decision Tree Classifier

Describes supervised ML techniques for cyber defense and their application in anti-malware detection.

O. Oriola et al. [5] ML Algorithm Enhancement, SHOWAN System

Investigates the improvement of ML algorithms and their impact on enhancing threat detection performance.

I. Baptista et al. [6] AI Vulnerability Detection, Threat Identification

Discusses the role of AI in identifying vulnerabilities and detecting threats on social media platforms.

E. Menahem et al. [7] Multi-Inducer Ensemble Methods Demonstrates improved malware detection accuracy using ensemble-based learning approaches.

Ionita and L. Ionita [8] Agent-Based IDS Framework Explores the application of agent-based models for designing intrusion detection systems.

Barbara D. et al. [9] Data Mining for Intrusion Detection Utilizes data mining approaches to identify and detect intrusive behaviors.

C. Wang et al. [10] Hierarchical Temporal Memory (HTM)

Proposes distributed anomaly detection for in-vehicle networks using HTM models.

J. Raiyn [11] Survey of Cyberattack Detection Provides a comprehensive review and comparative analysis of cyberattack detection techniques.

Bose S. et al. [12] MalConv-Based Analysis Analyzes and explains convolutional approaches for malware detection.

Chowdhury M. et al. [13] Data Mining and ML Classification Discusses malware identification through data mining and machine learning classification methods.

Coull S., Gardner [14] Byte-Level Deep Neural Network Conducts activation analysis of deep neural networks for improved malware classification.

complex system configurations, remains a significant vulnerability. As digital systems grow more sophisticated, security alert systems help identify threats and support timely remediation [6].

This paper provides an overview of AI-driven cybersecurity applications, illustrating how intelligent systems strengthen defenses against evolving threats. A summary of key AI-based techniques is presented in Table 1, highlighting their role in proactive threat detection and mitigation.

3. AI Driven Approach in Cyber Security

AI enables rapid and efficient analysis of user behavior, allowing for the quick identification of network anomalies

Table 2: Application of AI in Cyber Security

AI in Cybersecurity Definition

AI-enabled solutions that continuously monitor networks or systems for suspicious behavior or policy breaches, allowing real-time identification and mitigation of possible threats.

Intrusion Detection and Prevention Systems (IDPS)

Predictive Analytics AI models that study historical patterns and system activities to anticipate future cyber risks or weaknesses, supporting proactive defence strategies.

User Behavior Analytics (UBA) AI tools that observe and evaluate user activity to detect abnormal patterns or deviations that may signal insider threats or security intrusions.

Automated Threat Response Intelligent systems designed to independently react to security events, reduce risks, and perform necessary corrective measures without human delay.

Vulnerability Management AI-powered applications that discover, assess, and address system vulnerabilities, helping maintain a stronger overall security framework.

Security Orchestration, Automation, and Response (SOAR)

AI-driven platforms that unify various security tools, streamline automated processes, and manage incident response activities for more effective threat handling.

4. AI – Driven Transformation in Cyber Security

Businesses today prioritize system security due to the significant impact of cyberattacks. To protect their infrastructure, organizations employ multilayered defenses, starting with firewalls that filter incoming network traffic, followed by antivirus software to detect malicious files and suspicious code. Data backups are also implemented as part

Table 3: Traditional vs. AI-based Cyber Security

Traditional Cybersecurity AI-Based Cybersecurity

Depends mainly on human analysis and manual intervention Relies more on automated, AI-driven detection and response

Primarily uses signature-based techniques to spot known threats

Uses AI-driven behavioral analysis to uncover new and evolving threats

Treats incidents reactively, with responses triggered after problems are detected

Focuses on proactive, AI-enabled prediction and prevention of cyber attacks

Has limited flexibility and scalability when dealing with complex or large-scale attacks

Improves scalability and agility through automated, AI-supported incident handling

Follows fixed, rule-based security protocols Utilizes adaptive AI systems capable of self-learning and adjusting to emerging threats

Heavily relies on human specialists to interpret data and respond to threats

Employs AI for fast analysis and decision support, strengthening and extending the capabilities of experts

and potential cybersecurity vulnerabilities. However, continued dependence on human expertise for critical tasks can introduce risks, as attackers may deploy malicious programs that imitate legitimate AI algorithms (Table 2).

of disaster recovery strategies [7]. Table 3 illustrates the current reliance on human-driven, traditional cybersecurity methods. Looking ahead, AI is expected to transform the field, enabling automation, adaptive security measures, and proactive threat detection, thereby enhancing organizational resilience and improving defenses against increasingly sophisticated cyber threats.

Domain AI/ML Techniques Applications

5. AI-Based Algorithms for Cyber Security

AI leverages classification algorithms to distinguish normal from abnormal patterns in datasets, learning from historical data to identify complex behaviors and make accurate predictions [8–9]. Algorithms such as Random Forests and Decision Trees are widely applied in Network Intrusion Detection and Spam Filtering.

Table 4: AI Algorithms for Cyber Security

Intrusion Detection and Prevention Systems (IDPS)

SVM, Random Forests,

KNN, Decision Trees

CNNs, LSTMs, Genetic Algorithms, Clustering (K-

Malware Detection and

Prevention

means)

User Behavior Analytics

(UBA) GMMs, HMMs, PCA

Reinforcement Learning,

Automated Incident

Case-Based Reasoning,

Response

Fuzzy Logic

Bayesian Networks, Neural

Vulnerability Management

Networks, Genetic Programming, MDPs

6. AI-Driven Applications in Cyber Security

AI methodologies are integral to modern cybersecurity, providing intelligent, adaptive, and automated mechanisms to protect digital systems. Each approach contributes specialized capabilities for detecting, predicting, and mitigating cyber threats, creating a comprehensive and robust security framework. By employing machine learning, behavior analysis, predictive analytics, and

Table 5: Applications of AI in Cyber Security

AI Technique Methods/Models Applications in Cybersecurity

Machine Learning (ML) Supervised Learning, Unsupervised Learning Detect malicious software, classify threats, identify anomalies or novel attacks

Natural Language Processing (NLP) Sentiment Analysis, Text Classification Detect harmful communications, categorize and prioritize security-related textual data

Deep Learning Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs)

Reinforcement Learning (RL) Trial-and-error learning, Policy Optimization Adaptive security measures, dynamic defense adjustments, refining security policies

Automated Reasoning Logical inference, Rule-based frameworks Deduce, predict, and respond to potential threats based on defined rules

Their strength lies in accurately differentiating legitimate activity from malicious behavior, enabling precise detection of network intrusions and effective filtering of spam. This predictive accuracy reduces security risks, enhances overall system performance, and makes classification algorithms essential tools for maintaining secure and reliable digital infrastructures [10].

Identify and classify anomalous network behavior;

detect malicious activities

Analyze malware signatures,

sequential behaviors; optimize detection rules

Detect abnormal user actions,

insider threats, and deviations from normal

behavior

Automate mitigation, adaptive responses, and

decision-making

Predict, prioritize, and

mitigate system

vulnerabilities

automated decision-making, AI enhances the detection of anomalies, enables rapid incident response, and safeguards infrastructures against sophisticated attacks. These technologies not only strengthen defenses but also optimize security operations by reducing human workload, improving accuracy, and enabling proactive protection, making AI an essential component of resilient and effective cybersecurity strategies.

Image-based threat detection, sequential data analysis (network traffic, system logs)

7. Challenges of Using AI in Cyber Security

While AI provides significant benefits for cybersecurity, it also faces notable limitations and challenges, exemplified by deepfake detection:

Adversarial Attacks: AI models can be deceived by subtle manipulations in data that are imperceptible to humans, allowing attackers to bypass detection systems [11].

Lack of Training Data: Effective AI detection relies on diverse, high-quality datasets of deepfakes (video, audio, images). Obtaining such data is challenging, limiting model accuracy and generalizability.

Resource Intensity: Training and maintaining advanced AI models requires substantial computational power, which can be costly and difficult for smaller organizations to implement.

False Positives/Negatives: AI systems may misclassify legitimate content as fake or fail to detect actual deepfakes, undermining trust, reliability, and overall effectiveness.

These challenges highlight the need for careful design, validation, and ongoing monitoring of AI-driven cybersecurity solutions.

8. Conclusion

Artificial Intelligence (AI) has become a transformative tool in cybersecurity, enhancing the capabilities of human security teams in managing complex and evolving threats. By analyzing large-scale data and generating real-time alerts, AI enables the identification and prioritization of risks, allowing teams to focus on the most critical vulnerabilities. The collaboration between AI and human experts creates a powerful synergy, where AI handles repetitive detection tasks and humans concentrate on strategic decision-making and proactive threat mitigation. This human–machine partnership acts as a force multiplier, improving precision, agility, and overall effectiveness in safeguarding digital infrastructures against ever-evolving

cyber threats. The leather industry faces increasing cybersecurity risks due to automation, IoT adoption, and complex global supply chains. Cyberattacks can cause financial losses, production downtime, and data breaches, making strong security practices essential.

Reference

a) W. Al-Yaseen, Z. Othman, and M. Z. Ahmad Nazri, “Multi-level hybrid support vector machine and extreme learning machine based on modified kmeans for intrusion detection system,” Expert Systems with Applications, vol. 67, 2017.

b) S. B. Atiku and A. U. Aaron, “Survey on the applications of artificial intelligence in cyber security, ITU, and WCIT,” in 7th Int. Conf. on Cyber Conflict: Architectures in Cyberspace, 2019, pp. 119–134.

c) R. Banu, M. A., C. A., S. A., H. Ujwala, and N. H., “Detecting phishing attacks using natural language processing and machine learning,” 2019, pp. 1210–1214.

d) S. Kohli, “Developing cyber security asset management framework,” Int. J. of Advanced Research in Artificial Intelligence (IJARAI), vol. 2, no. 4, 2018.

e) O. Oriola, A. Adeyemo, and A. Robert, “Distributed intrusion detection system using P2P agent mining scheme,” African J. of Computing & ICT, vol. 5, no. 2, 2020.

f) I. Baptista, S. Shiaeles, and N. Kolokotronis, “A novel malware detection system based on machine learning and binary visualization,” 2019, pp. 1–6, doi: 10.1109/ICCW.2019.8757060.

g) E. Menahem, A. Shabtai, L. Rokach, and Y. Elovici, “Improving malware detection by applying multiinducer ensemble,” Comput. Statist. Data Anal., vol. 53, no. 4, pp. 1483–1494, Feb. 2013.

h) L. Ionita and I. Ionita, “An agent-based approach for building an intrusion detection system,” RoEduNet Int. Conf. 12th Edition: Networking in Education and Research, 2020, pp. 1–6.

i) D. Barbara, J. Couto, S. Jajodia, L. Popyack, and N. Wu, “ADAM: Detecting intrusions by data mining,” 2001, pp. 5–6.

j) C. Wang, Z. Zhao, L. Gong, L. Zhu, Z. Liu, and X. Cheng, “A distributed anomaly detection system for in-vehicle network using HTM,” IEEE Access, vol. 6, pp. 9091–9098, 2018, doi: 10.1109/ ACCESS.2018.2799210.

k) J. Raiyn, “A survey of cyber attack detection strategies,” Int. J. of Security and Its Applications, vol. 8, no. 1, pp. 247–256, 2014.

l) S. Bose, T. Barao, and X. Liu, “Explaining AI for malware detection: Analysis of mechanisms of MalConv,” in 2020 Int. Joint Conf. on Neural Networks (IJCNN), 2020, pp. 1–8.

m) M. Chowdhury, A. Rahman, and M. R. Islam,

“Malware analysis and detection using data mining and machine learning classification,” 2018, pp. 266– 274, doi: 10.1007/978-3-319-67071-3_33.

n) S. Coull and C. Gardner, “Activation analysis of a byte-based deep neural network for malware classification,” 2019, pp. 21–27, doi: 10.1109/ SPW.2019.00017.