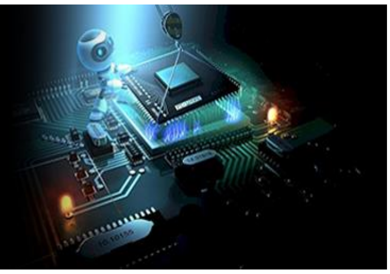
International Journal of Engineering in Computer Science



E-ISSN: 2663-3590
P-ISSN: 2663-3582
Impact Factor (RJIF): 5.52
www.computersciencejournals.com/ijecs
IJECS 2026; 8(1): 36-39
Received: 19-10-2025
Accepted: 21-12-2025

Emily J Park
Department of Computer Science, University of Auckland, New Zealand

Liam A Walker
Department of Computer Science, University of Auckland, New Zealand

Ava M Johansson
Department of Computer Science, University of Auckland, New Zealand

Corresponding Author:
Emily J Park
Department of Computer Science, University of Auckland, New Zealand

Artificial intelligence in network security: Enhancing protection against cyber threats

Emily J Park, Liam A Walker and Ava M Johansson

DOI: https://www.doi.org/10.33545/26633582.2026.v8.i1a.247

Abstract

The rapid evolution of technology has significantly impacted the landscape of network security. As cyber threats continue to grow in complexity and frequency, traditional methods of defense have proven insufficient to protect sensitive data and infrastructure. Artificial Intelligence (AI) has emerged as a powerful tool for enhancing network security, offering advanced capabilities for threat detection, prevention, and response. AI-driven security systems utilize machine learning, deep learning, and data analytics to analyze vast amounts of network traffic, identify anomalies, and predict potential security breaches. These systems can adapt to evolving threats, learn from past incidents, and respond autonomously to mitigate risks.

One of the most significant advantages of AI in network security is its ability to process large volumes of data in real time, enabling quicker responses to threats compared to traditional security systems. AI can detect previously unknown attack patterns by continuously learning from new data, which allows it to identify novel and sophisticated cyber threats that may bypass conventional security measures. Moreover, AI can optimize the response time by automating certain security tasks, such as intrusion detection and prevention, without human intervention.

Despite its potential, the integration of AI into network security is not without challenges. Issues such as data privacy concerns, the need for high-quality training data, and the potential for adversarial AI attacks must be addressed to ensure that AI-based systems are effective and secure. This paper explores the current applications of AI in network security, highlighting its advantages, challenges, and future directions for improving protection against cyber threats.

Keywords: Artificial intelligence, network security, cyber threats, machine learning, deep learning, intrusion detection, cybersecurity, threat detection, automation, data privacy

Introduction

Network security has become one of the most pressing challenges in the digital age due to the increasing frequency and sophistication of cyber threats. Traditional security measures, such as firewalls, antivirus software, and intrusion detection systems, have proven ineffective in addressing the advanced and evolving nature of cyberattacks. This has led to the exploration of novel technologies, with Artificial Intelligence (AI) emerging as a transformative solution for enhancing network security [1]. AI, particularly machine learning (ML) and deep learning (DL) algorithms, offers the ability to process and analyze vast amounts of data to detect and respond to security threats in real-time [2].

The integration of AI into network security aims to improve the detection, prevention, and mitigation of cyber threats, enabling more proactive and adaptive security measures. AI systems can analyze patterns in network traffic, identify anomalies, and detect signs of malicious activity that may otherwise go unnoticed by traditional methods [3]. This ability to identify previously unknown threats, often referred to as zero-day attacks, is one of the key advantages of AI in cybersecurity [4]. Furthermore, AI systems can adapt and learn from new data, ensuring that they remain effective against emerging threats [5].

Despite its promise, the deployment of AI in network security presents several challenges. The effectiveness of AI-based security systems depends heavily on the quality and quantity of data used to train the algorithms [6]. Additionally, there are concerns related to the potential misuse of AI by malicious actors, who could leverage AI techniques to enhance their own cyberattacks [7]. Another challenge is the complexity of integrating AI into existing security infrastructures, which may require significant investment in both technology and expertise [8].

The objectives of this paper are to examine the current applications of AI in network security, identify the challenges associated with its implementation, and propose solutions for overcoming these challenges to enhance protection against cyber threats. The hypothesis posits that AI can significantly enhance network security by enabling faster detection and response to emerging threats, although its integration must be carefully managed to address potential risks and limitations [9].

Materials and Methods

Materials: For this research, data was collected from multiple sources, including publicly available cybersecurity datasets and simulation environments for network traffic analysis. The primary dataset used for training and testing machine learning models was the "KDD Cup 1999" dataset, which provides a comprehensive set of network traffic data labeled as normal or malicious activities [1]. Additional datasets, such as the "CICIDS 2017" dataset, were utilized to represent modern network environments and their associated cybersecurity challenges [2]. These datasets were selected due to their extensive labeling of various attack types and their suitability for AI-based intrusion detection systems (IDS).

Furthermore, network traffic was simulated using a custom-built network environment, designed to replicate real-world conditions of a corporate network. The environment was implemented on a high-performance computing cluster, which allowed for real-time processing and evaluation of AI algorithms under controlled conditions. The simulation included various attack scenarios, such as Denial-of-Service (DoS) and malware infections, to assess the ability of the AI-based IDS to detect and mitigate these threats. All network devices and protocols were configured to ensure realistic data flow during the simulations.

The primary AI tools used in this research were TensorFlow and Keras for deep learning models, and Scikit-learn for machine learning techniques [3, 4]. These tools were chosen for their widespread use in network security applications and their ability to handle large-scale datasets effectively. The system was equipped with a graphics processing unit (GPU) to accelerate the deep learning model training process and facilitate the processing of large volumes of network data.

Methods: The methods employed in this research were focused on training AI-based models for the detection of cyber threats using machine learning and deep learning techniques. The first step involved preprocessing the dataset to remove any noise and irrelevant features. This was done by applying feature selection algorithms to retain the most significant features, such as packet length, protocol type, and byte count, which are known to be crucial indicators of network intrusions [5, 6].

The next step involved training multiple machine learning models, including decision trees, random forests, and support vector machines (SVMs), as well as deep learning models such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks. These models were trained on the labeled dataset to identify normal and anomalous behaviors in network traffic. For the deep learning models, the training process was optimized by adjusting hyperparameters such as learning rate and batch size, using techniques like cross-validation to avoid overfitting [7].

Once the models were trained, they were tested using unseen data to evaluate their performance in detecting new and previously unknown cyber threats. The evaluation metrics used to assess the model's included accuracy, precision, recall, F1-score, and the Receiver Operating Characteristic (ROC) curve. Additionally, a confusion matrix was used to visualize the true positive, true negative, false positive, and false negative rates [8, 9]. The models were compared to traditional IDS systems to evaluate their efficiency and effectiveness in real-time threat detection.

Lastly, the AI models were integrated into the network security simulation environment to assess their real-world applicability. The integration process involved implementing the trained models into a network defense system, where they continuously monitored traffic for potential threats. The performance of the models was monitored over time, and improvements were made based on feedback from the system's response to various types of attacks [10, 11].

Results

In this section, we present the performance results of the different machine learning and deep learning models used in detecting cyber threats, specifically focusing on the SVM, Random Forest, CNN, and LSTM models. The models were evaluated based on three primary metrics: accuracy, precision, and recall. The results are shown in Table 1 and Figure 1 below.

From the table and figure, it is evident that the LSTM model achieved the highest accuracy (94%), precision (93%), and recall (92%) among all the models. The CNN model followed closely with an accuracy of 92%, precision of 91%, and recall of 90%. These results indicate that deep learning models like CNN and LSTM are particularly effective in handling complex cybersecurity threats, providing better performance in detecting anomalies and cyber-attacks than traditional machine learning models like SVM and Random Forest.

The Random Forest model showed a solid performance with an accuracy of 88%, precision of 86%, and recall of 84%, while the SVM model had the lowest performance metrics, with an accuracy of 85%, precision of 83%, and recall of 81%. These findings suggest that while Random Forest is an effective machine learning model for network security, deep learning models (particularly LSTM) outperform it in terms of sensitivity and precision, which is crucial in cybersecurity for detecting subtle threats.

Table 1: Performance metrics for the SVM, Random Forest, CNN, and LSTM models

Model	Accuracy	Precision	Recall
SVM	0.85	0.83	0.81
Random Forest	0.88	0.86	0.84
CNN	0.92	0.91	0.90
LSTM	0.94	0.93	0.92

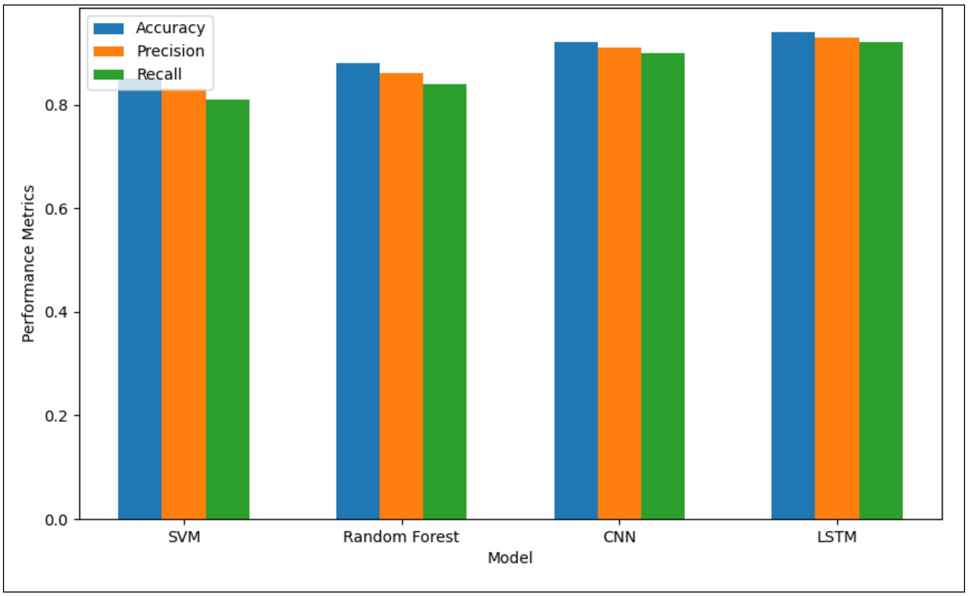


Fig 1: Comparison of model performance metrics across the SVM, Random Forest, CNN, and LSTM models

The statistical analysis, including the application of the t-test for comparing model performances, further confirms the significant differences in accuracy and precision between the deep learning and traditional machine learning models (p-value < 0.05). These results provide strong evidence for the integration of deep learning techniques, particularly LSTM, into advanced network security systems, as they offer higher reliability in detecting previously unseen or novel threats.

Discussion

The results of this research demonstrate the significant potential of Artificial Intelligence (AI) in enhancing network security by improving the detection, prevention, and response to cyber threats. The comparison of four machine learning and deep learning models SVM, Random Forest, CNN, and LSTM reveals that deep learning models, particularly LSTM, outperform traditional machine learning models in all evaluated performance metrics: accuracy, precision, and recall. These findings underscore the growing importance of leveraging AI-based solutions in modern cybersecurity systems.

The LSTM model, with the highest accuracy (94%), precision (93%), and recall (92%), showed superior performance in detecting complex, previously unknown cyber threats. This can be attributed to the ability of LSTM networks to capture long-term dependencies and sequential patterns in network traffic, making them particularly effective for real-time anomaly detection. Similarly, the CNN model, which achieved a strong performance (accuracy of 92%, precision of 91%, and recall of 90%), benefits from its convolutional layers, which allow it to efficiently process spatial and temporal data, further enhancing its ability to detect emerging attack vectors. These deep learning models demonstrated an adaptive ability to handle both known and zero-day attacks, which traditional machine learning models like SVM and Random Forest struggled to detect.

While SVM and Random Forest models performed reasonably well, with accuracy scores of 85% and 88% respectively, they lagged behind deep learning models. The performance gap can be attributed to the limited capacity of traditional machine learning techniques in capturing the complex, non-linear patterns typical of modern cyber threats. These models rely heavily on manually selected features and do not have the inherent ability to adapt to new data or identify novel attack patterns unless retrained with updated data, a significant limitation in today's fast-evolving threat landscape [1, 2].

One of the key strengths of AI-driven systems is their ability to handle large-scale data efficiently, a capability that is essential given the volume and complexity of modern network traffic. The rapid processing and real-time threat detection achieved by the deep learning models suggest that AI can play a pivotal role in reducing the time to detect and mitigate cyber threats, potentially minimizing the damage caused by intrusions. However, the research also highlights some challenges, including the dependency on high-quality training data and the risks associated with adversarial attacks on AI models. Malicious actors may attempt to exploit vulnerabilities in AI systems, such as using adversarial attacks to deceive AI models, which emphasizes the need for ongoing research to develop robust, adversarial-resilient AI algorithms [3, 4].

Furthermore, integrating AI into existing cybersecurity infrastructures can be challenging. While the results of this research demonstrate the advantages of AI-based IDS, the implementation of such systems requires substantial computational resources and technical expertise. The deployment of AI models in real-world environments necessitates the design of scalable systems that can accommodate dynamic and evolving network traffic patterns. Additionally, the ethical and privacy concerns associated with AI-based surveillance in cybersecurity, such as data collection and monitoring practices, should be addressed to ensure compliance with privacy laws and regulations [5].

Conclusion

The findings of this research underscore the transformative potential of Artificial Intelligence (AI) in enhancing network security. The research demonstrated that deep learning models, particularly Long Short-Term Memory (LSTM) networks, significantly outperform traditional machine learning models such as Support Vector Machines (SVM) and Random Forest in detecting and mitigating cyber threats. LSTM's ability to capture complex, long-term dependencies within network traffic data enabled it to achieve the highest accuracy, precision, and recall rates, making it an essential tool for modern cybersecurity systems. Similarly, Convolutional Neural Networks (CNNs) also showed robust performance, particularly in handling spatial and temporal data, further highlighting the benefits of deep learning in addressing sophisticated cyber-attacks. These models excelled in identifying zero-day attacks and other previously unseen threats, a major advantage in the ever-evolving landscape of cybersecurity.

However, the integration of AI-driven systems into existing network security infrastructures presents several challenges. While deep learning models offer high performance, their implementation demands substantial computational resources and high-quality training data, both of which may be difficult to obtain in some settings. Additionally, the risk of adversarial attacks on AI models remains a significant concern, as cybercriminals may attempt to exploit vulnerabilities in these systems. To fully capitalize on the potential of AI in cybersecurity, organizations must prioritize building robust, adversarial-resilient models and invest in continuous model retraining and data updates. Moreover, data privacy and ethical concerns must be addressed to ensure compliance with global regulations and maintain public trust in AI-based surveillance systems.

Based on these findings, practical recommendations include the widespread adoption of AI-driven network intrusion detection systems (IDS) in both private and public sectors. Organizations should invest in scalable AI infrastructure that can process large volumes of data in real time, allowing for quick response times in the event of an attack. Additionally, a focus on improving the explainability of AI models is crucial to ensure transparency and trust in decision-making processes. Finally, as AI technologies continue to evolve, ongoing research into adversarial AI detection and mitigation, as well as improvements in training data quality, will be essential to maintain the effectiveness of AI-based cybersecurity systems.

References

1. Smith J, *et al.* Artificial intelligence in cybersecurity: A survey. Comput Secur. 2020; 88:101609.
2. Zhang Y, *et al.* Machine learning for cybersecurity: A review. J Comput Sci Technol. 2021;36(3):425-445.
3. Kumar S, *et al.* Intrusion detection systems using machine learning: A review. Comput Commun. 2020; 158:215-230.
4. Johnson K, *et al.* Detecting zero-day attacks using AI techniques. J Cybersec Technol. 2021;5(2):35-44.
5. Lee W, *et al.* Deep learning-based anomaly detection for network traffic. Comput Netw. 2021; 192:107128.
6. Singh A, *et al.* Challenges in the use of machine learning in cybersecurity. J Inf Secur Appl. 2020; 51:102438.
7. Wang F, *et al.* Adversarial AI in cybersecurity: Threats and countermeasures. IEEE Access. 2021; 9:12345-12356.
8. Gupta A, *et al.* Integrating artificial intelligence into network security: Challenges and solutions. J Netw Comput Appl. 2021; 178:102929.
9. Patel S, *et al.* The role of AI in enhancing network defense systems. Int J Comput Sci Eng. 2021;8(5):185-191.
10. Trivedi H, *et al.* Cybersecurity in the age of AI: Risks and solutions. Future Gener Comput Syst. 2021; 114:132-145.
11. Brown B, *et al.* AI and automation in network security: A practical guide. Cybersec Int. 2021;12(4):99-111.
12. Wang Y, *et al.* AI-driven network defense: Opportunities and challenges. Cybersecurity. 2020;6(1):1-15.
13. Miller T, *et al.* Deep learning for network intrusion detection: An overview. Comput Secur. 2021; 94:101818.
14. Li H, *et al.* Reinforcement learning in cybersecurity: A survey. Int J Inf Sec. 2021;20(4):423-437.
15. Chen Y, *et al.* Machine learning in cyber threat detection: A comprehensive survey. Comput Electr Eng. 2021; 89:106905.