

“Review of Intrusion Detection System Using AI”

[Mayuri R. Gandole]¹

MCA I Sem IV

(PGDCA, PRIMTR Badnera)

mayurigandole@gmail.com[Sakshi Malange]²

MCA I Sem IV

(PGDCA, PRIMTR Badnera)

malangesakshi446@gmail.com[Rupali R.Sherekar]³

Head Of Departement

(PGDCA, PRIMTR Badnera)

hodmca@mitra.ac.in

ABSTRACT:-

The increasing dependence on computer networks and internet-based services has made information systems more vulnerable to cyber attacks and unauthorized access. Conventional security mechanisms are often limited in their ability to identify complex and evolving threats in real time.

An Intrusion Detection System (IDS) is an essential component of network security that monitors system activities and network traffic to detect potential security breaches. This research paper presents a comprehensive review of Intrusion Detection Systems (IDS) using Artificial Intelligence (AI) techniques to enhance the detection capability of modern security systems. Various machine learning algorithms discussed in the literature analyze network traffic patterns and distinguishes between normal and suspicious behavior.

The AI-based model is trained using historical network data, allowing it to recognize hidden patterns associated with malicious activities. The reviewed studies indicate that AI-based approaches can improve detection accuracy, reduce false

alarms, and identify both known and unknown attacks effectively. The integration of artificial intelligence with intrusion detection mechanisms provides a more adaptive and intelligent solution for protecting network infrastructures. The study highlights how AI-driven IDS can contribute to strengthening cybersecurity by enabling faster and more reliable threat detection in dynamic network environments.

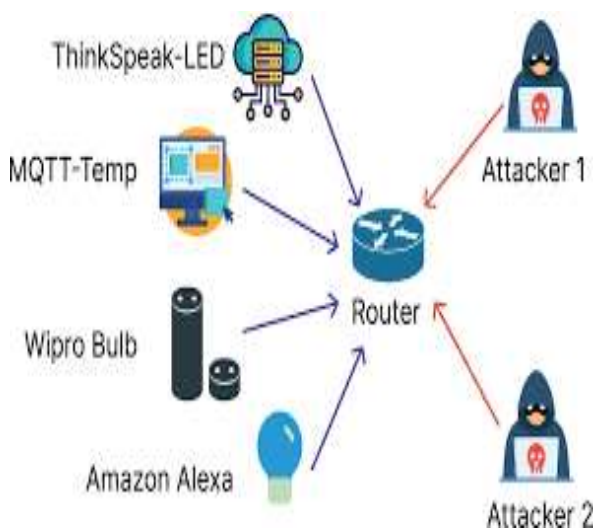
KEYWORDS:- Artificial Intelligence, Intrusion Detection System, Machine Learning Algorithms, Network Traffic Analysis, Cybersecurity, Anomaly Detection.

1.INTRODUCTION:-

An Intrusion Detection System (IDS) is an important security mechanism that monitors network traffic and system activities to identify suspicious behavior and potential security violations. Traditional IDS methods mainly rely on predefined rules and signature-based detection techniques. Although these approaches are effective in detecting known threats, they often fail

to identify new or unknown attacks and may generate a high number of false alarms

This paper focuses on reviewing existing AI-based intrusion detection techniques rather than proposing a new system. It analyzes different algorithms, methodologies, and their effectiveness in detecting cyber threats.



2. LITERATURE REVIEW:-

[1] Sharma et al.(2024): This study presents a detailed survey on Artificial Intelligence based Intrusion Detection Systems. The research highlights the role of machine learning and deep learning techniques in analyzing network traffic and detecting cyber attacks. The study emphasizes that AI-based IDS can improve detection accuracy, reduce false alarms, and enhance overall network security.

[2] Bunyaminu et al. (2024):This study presents a systematic review of AI-driven Network Intrusion Detection Systems, focusing on machine learning, deep learning, and hybrid models for detecting cyber attacks. The research highlights the importance of AI techniques in identifying zero-

day attacks, improving detection accuracy, and strengthening modern cybersecurity systems.

[3] AmruthaM.Holla et al.(2025):This study proposes an AI-based Network Intrusion Detection System using machine learning for real-time network security. The research highlights that machine learning models trained on modern datasets such as CICIDS2017 and CICIDS2018 can effectively detect cyber attacks and improve network monitoring through real-time traffic analysis and visualization.

[4] Repalle&Kolluru et al.(2017): This study explores the use of Artificial Intelligence and Machine Learning algorithms in Intrusion Detection Systems to automatically detect cyber attacks in network traffic. The research highlights that machine learning techniques can learn patterns from network data and help in identifying malicious activities with improved accuracy compared to traditional security systems.

[5] Joshi et al.:This study explores the use of Artificial Intelligence and deep learning techniques for developing advanced Intrusion Detection Systems to enhance network security. The research highlights that models such as CNN, DNN, and RNN can analyze large network datasets and accurately identify abnormal activities and cyber attacks, improving the overall detection performance of modern cybersecurity systems.

[6] Johi et al. (2024): This study explores the use of Artificial Intelligence and deep learning techniques for developing advanced intrusion detection systems. The research focuses on analyzing network traffic data to identify malicious

activities and cyber threats. The study highlights that deep learning models can improve the accuracy and efficiency of intrusion detection while reducing false alarms. It also emphasizes that AI-driven security systems can strengthen modern network protection against evolving cyber attacks.

[7] Kumar et al. (2023): This study presents an AI-based approach for improving intrusion detection systems in network security. The research focuses on the use of machine learning techniques to analyze network traffic and detect malicious activities. The study highlights that AI-based IDS can effectively identify cyber threats, improve detection accuracy, and reduce response time. The results indicate that intelligent security systems can provide stronger protection against modern cyber attacks.

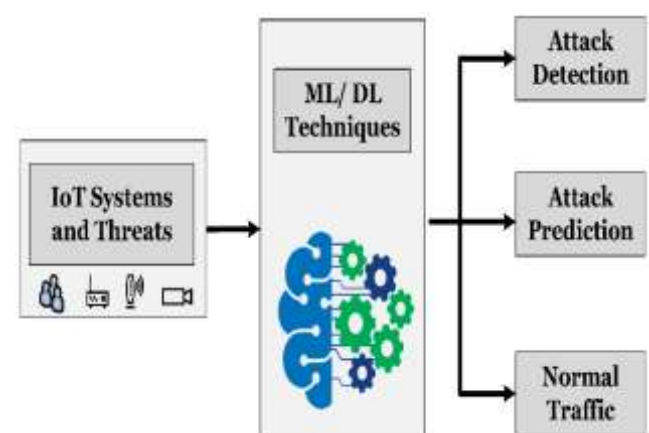
[8] Singh et al. (2022): This study discusses the use of Artificial Intelligence techniques in intrusion detection systems for improving network security. The research focuses on analyzing network traffic data to identify abnormal patterns and cyber attacks. The study highlights that AI-based intrusion detection systems can enhance detection accuracy, reduce false positives, and provide efficient protection against various types of cyber threats.

[9] Patel et al. (2021): This study presents an intelligent intrusion detection system using Artificial Intelligence techniques to enhance network security. The research focuses on applying machine learning algorithms to analyze network traffic and detect suspicious activities. The study highlights that AI-based IDS can improve

detection performance, identify unknown cyber attacks, and reduce false alarm rates. The findings indicate that intelligent security systems can provide more reliable protection for modern computer networks.

[10] Kethireddy (2020): This study presents an Artificial Intelligence-based intrusion detection system designed for edge computing environments. The research highlights the use of machine learning and deep learning techniques to and detect cyber threats in real time. The study emphasizes that AI-based IDS can improve detection accuracy, reduce false positive rates, and enhance the overall security of distributed edge computing systems.

From the above studies, it is observed that machine learning and deep learning techniques play a significant role in improving intrusion detection performance. However, each approach has its own advantages and limitations depending on the dataset, algorithm, and network environment.



3. Benefits of AI-Based Intrusion Detection:-

AI-based Intrusion Detection Systems (IDS) have been widely studied in recent research due to their ability to enhance network security beyond traditional rule-based approaches. Based on the reviewed literature, these systems offer several significant advantages in detecting and preventing cyber threats.

One of the primary benefits observed in various studies is the capability of AI-based IDS to data efficiently. Unlike conventional systems that rely on predefined signatures, machine learning models can identify hidden patterns and anomalies within complex datasets, enabling the detection of both known and unknown attacks.

Another important advantage is the adaptability of machine learning algorithms. Techniques such as **Support Vector Machine (SVM)** and **Random Forest** have been extensively used in intrusion detection due to their high classification accuracy and ability to handle high-dimensional data. SVM is particularly effective in distinguishing between normal and malicious traffic by constructing optimal decision boundaries, while Random Forest improves detection performance by combining multiple decision trees and reducing overfitting.

In addition, algorithms like **K-Nearest Neighbors (KNN)** have been applied for anomaly detection by measuring similarity between data points, although they may involve higher computational cost for large datasets. **Naïve Bayes** classifiers are also used due to their simplicity and efficiency in probabilistic classification, especially for real-time detection scenarios.

Recent research also highlights the growing importance of deep learning techniques in IDS. Models such as **Artificial Neural Networks (ANN)** can learn complex non-linear relationships in network traffic data. Furthermore, **Convolutional Neural Networks (CNN)** are capable of automatic feature extraction, improving detection accuracy without extensive manual feature engineering. Similarly, **Recurrent Neural Networks (RNN)** and **Long Short-Term Memory (LSTM)** networks are effective in analyzing sequential data, making them suitable for detecting time-based and evolving cyber attacks.

Another emerging approach is the use of **Reinforcement Learning (RL)**, where the system learns optimal detection strategies through interaction with the environment. This allows IDS to dynamically adapt to new and sophisticated attack patterns over time.

Overall, the reviewed studies indicate that AI-based intrusion detection systems significantly improve detection accuracy, reduce false positive rates, and enhance the ability to identify zero-day attacks. These systems provide a more intelligent and adaptive solution for modern cybersecurity challenges compared to traditional intrusion detection methods.

AI-based IDS can also adapt to evolving cyber threats without requiring frequent manual updates.

4.Challenges of AI-Based Intrusion Detection Systems:-

challenges is the requirement of large and high-quality datasets for training machine learning models. If the dataset used for training is incomplete or imbalanced, the model may produce inaccurate predictions or fail to detect certain types of attacks.

Another challenge is high computational **cost**. Training complex machine learning models requires significant processing power and memory resources, especially when dealing with large-scale network traffic data.

AI-based systems may also suffer from false positive alerts, where normal network activities are mistakenly classified as malicious. This can create unnecessary alerts and increase the workload of system administrators.

Another important concern is data privacy and security. Intrusion detection systems analyze sensitive network data, which raises concerns about protecting confidential information during data collection and processing.

5.CONCLUSION :-

The study is purely based on analysis of existing research and does not involve the development of a new IDS model. The study examined various machine learning techniques used for detecting cyber attacks and analyzed the benefits and challenges associated with these approaches.

The review findings indicate that AI technologies can significantly improve intrusion detection by analyzing network traffic patterns and identifying abnormal activities. Compared to traditional detection methods, AI-based systems offer higher detection accuracy, faster threat identification, and the ability to detect previously unknown attacks.

Despite these advantages, challenges such as data quality, computational requirements, and privacy concerns still need to be addressed for the effective implementation of AI-based security systems.

Overall, Artificial Intelligence has strong potential to transform intrusion detection technologies and strengthen cybersecurity infrastructure. Future research can focus on advanced techniques such as deep learning and real-time threat analysis to further enhance the effectiveness of intrusion detection systems.

6.FUTURE SCOPE :-

The future of intrusion detection systems is expected to be strongly influenced by advancements in Artificial Intelligence and machine learning technologies. As cyber attacks become more sophisticated, traditional security systems may not be sufficient to detect complex threats. Therefore, AI-based intrusion detection systems will continue to play an important role in improving network security.

Future research can focus on the use of advanced techniques such as Deep Learning and Reinforcement Learning to improve the accuracy and efficiency of intrusion detection systems.

These technologies have the potential to data and detect complex attack patterns more effectively.

Another important direction for future work is the development of real-time intrusion detection systems that can monitor network activities continuously and respond immediately to potential threats. Integration of AI-based IDS with cloud computing and Internet of Things (IoT) environments can also enhance the capability of cybersecurity systems.

Additionally, future studies can focus on improving dataset quality and developing more balanced datasets for training machine learning models. This can help reduce false positive alerts and improve the reliability of intrusion detection systems.

7.Reference:-

- [1] Artificial Intelligence based Intrusion Detection System – A Detailed Survey ITM Web of Conferences 65, 04002 (2024) <https://doi.org/10.1051/itmconf/20246504002> ICMAETM-24
- [2] AI-Driven Network Intrusion Detection Systems: A Systematic Review of Hybrid Models, Zero-Day Attack Mitigation, and Emerging Challenges in Cyber Security International Journal of Computer Applications (0975 – 8887) IJCATM : www.ijcaonline.org
- [3] AI-Based Network Intrusion Detection System Using Machine Learning for Real-Time Network Security © December 2025 | IJIRT | Volume 12 Issue 7 | ISSN: 2349-6002
- [4] Intrusion Detection System using AI and Machine Learning Algorithm International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 04 Issue: 12 | Dec-2017 www.irjet.net
- [5] AI-Driven Intrusion Detection Systems: Leveraging Deep Learning for Network Security Nanotechnology Perceptions ISSN 1660-6795 www.nano-ntp.com
- [6] A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (ai) michal markevych, maurice dawson illinois institute of technology, chicago, usa mmarkevych@hawk.iit.edu
- [7] AI-enabled intrusion detection systems in IoT networks: Advancing defense mechanisms for resource-constrained devices International Journal of Science and Research Archive, 2023, 09(01), 752–769 Article DOI: <https://doi.org/10.30574/ijrsra.2023.9.1.0316>
- [8] Network Intrusion Detection System: A systematic study of Machine Learning and Deep Learning approaches Received: 20 May 2020 Revised: 31 August 2020 Accepted: 29 September 2020 <https://doi.org/10.1002/ett.4150>
- [9] AI-based Intrusion Detection System for Internet of Things (IoT) Networks Turkish Journal of Computer and Mathematics Education Vol.10 No.02 (2019), 1095-1100 DOI: <https://doi.org/10.17762/turcomat.v10i2.13631>
- [10] AI-based intrusion detection systems for edge computing environments systems (ijitmis)



volume 11, issue 1, january-december 2020, pp.

45-53, article id: ijitmis_11_01_007

<https://iaeme.com/home/journal/ijitmis>