EdinBurg Peer-Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 12||pp 1-9||November||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

Improving Cybersecurity with Artificial Intelligence

Mukunzi Thomas[1*], Djuma Sumbiri[2], Jonathan Ngugi[3]
[1,2,3]Computing and Information Sciences, University of Lay Adventists of Kigali, Rwanda
Corresponding Emails: mukmaforo@gmail.com; sumbirdj@gmail.com; phialn1@gmail.com

Accepted: 13 July 2025 || Published: 03 November 2025

Abstract

With the continued growth of the Internet of Things (IoT), the rise of connected devices poses substantial challenges to cybersecurity. The swift digital transformation across governments, businesses, and personal spheres has escalated the frequency and severity of cyberattacks, posing significant risks to individuals, organizations, and entire nations. Predictive approaches are becoming crucial in addressing these constantly evolving cyber threats before they can cause extensive harm, as conventional security strategies are inadequate. This article delves into various cyber threats, such as ransomware, phishing, malware, and denial of service (DoS) attacks, highlighting the vital role that artificial intelligence (AI) plays in fortifying cybersecurity defenses, such as intrusion detection systems, network protection, and the deployment of intelligent agents. Additionally, it discusses the importance of machine learning methods and predictive modeling in anticipating and preventing cyberattacks. While AI-driven cybersecurity offers numerous benefits, challenges related to data privacy, scalability, and human-machine collaboration remain prominent. In today's increasingly digital environment, organizations can bolster their defenses against cyberattacks and safeguard critical assets by leveraging AI-powered cybersecurity solutions.

Keywords: *Artificial intelligence, Internet of Things, Cyber-attacks, Cybersecurity*

How to Cite: Mukunzi, T., Sumbiri, D., & Ngugi, J. (2025). Improving Cybersecurity with Artificial Intelligence. *Journal of Information and Technology, 5*(12), 1-9.

1. Introduction

As the Internet of Things rapidly expands, also threat of cyberattacks continues to grow, and the importance of artificial intelligence in cybersecurity has never been greater. This paper explores various types of cyber-attacks and their evolving nature, examining how utilized to predict and mitigate these threats. Additionally, the article discusses the role of predictive modeling in cyber-attack forecasting and machine learning algorithms designed to prevent cyber threats. However, despite Artificial Intelligence's significant contribution to cybersecurity, attention must be given to the challenges and limitations associated with Artificial Intelligence, including concerns about data privacy, scalability, and collaboration between humans and machines (Aya H. Salem1*, 2014).

2. Types of cyber-attacks

A cyber-attack is a deliberate attempt by a Person or group to compromise a system's data for financial gain or to steal sensitive information from the targeted systems. Below are the main types of cyber-attacks:

Malware Attacks: These are a broad range of harmful programs created to gain unauthorized access to computer systems, often referred to as malicious software. Examples include Trojan horses, worms, viruses, and other forms of malware. Malware can be spread through malicious websites, compromised software, or infected email attachments. Once installed, steal sensitive information or malware can destroy files, also it can also take control of a system to carry out malicious actions.

Phishing Attacks: It involves deceiving individuals into disclosing sensitive data, such as credit card numbers or login credentials, by masquerading as a legitimate company. Cybercriminals often create fake websites or send convincing emails that appear genuine, tricking unsuspecting individuals into trusting them. In the financial sector, phishing attacks are particularly aimed at stealing personal or financial information from bank customers or employees without their knowledge.

Ransomware: Attackers gain access to individual or organizational data and encrypt it once a ransom is paid for recovery. Victims are left to choose whether to pay the ransom or attempt alternative methods to restore their data.

Denial of Service (DoS): DoS attacks aim to disrupt targeted networks, systems, or software by overwhelming them with excessive malicious traffic. These attacks are commonly aimed at organizations to damage their reputation, cause financial losses, and disrupt business operations.

3. The role of artificial intelligence in cybersecurity:

Artificial Intelligence (AI) is a vital element in the field of cybersecurity, reinforcing defense strategies. It plays a key role in predicting and preventing cyberattacks by processing vast volumes of data. To safeguard against cyber threats, a comprehensive approach involving various security measures across an organization’s infrastructure is essential. Below is a detailed examination of methods for preventing cyberattacks:

Network Security Measures: Security measures of the network are essential to protect an organization’s network perimeter and prevent unauthorized access to internal systems and data. These measures include:

- **Firewalls:** Firewalls are designed to effectively prevent unauthorized access to computers when they connect to the internet or other networks.
- **Encryption:** Encryption transforms data into unreadable forms, requiring the correct key to decrypt. The process of decrypting involves solving complex mathematical challenges, like factoring large prime numbers, which consumes considerable time and resources. Symmetric encryption uses keys with equal security levels for encoding and decoding messages.

Intrusion Detection: Artificial Intelligence techniques, including machine learning and deep learning, enhance intrusion detection systems (IDS) by analyzing network traffic patterns and

identifying suspicious activities indicative of a potential attack. By learning from past historical data, AI-powered IDS can detect deviations from normal system, network, or service behavior, facilitating early threat detection. These systems can continuously adapt their detection capabilities to evolving attack methods.

Intelligent Agents: Intelligent agents, which are autonomous computer-generated entities, interact and collaborate to share information and take appropriate actions when faced with unexpected events. This technology is especially useful in preventing cyberattacks due to its flexibility, cooperation, and adaptability to changing circumstances.

4. Predictive modeling for cyber-attack forecasting

A key element of artificial intelligence is predictive modeling, which identifies patterns and anomalies in data to anticipate potential cyber threats and attacks. This approach combines data and mathematical techniques to estimate future risks before they occur. Predictive modeling operates similarly to weather forecasting, predicting cyber-attacks as weather forecasts predict storms. Federated learning differs from traditional distributed machine learning by enabling multiple computing nodes in a network to share training data and collaboratively develop a machine learning model. This reduces the time needed to update models by allowing node adjustments during training. The FedAvg federated learning algorithm, tested against centralized learning using the MNIST dataset, achieved the highest accuracy, although a centralized approach worked better with non-i.i.d. data. Federated learning enhances predictive models by gathering data from multiple sources without compromising privacy, making them more effective at detecting and preventing cyber threats. The predictive modeling process includes several steps:

- **Data Collection:** Gathering relevant data from different sources, which include sensors, databases, and the internet.
- **Data Preprocessing:** a crucial step of cleaning, transforming, and organizing raw data into a usable format for analysis and modeling, also including resolving missing values, removing anomalies, and adjusting variables.
- **Feature Selection:** Choosing the most relevant variables that significantly influence the predicted outcome.
- **Model Training:** Refining the chosen model's parameters using historical data to minimize prediction errors.
- **Model Evaluation:** Assessing the trained model's accuracy and reliability with validation techniques.
- **Prediction:** Using the trained model to forecast future outcomes with fresh or untested data. Predictive modeling is used across industries to gather insights, make informed decisions, and optimize workflows. With artificial intelligence tools and historical data, Companies can identify opportunities, reduce risks, predict future trends, and enhance performance.

5. Machine learning algorithms for preventing cyber-attacks

Machine learning algorithms provide a crucial fight against cyberattacks by enabling more effective threat detection, prevention, and response, identifying patterns in network traffic and

system behavior. ML algorithms, when combined with traditional cybersecurity methods, create a multi-layered defense system against cyber threats.

By predicting the types of attacks that may occur, newer deep learning models like LSTM, RNN, and MLP help mitigate the growing complexity of cyberattacks. Noteworthy results were obtained from validating the CTF dataset, especially when an LSTM model achieved an f-measure above 93%. AI-assisted Cyber-Physical Systems (AI-CPS) can improve security in environments such as sports stadiums by predicting cyber-attacks and network irregularities. The proposed AI-CPS model, which analyzes collected data, achieves excellent prediction accuracy, promising enhanced security for sports events. Logistic regression and large language models (LLMs) are machine learning models used to detect and prevent cyber-attacks. Logistic regression is a data classification algorithm that evaluates input features and determines the likelihood of an event occurring. It is applied in various industries, including healthcare, finance, and cybersecurity, where it helps classify network traffic or system events as benign or malicious. In cybersecurity, logistic regression can classify system events based on features such as protocol type, IP address, and packet size, helping to detect potential security breaches or intrusions. Similarly, large language models (LLMs) can be valuable tools for cybersecurity, assisting in decision-making, automated detection, and augmenting human expertise. LLMs analyze data from various sources, such as threat reports and forums, to extract relevant information like malware and vulnerabilities, contributing to threat intelligence. LLMs also enhance cybersecurity by identifying suspicious web addresses, phishing emails, and malware, allowing for early intervention and preventing breaches, especially in sectors like healthcare and finance.

The distinct strengths of various types of AI are employed in versatile ways to enhance our digital protection. From straightforward solutions utilizing a single type of neural network to more sophisticated systems that integrate multiple neural networks, AI presents an array of precise and potent security tools to tackle diverse challenges. Here, we will talk about use cases where these AI-driven technologies are put to work (Laylo Bakhronkulova, 2025).

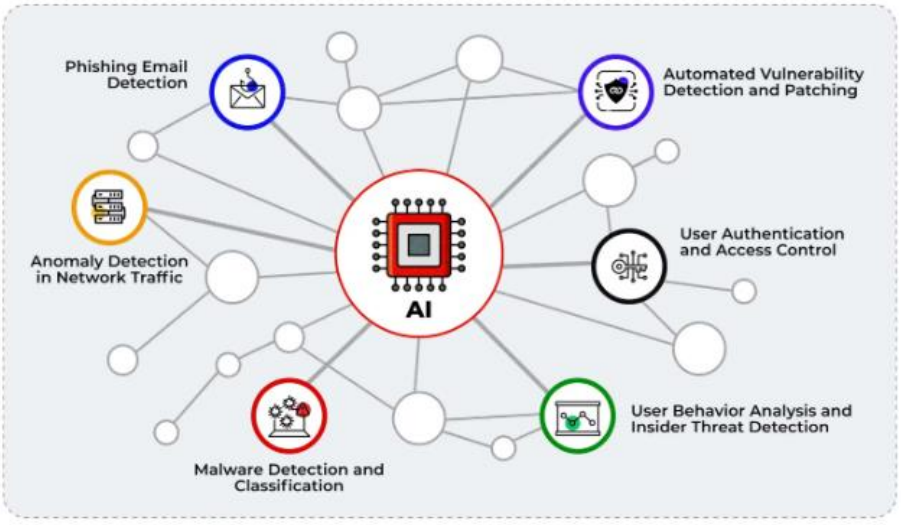

Figure 1: The use cases of AI in cybersecurity

EdinBurg Peer-Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 12||pp 1-9||November||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

6. Methodologies: Data collection

To gather background knowledge and current advancements in AI and cybersecurity. Analysis of real-world implementation of AI in cybersecurity. For example, examining how organizations use AI in malware detection and automated response systems. Conducting surveys and interviews with cybersecurity professionals, AI experts, and industry practitioners to gather insights into the practical challenges and benefits of AI-driven cybersecurity solutions.

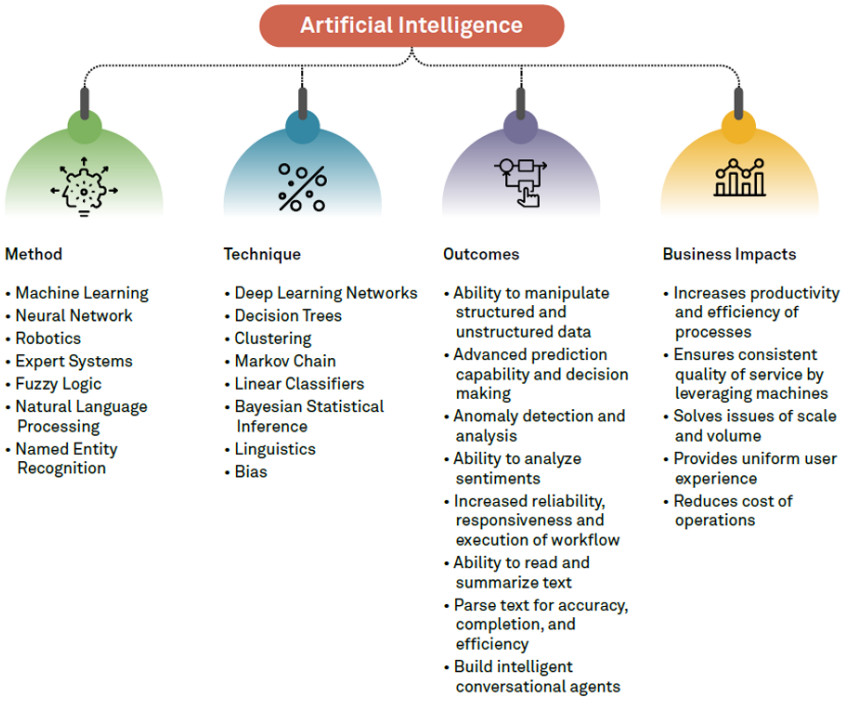

Figure 2: Methods and Techniques/Algorithms of improving cybersecurity with artificial intelligence

Machine learning (ML) techniques are increasingly vital for cyber-attack detection, offering the ability to analyze vast datasets and identify patterns indicative of malicious activity. These techniques are broadly categorized into supervised, unsupervised, and reinforcement learning, each with its own applications in cybersecurity.

Supervised Learning:

Classification:

Algorithms like Support Vector Machines (SVM), Decision Trees, and Neural Networks are trained on labeled data (e.g., network traffic with known attacks) to classify incoming data as either normal or malicious. Used to predict attack severity or duration based on historical data, enabling proactive measures. Liked detecting DoS/DDoS attacks, identifying malware, and classifying phishing emails.

Unsupervised Learning:

Anomaly Detection:

Algorithms like K-means clustering and autoencoders are used to identify unusual patterns in network traffic or system behavior that deviate from the norm, potentially indicating an attack.

Clustering: Grouping similar data points to identify potential threats or attack patterns. Like detecting unauthorized access attempts, identifying unusual network behavior, and uncovering hidden relationships between data points.

Reinforcement Learning: Dynamic Defense: Algorithms learn optimal responses to threats through trial and error, improving security strategies in real-time (Humied, 2023).

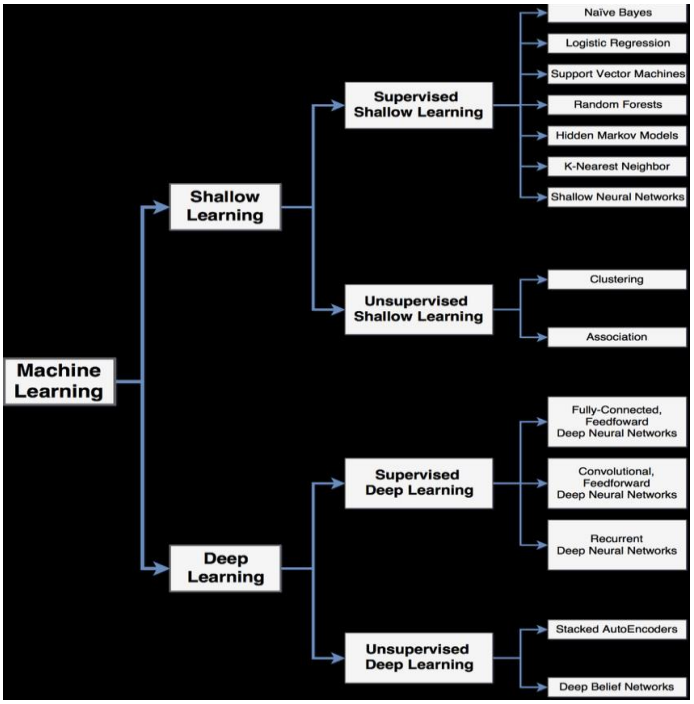

Figure 3: Classification of ML algorithms for cybersecurity applications.

7. Challenges and Limitations of AI

a. Adapting to Evolving Threats

Despite advancements in defensive strategies, organizations must still address the challenges posed by ever-changing cybersecurity threats. Cybercriminals continuously develop new methods to bypass security measures, making cyber risks ever-evolving. Organizations must stay updated with the latest threat intelligence and invest in cutting-edge security solutions to handle the increasing risks and tackle the evolving sophistication of cyber attackers.

b. Data Privacy

Many businesses rely heavily on machine learning and deep learning algorithms to extract valuable patterns and insights from data gathered by devices. However, a significant risk in this process is the transfer of sensitive data to central training locations, where it could be exposed to unauthorized access or theft by hackers, compromising the privacy of sensitive company data.

c. Scalability

Training AI algorithms requires massive amounts of data. Cybersecurity generates vast quantities of data from various sources, including user activities, system events, and network traffic. As the volume of this data increases, scalability issues can arise, making it difficult to process and analyze the ever-growing dataset efficiently.

d. Human-Machine Collaboration

While artificial intelligence (AI) significantly enhances cybersecurity defenses, it also introduces complex challenges, especially in human-machine collaboration. Incorporating AI systems into cybersecurity operations requires finding a balance between automation and human intervention. This balance is essential not only for maximizing the benefits of AI but also for avoiding the unintended outcomes that fully automated systems may produce. Effective collaboration between humans and machines ensures that AI systems serve as supportive tools for cybersecurity experts, boosting their decision-making abilities rather than replacing them. Additionally, human oversight is vital for interpreting and contextualizing alerts generated by AI, as these can lead to false positives or miss subtle details in cyber threats. By fostering a synergistic relationship between AI and human knowledge, organizations can create a more flexible, responsive, and resilient cybersecurity framework. This collaborative approach also facilitates continuous learning and refinement of AI models, as human feedback plays a critical role in fine-tuning algorithms to adapt to the evolving cyber threat landscape. Therefore, developing strategies and practices that enhance human-machine collaboration is crucial for fully realizing the potential of AI in cybersecurity while mitigating associated risks.

8. Conclusion

In conclusion, integrating artificial intelligence into cybersecurity offers significant potential to strengthen defenses against the ever-changing nature of cyber threats, particularly through predictive modeling and machine learning algorithms. However, it also brings new challenges that require ongoing research and refinement. AI has proven effective in forecasting and preventing cyberattacks, but further advancements could revolutionize cybersecurity practices.

Future studies should focus on key areas to fully unlock the potential of AI-driven cybersecurity solutions. More advanced predictive modeling techniques, driven by recent innovations in machine learning and deep learning, could enable more precise threat detection and responses. Research on real-time predictive analytics is critical, as it could offer immediate insights and counteract emerging threats. Addressing the scalability and data privacy challenges involved in training AI models on large datasets remains an important hurdle. Federated learning, which enables models to learn from decentralized data sources while preserving privacy, is a promising research avenue. Exploring secure multi-party computing and differential privacy methods could enhance the privacy-preserving features of AI in cybersecurity (Laylo Bakhronkulova, 2025).

An important area of research is the ethical use of AI in cybersecurity. It is crucial to ensure that prediction models remain unbiased and adhere to privacy standards. Research on creating transparent and explainable AI models can help alleviate these concerns, increasing trust in AI-based decisions. Integrating AI with existing cybersecurity technologies, such as intrusion detection systems and secure gateways, opens new growth opportunities. This seamless integration

could improve the responsiveness and adaptability of cybersecurity measures, leading to stronger protection against sophisticated cyberattacks.

Additionally, fostering a collaborative environment between academia and industry to exchange knowledge, data, and best practices is essential. Such partnerships could accelerate the development of successful AI-driven cybersecurity solutions, benefiting businesses worldwide. Considering these factors, the growing threat of cyberattacks requires a proactive cybersecurity approach. By leveraging AI and machine learning, along with continued research into advanced techniques and ethical considerations, businesses can strengthen their defenses against future risks. Although the path ahead is complex and challenging, it holds the promise of a safer digital world, supported by cutting-edge technology.

References

[1] Jun, A. Craig, W. Shafik, and L. Sharif, "Artificial Intelligence Application in Cybersecurity and Cyberdefense," Wireless Communications and Mobile Computing, vol. 2021, pp. 1–10, Oct. 2021, DOI: https://doi.org/10.1155/2021/3329581.

2] Mtair, "Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures," IJACSA) International Journal of Advanced Computer Science and Applications, vol. 14, no. 2, p. 2023.

[3] Dr. A. M. Shamiulla*, "Role of Artificial Intelligence in Cyber Security," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 1, pp. 4628–4630, Nov. 2019, https://doi.org/10.35940/ijitee.a6115.119119. DOI:

[4] Bécue, I. Praça, and J. Gama, "Artificial intelligence, cyber-threats pp. and Industry 4.0: challenges and opportunities," Artificial Intelligence Review, vol. 54, no. 5, 3849–3886, Feb. 2021, https://doi.org/10.1007/s10462-020-09942-2. DOI:

[5] Dilek, S., H. Cakır, and M. Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review," International Journal of Artificial Intelligence & Applications, vol. 6, no. 1, pp. 21–39, Jan. 2015, DOI: https://doi.org/10.5121/ijaia.2015.6102.

[6] Gonaygunta, D. Kumar, S. Maddini, and S. F. Rahman, "How can we make IoT Applications better with Federated Learning- A Review," IJARCCE, vol. 12, no. 2, Feb. 2023, https://doi.org/10.17148/ijarcce.2023.12213 DOI:

[7] Nilsson, S. Smith, G. Ulm, E. Gustavsson, and M. Jirstrand, "A performance evaluation of federated learning algorithms," Rennes, France: Association for Computing Machinery, 2018, pp. 1–8. DOI: https://doi.org/10.1145/3286490.3286559.

[8] Gonaygunta, D. Kumar, S. Maddini, and S. F. Rahman, "How can we make IoT Applications better with Federated Learning- A Review," IJARCCE, vol. 12, no. 2, Feb. 2023, https://doi.org/10.17148/ijarcce.2023.12213 DOI:

[9] Fredj, A. Mihoub, M. Krichen, O. Cheikhrouhou, and A. Derhab, "CyberSecurity attack prediction: A deep learning approach," Merkez,

Turkey: Association for Computing Machinery, 2021. https://doi.org/10.1145/3433174.3433614 . DOI: [10] B. Wan, C. Xu, R. P. Mahapatra, and P. Selvaraj, "Understanding the Cyber-Physical System in International Stadiums for Security in the Network from Cyber-Attacks and Adversaries using AI," Wireless Personal Communications, vol. 127, no. 2, pp. 1207- 1224, May 2021, DOI: https://doi.org/10.1007/s11277 021-08573-2.

[11] Gonaygunta, "MACHINE LEARNING ALGORITHMS TO DETECT CYBER THREATS 1 Factors Influencing the Adoption of Machine Learning Algorithms to Detect Cyber Threats in the Banking Industry," 2023.

[12] Hari Gonaygunta Using and Regression, "Article 6," International Journal of Smart Sensors and Ad Hoc Networks, vol. 3, no. 4, https://doi.org/10.47893/IJSSAN.2023.1229 DOI:

[13] Meduri, H. Gonaygunta, G. S. Nadella, P. P. Pawar, and D. Kumar, "Adaptive Intelligence: GPT-Powered Language Models for Dynamic Responses to Emerging Healthcare Challenges," IJARCCE, vol. 13, no. 1, Jan. 2024, DOI: https://doi.org/10.17148/ijarcce.2024.1311

[14] Atetedaye, Julius. (2024). Cybersecurity in the Internet of Things (IoT): Challenges and Solutions.

[15] Laylo Bakhronkulova, Muhammad Ramzan Ali, Zulfiya Khabirova, "Artificial Intelligence in Cybersecurity: Threats, Defenses, and Future Directions" © 2025 The Author(s). Published by RTU PRESS https://doi.org/10.17770/etr2025vol2.8592