Enhancing Cybersecurity Using Artificial Intelligence and Machine Learning: A Review

Sumit Kumar
B.Tech Student, Global Institute of Technology, Jaipur, Rajasthan, India
23egjcs816@gitjaipur.com

Sumit Kumawat
B.Tech Student, Global Institute of Technology, Jaipur, Rajasthan, India
23egjcs817@gitjaipur.com

Sunil Kumar
B.Tech Student, Global Institute of Technology, Jaipur, Rajasthan, India
23egjcs818@gitjaipur.com

Chandrabhan Mishra
Assistant Professor, Global Institute of Technology, Jaipur, Rajasthan, India
chandrabhan.mishra@gitjaipur.com

Abhay Purohit
Assistant Professor, Global Institute of Technology, Jaipur, Rajasthan, India
abhay.purohit@gitjaipur.com

ABSTRACT: The rapid expansion of digital infrastructure and internet-based services has significantly increased the frequency and sophistication of cyber threats. Traditional cybersecurity mechanisms, which rely on signature-based detection and predefined rules, are often inadequate against evolving and unknown attacks. Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful tools for strengthening cybersecurity by enabling automated threat detection, real-time analysis, and adaptive defense mechanisms. This paper presents a short review of AI- and ML-based approaches used in cybersecurity. It discusses key applications, commonly used algorithms, advantages, challenges, and future research directions in developing intelligent and resilient security systems.

IJGRST
INTERNATIONAL JOURNAL OF
GLOBAL RESEARCH IN SCIENCE AND TECHNOLOGY

KEYWORDS: Cybersecurity, Artificial Intelligence, Machine Learning, Intrusion Detection, Malware Detection, Network Security.

1. INTRODUCTION

The rapid growth of digital technologies, cloud computing, Internet of Things (IoT), mobile networks, and online services has transformed the way information is created, stored, and shared. While this digital transformation has improved efficiency, connectivity, and accessibility, it has also significantly increased the vulnerability of systems to cyber threats. Modern cyberattacks such as malware, ransomware, phishing, denial-of-service (DoS), and advanced persistent threats (APTs) are becoming more frequent, sophisticated, and difficult to detect. These attacks can lead to severe consequences, including data breaches, financial losses, service disruptions, and loss of user trust.

Traditional cybersecurity solutions primarily rely on rule-based systems and signature-based detection techniques. These methods are effective in identifying known threats but fail to detect zero-day attacks, polymorphic malware, and rapidly evolving attack strategies.

Additionally, manual monitoring and static security rules are insufficient to handle the massive volume, velocity, and variety of modern network traffic. As cyber threats continue to evolve, there is a growing need for intelligent, automated, and adaptive security mechanisms capable of responding to attacks in real time.

Artificial Intelligence (AI) and Machine Learning (ML) have emerged as promising technologies to address these challenges. Unlike conventional security approaches, AI-based systems can learn from historical data, identify hidden patterns, and make accurate predictions without explicit programming. Machine learning algorithms enable cybersecurity systems to detect anomalies, classify malicious activities, and adapt to new attack behaviors over time. These capabilities make AI and ML particularly suitable for securing complex and dynamic digital environments.

In recent years, AI and ML have been widely applied in various cybersecurity domains, including intrusion detection systems, malware analysis, phishing detection, fraud prevention, and network traffic monitoring. Supervised, unsupervised, and deep learning techniques are used to analyze large-scale security data and improve detection accuracy while reducing false alarms. Furthermore, AI-driven automation enhances incident response by enabling faster decision-making and minimizing human intervention.

This paper presents a short review of AI- and ML-based approaches in cybersecurity. It explores key application areas, commonly used machine learning algorithms, advantages of intelligent security systems, and the challenges associated with their deployment. The paper also highlights future research directions aimed at developing robust, scalable, and resilient cybersecurity solutions capable of protecting modern digital infrastructure.

IJGRST INTERNATIONAL JOURNAL OF GLOBAL RESEARCH IN SCIENCE AND TECHNOLOGY

2. ROLE OF AI AND ML IN CYBERSECURITY

AI and ML are applied across various domains of cybersecurity to improve detection accuracy and response time.

A. Intrusion Detection Systems (IDS)

Machine learning algorithms such as Support Vector Machine (SVM), Random Forest, and Neural Networks are used to identify abnormal network traffic and unauthorized access attempts. Deep learning models enhance detection performance in complex and high-volume network environments.

B. Malware Detection

AI-based techniques analyze executable files, system behavior, and network activities to detect known and unknown malware. Deep learning models such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) enable accurate classification of malicious software.

C. Phishing and Spam Detection

ML algorithms analyze email content, URLs, and user behavior to identify phishing attacks and spam messages. Natural Language Processing (NLP) techniques improve detection of deceptive text-based attacks.

D. Fraud and Anomaly Detection

AI-driven systems detect unusual patterns in financial transactions, user activities, and system logs, helping prevent fraud and insider threats.

3. COMMONLY USED MACHINE LEARNING TECHNIQUES

- **Supervised Learning:** SVM, Logistic Regression, Decision Trees, Naïve Bayes
- **Unsupervised Learning:** K-Means, Autoencoders, Isolation Forest
- **Deep Learning:** CNN, RNN, LSTM
- **Reinforcement Learning:** Adaptive security policies and automated response systems.

4. ADVANTAGES OF AI AND ML IN CYBERSECURITY

Artificial Intelligence (AI) and Machine Learning (ML) provide several significant advantages that enhance the effectiveness and resilience of modern cybersecurity systems:

- **Real-Time Threat Detection:** AI- and ML-based systems can continuously monitor network traffic, system logs, and user behavior in real time. By analyzing patterns and detecting anomalies instantly, these systems enable faster identification of cyberattacks such as intrusions, malware infections, and denial-of-service attacks, thereby minimizing potential damage.
- **Improved Accuracy:** Traditional security mechanisms often suffer from high false positive and false negative rates. Machine learning algorithms improve detection accuracy by learning from historical data and distinguishing between normal and malicious behavior more effectively. This results in more reliable threat detection and reduces unnecessary alerts for security teams.
- **Adaptive Defense Mechanisms:** One of the key strengths of AI and ML is their ability to adapt to evolving threats. As new attack patterns emerge, machine learning models can update themselves through continuous learning, allowing cybersecurity systems to respond proactively to previously unknown or zero-day attacks.
- **Automation and Efficiency:** AI-driven cybersecurity solutions automate routine tasks such as threat analysis, alert prioritization, and incident response. This reduces dependence on manual monitoring, lowers human error, and allows security professionals to focus on critical and complex security challenges.
- **Scalability and Big Data Handling:** Modern networks generate massive volumes of data from diverse sources. AI and ML techniques can efficiently process and analyze large-scale and high-dimensional data, making them suitable for securing enterprise

IJGRST INTERNATIONAL JOURNAL OF GLOBAL RESEARCH IN SCIENCE AND TECHNOLOGY

networks, cloud infrastructures, and IoT environments without compromising performance.

Overall, the integration of AI and ML into cybersecurity frameworks leads to faster, smarter, and more scalable security solutions capable of protecting complex digital ecosystems against advanced cyber threats.

5. CONCLUSION

Artificial Intelligence and Machine Learning are transforming cybersecurity by enabling intelligent, adaptive, and automated defense mechanisms. From intrusion detection to malware and fraud prevention, AI-driven security systems significantly enhance protection against evolving cyber threats. While challenges remain, continued research and innovation in AI and ML will play a crucial role in building robust and resilient cybersecurity frameworks for the digital future.

REFERENCES

[1] I. Yadav, V. Shekhawat, K. Gautam, G. Kumar Soni and R. Yadav, "Artificial Intelligence for Cybersecurity: Emerging Techniques, Challenges, and Future Trends," 2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), pp. 1176-1180, 2025.

[2] N. Sharma, “An analytical study of distributed data store using big data analysis technique,” Research Methods, Imparc, 2019.

[3] S. Thapar, G. K. Soni, H. Kaushik, R. Singh, S. Bisht and S. K. Bansal, "A Comparative Machine Learning Framework for Detecting Fake Accounts on Facebook," 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 1567-1571, 2025.

[4] N. Soni, N. Nigam, "Recent Advances in Artificial Intelligence and Machine Learning: Trends, Challenges, and Future Directions", International Journal of Engineering Trends and Applications (IJETA), Vol. 12, Issue. 1, pp. 9-12, 2025.

[5] R. Joshi, M. Farhan, U. Sharma, S. Bhatt, "Unlocking Human Communication: A Journey through Natural Language Processing", International Journal of Engineering Trends and Applications (IJETA), Vol. 11, Issue. 3, pp. 245-250, 2024.

[6] S. A. Saiyed, N. Sharma, H. Kaushik, P. Jain, G. K. Soni and R. Joshi, "Transforming portfolio management with AI and ML: shaping investor perceptions and the future of the Indian investment sector," Parul University International Conference on Engineering and Technology 2025 (PiCET 2025), pp. 1108-1114, 2025.

[7] R. Joshi, A. Maritammanavar, "Deep Learning Architectures and Applications: A Comprehensive Survey", International Conference on Recent Trends in Engineering & Technology (ICRTET 2023), pp. 1-5, 2023.

[8] A Johari, S Gupta, R Umrainiya, "Enhancing Bank Management Systems through Salesforce Technology", International Journal of Engineering Trends and Applications (IJETA), Vol. 11, Issue. 3, pp. 97-104, 2024.

IJGRST INTERNATIONAL JOURNAL OF GLOBAL RESEARCH IN SCIENCE AND TECHNOLOGY

[9] R Ajmera, A Johari, P Sharma, P Rani, "A Novel Image Encryption Technique Using Genetic Algorithm for Enhanced Data Security", 5th International Conference on Data Science & Engineering Applications (DESA-2025), pp. 209-215, 2025.

[10] D. Shekhawat and R. Ajmera, “Survey on security implication for the downtime of VM in cloud,” in Proc. 2nd World Conf. on Smart Trends in Systems, Security and Sustainability, IEEE, Oct. 2018.

[11] R. Kawatra, D. K. Dharamdasani, R. Ajmera et al., “Internet of Things (IoT) applications, tools and security techniques,” in Proc. 2nd Int. Conf. on Advance Computing and Innovative Technologies in Engineering (ICACITE), Apr. 2022.

[12] M. K. Sain and N. Sharma, “A study of research issues and challenges of big data analytics,” Journal of Advances and Scholarly Researches in Allied Education, vol. 16, no. 5, pp. 1699–1707, 2019.

[13] A. Kumar, N. Hemrajani, "Comparative Analysis of Different Transport Layer Protocol Techniques Incognitive Network", Recent Advances in Computer Science and Communications, Bentham Science Publishers, 2024.

[14] N. Tiwari, D. Goyal, and N. Hemrajani, “A hybrid method for image watermarking,” International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), vol. 6, no. 6, pp. 894–898, 2017.

[15] P. Upadhyay, K. K. Sharma, R. Dwivedi and P. Jha, "A Statistical Machine Learning Approach to Optimize Workload in Cloud Data Centre," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), pp. 276-280, 2023.

[16] Dr. Neeraj Sharma, "Cloud Computing Architecture: Models, Services, and Deployment Strategies", International Journal of Recent Research and Review, Vol. 18, Issue. 1, pp. 209-216, 2025.

[17] P. Jha, K. K. Sharma, B. Jain, V. Sharma, " Encryption Using AES Algorithm", EIJO Journal of Engineering, Technology And Innovative Research (EIJO–JETIR), Vol. 4, Issue. 2, 2019.

[18] S. P. Chaturvedi, A. Yadav, A. Kumar, R. Mukherjee, "Unlocking IoT Security: Enabling the Future with Lightweight Cryptographic Ciphers", Intelligent Computing Techniques for Smart Energy Systems, ICTSES 2023, Lecture Notes in Electrical Engineering, Vol. 1277, pp 189–199, 2025.

IJGRST INTERNATIONAL JOURNAL OF GLOBAL RESEARCH IN SCIENCE AND TECHNOLOGY