AI-Powered Intrusion Detection System Using Deep Learning in Cybersecurity

Dr. Arjun Menon [1*], Dr. Rajesh Gupta [2]
[1] School of Computational Sciences, Indian Institute of Science (IISc), India
[2] Department of Computer Science, Indian Institute of Technology Bombay (IITB), India

* Corresponding Author: **Dr. Arjun Menon**

Article Info

Volume: 01
Issue: 01
January-February 2025
Received: 26-01-2025
Accepted: 20-02-2025
Page No: 12-14

Abstract
With the exponential growth of networked systems and digital assets, cybersecurity threats have become increasingly sophisticated, posing significant risks to organizations and individuals alike. Traditional intrusion detection systems (IDS) struggle to keep pace with evolving attack vectors and the sheer volume of network traffic. Artificial Intelligence (AI), particularly deep learning, offers powerful tools for automating and enhancing intrusion detection. This paper surveys the design, implementation, and effectiveness of AI-powered intrusion detection systems using deep learning in cybersecurity. We discuss popular deep learning architectures, datasets, implementation strategies, challenges, and future directions, supported by recent research and empirical results.

Keywords: AI-powered intrusion detection systems, Deep learning in cybersecurity, Anomaly-based intrusion detection, Network security with machine learning, Adversarial attack detection

1. Introduction

In the digital era, safeguarding sensitive data and critical infrastructure from cyber threats is more important than ever. Intrusion Detection Systems (IDS) are essential components of a comprehensive cybersecurity strategy, monitoring network traffic and system activities for signs of malicious behavior. However, the dynamic nature of cyber-attacks, including zero-day exploits and advanced persistent threats, often renders traditional, signature-based IDS insufficient5.

AI-powered IDS, leveraging machine learning (ML) and deep learning (DL) techniques, have emerged as a promising solution. These systems can learn complex patterns from vast amounts of data, adapt to new threats, and reduce false positives, making them highly effective for modern cybersecurity needs124.

2. Traditional vs. AI-Powered Intrusion Detection Systems

2.1 Traditional IDS

Traditional IDS can be classified into:

- **Signature-Based IDS:** Detects known threats by matching patterns or signatures. Efficient for known attacks but ineffective against novel threats.
- **Anomaly-Based IDS:** Identifies deviations from normal behavior. Can detect unknown attacks but often suffers from high false positive rates.

2.2 AI and Deep Learning in IDS

AI-powered IDS use ML and DL algorithms to automatically learn and identify both known and unknown threats. Deep learning models, such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Deep Neural Networks (DNN), can extract hierarchical features from raw data and recognize complex attack patterns145.

3. Deep Learning Architectures for Intrusion Detection

3.1 Convolutional Neural Networks (CNN)

CNNs are adept at capturing spatial features in data. In IDS, CNNs can process network traffic as structured data, learning to detect intrusions without manual feature engineering. Studies show that CNN-based IDS achieve high accuracy, especially

in identifying subtle attack patterns in large datasets12.

3.2 Deep Neural Networks (DNN)
DNNs, with multiple hidden layers, can model complex, non-linear relationships in network traffic. They have been successfully applied to both binary and multi-class intrusion detection tasks, often outperforming traditional ML models in accuracy and robustness13.

3.3 Long Short-Term Memory (LSTM) Networks
LSTM networks are a type of recurrent neural network (RNN) designed to capture temporal dependencies in sequential data. In cybersecurity, LSTM-based IDS can analyze sequences of network events, making them effective for detecting sophisticated attacks that unfold over time45.

3.4 Hybrid and Ensemble Models
Combining different deep learning models or integrating them with optimization algorithms (e.g., Genetic Algorithms, Artificial Bee Colony) can further enhance detection rates and reduce false positives. Hybrid models leverage the strengths of multiple techniques for improved performance12.

4. Datasets for Training and Evaluation
High-quality datasets are crucial for developing and benchmarking IDS. Commonly used datasets include:

- **KDD Cup 99 and NSL-KDD:** Benchmark datasets for IDS research, though criticized for outdated attack types and data redundancy.
- **UNSW-NB15:** Contains contemporary attack scenarios and diverse features, offering a more realistic evaluation environment1.
- **CIC-IDS2017 and CSE-CIC-IDS2018:** Modern datasets capturing various attack types and normal traffic in realistic settings1.

Using diverse and up-to-date datasets ensures that IDS models generalize well and remain effective against emerging threats.

5. Implementation Strategies
5.1 Data Preprocessing
Preprocessing steps include:

- **Data Cleaning:** Removing duplicates and handling missing values.
- **Feature Selection:** Identifying relevant features using statistical or optimization techniques.
- **Normalization:** Scaling features to a standard range to improve model convergence12.

5.2 Model Training and Evaluation
Deep learning models are trained using labeled data, with performance evaluated on metrics such as accuracy, precision, recall, F1-score, and false positive rate. Cross-validation and hyperparameter tuning are essential for robust results134.

5.3 Deployment
IDS can be deployed as:

- **Host-Based IDS (HIDS):** Monitors activities on individual systems.
- **Network-Based IDS (NIDS):** Analyzes network traffic for suspicious patterns.

Cloud-based and edge-based deployments are increasingly popular, enabling scalable and real-time intrusion detection24.

6. Case Studies and Experimental Results
6.1 CNN-Based IDS
Arun *et al*. proposed a CNN-based IDS that achieved high precision in detecting complex attack patterns using the UNSW-NB15 dataset. The system demonstrated significant improvements in accuracy and robustness compared to traditional methods, highlighting the value of deep learning in real-world cybersecurity applications1.

6.2 DNN for IoT Security
Khan *et al*. developed a DNN-based IDS for MQTT-enabled IoT systems, achieving 99% accuracy for binary and 98% for multi-class attack classification. The model outperformed conventional ML algorithms, demonstrating the potential of deep learning for securing IoT environments1.

6.3 Hybrid Models
Gulia *et al*. introduced a hybrid IDS combining the Group-Artificial Bee Colony (G-ABC) algorithm for feature selection with a DNN for classification. Tested in cloud computing environments, the system achieved a 96% detection rate, showcasing the benefits of integrating optimization and deep learning techniques1.

6.4 Multi-Agent and Ensemble Approaches
Louati and Ktata proposed a deep learning-based multi-agent system using autoencoders, MLP, and KNN classifiers, achieving 99.95% accuracy on the KDD Cup 99 dataset. Such ensemble approaches can further enhance detection rates and adaptability1.

6.5 LSTM and MLP for DDoS Detection
Abdulrahman *et al*. and Alkahtani & Aldhyani demonstrated the effectiveness of MLP and LSTM models in detecting DDoS and other attacks, with LSTM achieving up to 99.82% accuracy on IoT datasets14.

7. Advantages of Deep Learning in IDS

- **High Accuracy:** Deep models can capture complex, non-linear attack patterns145.
- **Automated Feature Extraction:** Reduces reliance on manual feature engineering.
- **Adaptability:** Models can be retrained or fine-tuned as new threats emerge.
- **Reduced False Positives:** Advanced models can better distinguish between benign and malicious activities.

8. Challenges and Limitations
8.1 Data Quality and Availability
IDS performance depends on the quality and representativeness of training data. Many public datasets are outdated or lack diversity, limiting real-world applicability14.

8.2 Model Interpretability
Deep learning models are often seen as "black boxes," making it difficult to explain decisions to security analysts or

comply with regulatory requirements 45.

8.3 Computational Requirements
Training and deploying deep models require significant computational resources, which may be challenging for real-time or resource-constrained environments 23.

8.4 Adversarial Attacks
Deep learning models are vulnerable to adversarial examples—maliciously crafted inputs that can evade detection. Robustness to such attacks remains an active research area4.

9. Future Directions
9.1 Explainable AI (XAI)
Developing interpretable deep learning models will enhance trust and facilitate adoption in critical security applications45.

9.2 Online and Incremental Learning
Real-time IDS require models that can learn from new data on the fly, adapting to evolving threats without retraining from scratch4.

9.3 Integration with Other Security Tools
AI-powered IDS can be integrated with Security Information and Event Management (SIEM) systems, firewalls, and endpoint protection for holistic defense25.

9.4 Federated and Edge Learning
Federated learning and edge computing enable distributed, privacy-preserving IDS that can operate across multiple devices and locations24.

10. Conclusion
AI-powered intrusion detection systems using deep learning represent a transformative advance in cybersecurity. By leveraging sophisticated models such as CNNs, DNNs, and LSTMs, these systems can detect both known and novel threats with high accuracy and adaptability. While challenges remain in data quality, interpretability, and computational demands, ongoing research and technological advancements continue to improve the effectiveness and practicality of deep learning-based IDS. The future of cybersecurity will increasingly rely on intelligent, automated systems capable of defending against the ever-evolving landscape of cyber threats.

11. References

1. Deep Learning Algorithms Used in Intrusion Detection Systems. arXiv. 2024. Available from: https://arxiv.org/html/2402.17020v1
2. Ashiku I, Dagli D. Network Intrusion Detection System using Deep Learning. Procedia Computer Science. 2021;191:389-396. Available from: https://www.sciencedirect.com/science/article/pii/S1877050921011078
3. Gulia A, Sharma S, Gulia P, Sharma S. Design and implementation of a deep neural network approach for intrusion detection in computer networks. Journal of Information Security and Applications. 2024;80:103684. Available from: https://www.sciencedirect.com/science/article/pii/S2772671124000160
4. Louati A, Ktata O. Deep Learning for Intrusion Detection and Security of Internet of Things. Security and Communication Networks. 2022;2022:4016073. Available from: https://onlinelibrary.wiley.com/doi/10.1155/2022/4016073
5. Adewumi AO, Akinyelu AA, Adebiyi AA, *et al*. Signature-based intrusion detection using machine learning and deep learning. Scientific Reports. 2025;15:85866. Available from: https://www.nature.com/articles/s41598-025-85866-7
6. Arun K, *et al*. High-level Intrusion Detection System using Convolutional Neural Network. 2023.
7. Khan S, *et al*. DNN-based Intrusion Detection System for MQTT-enabled IoT Smart Systems. 2021.
8. Gulia P, *et al*. Group-Artificial Bee Colony Algorithm with Deep Neural Network for Cloud IDS. 2023.
9. Abdulrahman A, Mohammed M. Multilayer Perceptron Neural Network for DDoS Detection. 2020.
10. Rosay M, *et al*. Multilayer Perceptron for Network Intrusion Detection in Vehicular IoT. 2022.
11. Shettar P, *et al*. Intrusion Detection System using MLP and Chaotic Neural Networks. 2021.
12. Alkahtani A, Aldhyani TH. Deep Learning-based Intrusion Detection in IoT. 2021.
13. Ashiku I, Dagli D. Adaptive and Resilient IDS using Deep Learning. 2021.
14. Ghosh S, *et al*. Survey on Deep Learning for IDS. 2023.
15. Moustafa N, *et al*. UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection. 2015.