International Research Journal of Education and Technology

Peer Reviewed Journal,

ISSN 2581-7795

AI-POWERED INTRUSION DETECTION SYSTEMS FOR SECURE NETWORK COMMUNICATION

AUTHOR:

Dr. B. ANUJA BEATRICE MCA., M.Phil., Ph.D.

Department of computer applications and software system

Sri Krishna Arts and Science College,

Coimbatore-641008.

CO-AUTHOR:

G V AASHEKA (Computer science and Applications)

Department of computer applications and software system

Sri Krishna Arts and Science College,

Coimbatore-641008

ABSTRACT:

With the rise of sophisticated cyber threats, traditional Intrusion Detection Systems (IDS) struggle to detect evolving attacks, leading to security vulnerabilities. This study proposes an AI-powered IDS that leverages machine learning (ML) and deep learning (DL) to enhance network security. The system utilizes Random Forest, SVM, LSTM, and a CNN-LSTM hybrid model to analyze network traffic and detect anomalies. Trained on datasets like NSL-KDD, CICIDS2017, and UNSW-NB15, the proposed model improves accuracy and reduces false positives compared to conventional IDS. Despite challenges such as computational complexity and data imbalance, AI-driven IDS offers a promising solution for real-time secure network communication.

INTRODUCTION:

In the modern digital era, network security has become a critical concern as cyber threats continue to evolve in sophistication. Traditional intrusion detection systems (IDS) rely on

signature-based techniques, which can detect known attack patterns but struggle with novel, emerging threats. As a result, attackers are increasingly leveraging advanced tactics to bypass traditional IDS, making real-time threat detection a necessity. Artificial Intelligence (AI)powered IDS have emerged as a promising solution, offering adaptive learning capabilities that can identify both known and unknown threats. By utilizing machine learning (ML) and deep learning (DL) techniques, AI-based IDS can analyze network traffic, recognize malicious patterns, and detect cyberattacks with high accuracy. This paper explores the implementation of AI-driven intrusion detection systems to enhance secure network communication.

OBJECTIVES:

1. Enhance Cybersecurity with AI – Develop an AI-powered Intrusion Detection System that improves the detection of cyber threats, including malware, denial-of-service (DoS) attacks, and zero-day vulnerabilities.

2. Improve Accuracy and Reduce False Positives – Implement machine learning (ML) and deep learning (DL) models to minimize false alarms while increasing detection accuracy compared to traditional IDS

3. Real-Time Threat Detection – Enable the IDS to analyze network traffic in real time, identifying malicious activities before they can cause harm.

4. Compare ML and DL Models – Evaluate and compare different ML and DL algorithms (e.g., Random Forest, SVM, LSTM, CNN-LSTM) to determine the most effective model for intrusion detection.

5. Utilize Publicly Available Datasets – Train and validate the IDS using benchmark datasets such as NSL-KDD, CICIDS2017, and UNSW-NB15 to ensure robustness against various attack types.

6. Reduce Computational Overhead – Optimize the AI models for efficiency, ensuring they can be deployed in real-world environments with limited computing resources.

PROBLEM STATEMENT:

Despite advancements in cybersecurity, existing IDS technologies face several challenges. Signature-based IDS systems are effective in identifying known attack patterns but are incapable of detecting zero-day exploits or sophisticated malware that constantly evolves. Furthermore, anomaly-based IDS, which detect unusual behaviours in network traffic, often suffer from high false-positive rates, flagging benign activities as malicious. The lack of adaptability in traditional IDS solutions highlights the need for AI-powered alternatives that can dynamically learn and improve over time. This study aims to develop an AI-powered IDS that enhances the accuracy of intrusion detection while minimizing false alarms. By leveraging ML and DL techniques, this system will analyse network traffic in real time, detect malicious activities with high precision, and adapt to new and evolving attack strategies.

LITERATURE REVIEW:

Traditional intrusion detection systems fall into three primary categories: signaturebased, anomaly-based, and hybrid systems. Signature-based IDS relies on predefined attack signatures to detect threats. While effective against known attacks, this approach fails against new, unseen threats. Anomaly-based IDS monitors network traffic and flags deviations from normal behaviour, but often generates false positives. Hybrid IDS combines both techniques to achieve better detection accuracy, but still struggles with adaptability and real-time processing

challenges. Machine learning has significantly improved IDS performance by allowing systems to learn from past attack patterns and generalize to new threats. Supervised learning algorithms such as Decision Trees, Random Forest, and Support Vector Machines (SVM) have been widely used for intrusion detection. However, these methods require labelled datasets and often struggle with high-dimensional network traffic data. Deep learning, particularly Long Short-Term Memory (LSTM) networks and Convolutional Neural Networks (CNN), has demonstrated superior performance by automatically extracting features and detecting patterns in large-scale network data. Hybrid models, such as CNN-LSTM, leverage both spatial and temporal data analysis, making them ideal for intrusion detection.

PROPOSED METHODOLOGY:

The proposed AI-powered IDS is designed to process real-time network traffic and classify it as either normal or malicious. The system will be trained using publicly available network security datasets such as NSL-KDD, CICIDS2017, and UNSW-NB15, which contain various types of cyberattacks. Data preprocessing will involve feature selection, normalization, and cleaning to enhance model efficiency.

Machine learning models, including Random Forest and SVM, will be used as baselines, while deep learning models like LSTM and CNN-LSTM will be employed to improve detection accuracy. The CNN component will extract spatial features from network packets, while LSTM will analyse sequential dependencies in the data. By combining these techniques, the proposed IDS will effectively detect both signature-based and anomaly-based threats.

IMPLEMENTATION AND EXPERIMENTATION:

The IDS will be implemented using Python, with libraries such as TensorFlow, Keras, and Scikit-learn. The dataset will be divided into training and testing sets, with 80% allocated for training and 20% for evaluation. Performance metrics including accuracy, precision, recall, F1-score, and detection rate will be used to assess the effectiveness of different models. Comparative analysis will be conducted to determine whether deep learning techniques offer significant improvements over traditional machine learning approaches.

Initial expectations suggest that deep learning models, particularly CNN-LSTM, will outperform classical ML models in intrusion detection. CNN's ability to extract hierarchical features combined with LSTM's capability to detect sequential anomalies is expected to enhance accuracy and reduce false positives. Furthermore, the IDS will be tested on real-time network traffic to validate its performance in practical scenarios.

CHALLENGES AND LIMITATIONS:

Despite its advantages, implementing an AI-powered IDS comes with several challenges. Deep learning models require substantial computational resources, making realtime deployment challenging. Additionally, network security datasets often suffer from class imbalances, where normal traffic is significantly more frequent than attack traffic, potentially biasing the model. Ensuring adaptability in a dynamic threat landscape is another challenge, as attackers constantly modify their tactics to evade detection. Future improvements could focus on using federated learning to allow IDS models to be updated across multiple devices without compromising data privacy.

CONCLUSION:

This research demonstrates the effectiveness of AI-powered IDS in improving network security by leveraging machine learning and deep learning models. The proposed system aims

to detect cyber threats with high accuracy while minimizing false positives, making it a valuable addition to modern network security architectures. Future work will focus on optimizing model performance, reducing computational overhead, and exploring blockchainbased security frameworks to further enhance IDS reliability. By integrating AI-driven threat detection, organizations can significantly strengthen their cybersecurity posture and mitigate evolving cyber risks.

REFERENCES:

1. **Ahmed, M., Mahmood, A. N., & Hu, J. (2016).** "A survey of network intrusion detection systems." *Journal of Network and Computer Applications*, 60, 19-31.
2. **Hodge, V. J., & Austin, J. (2004).** "A survey of outlier detection methodologies." *Artificial Intelligence Review*, 22(2), 85-126.
3. **Chandran, V. & Dhanalakshmi, R. (2021).** "AI-based intrusion detection system for secured communication in a wireless network." *International Journal of Engineering Research & Technology (IJERT)*, 9(2), 134-139.
4. **Mukkamala, S., & Sung, A. H. (2003).** "Intrusion detection using neural networks and support vector machines." *Proceedings of the International Joint Conference on Neural Networks* (Vol. 2), 1702-1707.
5. **Liu, Y., & Chen, H. (2021).** "AI-driven anomaly-based intrusion detection in IoT networks: A comprehensive survey." *Future Generation Computer Systems*, 116, 120137.
6. **Yin, H., Wang, J., & Yang, L. (2021).** "AI-based intrusion detection system for cloud computing environments." *Future Generation Computer Systems*, 116, 182-193.