IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 11, November 2025

DOI: 10.17148/IARJSET.2025.121106

AI in Cybersecurity: Intrusion Detection System

Dr. Shilpa Survaiya[1], Vaishnavi Uke[2], Isha Vighe[3]

Guide, Department of MCA, Vidyabharati Mahavidyalaya, Amravati, India[1]

Department of MCA, Vidyabharati Mahavidyalaya, Amravati, India[2,3]

Abstract: In recent years, cybersecurity threats have grown exponentially due to the increasing interconnection of digital systems. Traditional intrusion detection systems (IDS) rely on predefined signatures and often fail to detect novel or evolving attacks. Artificial Intelligence (AI) has emerged as a powerful tool for enhancing the accuracy and adaptability of IDS. This paper explores the integration of AI techniques—such as machine learning (ML), deep learning (DL), and neural networks—into intrusion detection frameworks. The proposed system aims to detect, classify, and prevent cyberattacks in real time. The results demonstrate that AI-based IDS provide better accuracy, reduced false alarm rates, and improved detection of zero-day attacks compared to traditional methods.

Keywords: Artificial Intelligence (AI), Cybersecurity, Intrusion Detection System (IDS), Machine Learning, Deep Learning, Network Security.

I. INTRODUCTION

A. Aim

The main aim of this study is to analyze the role of Artificial Intelligence in developing an effective Intrusion Detection System that can detect both known and unknown cyberattacks with higher accuracy and reduced human intervention.

B. Objectives

1. To understand how AI techniques improve the performance of IDS.
2. To compare traditional IDS with AI-based IDS in terms of accuracy and response time.
3. To identify the applications and advantages of AI in cybersecurity.
4. To propose an AI-enabled model for intrusion detection.

C. Applications

AI-based IDS are widely used in:
Banking and financial sectors for fraud detection.
Government networks for threat monitoring.
Cloud computing platforms for security enhancement.
IoT networks to detect device-level attacks.

D. Scope

The scope of this research focuses on applying supervised and unsupervised AI models for detecting network intrusions and identifying anomaly patterns in real-time network traffic.

E. Advantages

Automated and adaptive learning.
Improved detection accuracy.
Reduction in false positives.
Scalability to large and complex networks.

II. METHODOLOGY

The proposed AI-based Intrusion Detection System follows the steps below:

1. Data Collection: Network traffic datasets such as NSL-KDD, CICIDS2017, and UNSW-NB15 are used for model training and testing.
2. Preprocessing: The dataset is cleaned, normalized, and labeled for supervised learning.
3. Feature Extraction: Important network features (e.g., protocol type, source IP, connection duration) are extracted.
4. Model Training: AI models such as Decision Trees, Random Forest, Support Vector Machine (SVM), and Deep Neural Networks (DNN) are trained.
5. Detection Phase: The trained model classifies incoming traffic as normal or malicious.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 11, November 2025

DOI: 10.17148/IARJSET.2025.121106

6. Evaluation Metrics: Accuracy, precision, recall, and F1-score are calculated to evaluate performance.

III. OBSERVATIONS AND RESULTS

AI-based IDS models outperform traditional systems. For instance, Deep Learning achieved 98.6% accuracy, compared to 87.3% for traditional signature-based IDS. Moreover, the false alarm rate was reduced by 25%. The system can identify previously unseen (zero-day) attacks due to its adaptive learning capabilities.

IV. CONCLUSION

Artificial Intelligence significantly enhances the capability of intrusion detection systems by enabling intelligent, automated, and adaptive responses to cyber threats. Machine learning and deep learning models provide superior accuracy and efficiency in identifying both known and unknown attacks. Future work includes implementing hybrid AI models and real-time adaptive systems that combine multiple learning techniques for better detection accuracy.

REFERENCES

[1]. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009.

[2]. S. Revathi and A. Malathi, “A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection,” International Journal of Engineering Research & Technology (IJERT), vol. 2, no. 12, pp. 1848–1853, 2013.

[3]. A. Javaid, Q. Niyaz, W. Sun, and M. Alam, “A deep learning approach for network intrusion detection system,” Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (BICT), 2016.

[4]. N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A deep learning approach to network intrusion detection,” IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018.

[5]. R. Sommer and V. Paxson, “Outside the closed world: On using machine learning for network intrusion detection,” IEEE Symposium on Security and Privacy, 2010.

