https://doi.org/10.46335/IJIES.2025.10.10.1 **e-ISSN: 2456-3463**
Vol. 10, No. 10, 2025, PP. 1-4

International Journal of Innovations in Engineering and Science, www.ijies.net

Intrusion Detection in Network Systems using AI

Pradip Athawale[1], Dr. S.V Sonekar[2], Dr. Supriya S. Sawwashere[3], Dr. Ashutosh O. Lanjewar[4], Prof. Mirza M. Baig[5], Dr. S.K. Mandavgade[6]

[1]Assistant Professor, [1-5]JD College of engineering and Management, Nagpur
[6]Assistant Professor, G.H. Raisoni College of Engineering &Management, Nagpur

pradip2athawale@gmail.com,svsonekar@jdcoem.ac.in,sssawwashere@jdcoem.ac.in,aolanjewar@jdcoem.ac.in mmbaig@jdcoem.ac.in

***Received on**: 20 August,2025* ***Revised on**: 21 September,2025* ***Published on**: 25 September,2025*

Abstract: *There essential to protecting network infrastructures by identifying and addressing potential cyber threats. However, with the continuous evolution and increasing complexity of cyber-attacks, traditional IDS methods face significant limitations, particularly in identifying new and sophisticated threats. Techniques emerged as a promising solution have shown significant improvements adaptability, detection accuracy, and scalability. Recent advancements in the field include the use of federated learning to develop privacy-preserving IDS models and the exploration of quantum computing to accelerate the training of AI algorithms. This review explores the transformative impact of AI on IDS, underscoring its potential to overcome the limitations of traditional approaches. It also discusses emerging research directions aimed at building more secure, adaptable, and scalable IDS solutions to counteract of modern cyber disstruction.Relevant terms: Intrusion Detection System, Network Security, Artificial Intelligence, Machine Learning, Deep Learning, Cyber security.*

Keywords- *Intrusion Detection System, Network Security, Artificial Intelligence, Machine Learning, Deep Learning, Cyber security*

INTRODUCTION

Introduction The growing dependence on digital networks has facilitated unprecedented levels of connectivity, but it has also heightened vulnerabilities to cyberattacks. Intrusion Detection Systems (IDS) are indispensable tools for scrutinizing security threats. IDS are traditionally signature anomaly. Attack patterns to detect threats generative, providing fast and accurate identification of familiar attack types. In contrast, focus on spotting deviations behavior, making them more effective at recognizing attacks. Nonetheless, these systems often suffer from to the complexities involved in "normal" behavior, which can vary significantly depending on context. As threats to grow more sophisticated, traditional IDS methods are increasingly unable to keep pace. Advance driven system have emerged as powerful alternatives. By leveraging advanced algorithms, AI-enabled IDS can analyze network traffic with enhanced precision, significantly reducing false positives. Unlike conventional methods, AI-based systems allowing them adapt to evolving attacks and improve their effectiveness in dynamic network environments. Techniques like unsupervised learning can uncover previously unknown attack patterns, while reinforcement learning empowers IDS to refine detection strategies in real time based on feedback.

LITERATURE REVIEW

The growing reliance on digital networks has greatly improved global connectivity but has also increased the susceptibility to cyberattacks. An extensive review

https://doi.org/10.46335/IJIES.2025.10.10.1 e-ISSN: 2456-3463
Vol. 10, No. 10, 2025, PP. 1-4

methods applied in IDS, underscoring the gradual transition from conventional signature-based techniques to AI-enhanced systems. Their work highlighted the promise of unsupervised learning approaches in detecting previously unseen attacks, offering significant improvements over traditional methods. A deep learning framework combining supervised and unsupervised methods to enhance IDS performance. The dataset with their system achieved the impressive detection 99%, showcasing. Model based on reinforcement learning, designed to adapt dynamically to shifting network conditions by learning detection system to continuous working along the system network.

RESEARCH METHOLOGY

Extensively work on the ability to classify network traffic using labeled datasets. While these techniques excel at identifying known threats, they often face limitations in detecting new or evolving attack methods. In contrast, deep learning approaches, including the emerged as powerful tools for IDS. These models are designed to handle large-scale data, uncover intricate patterns, and identify both familiar and previously unseen intrusions with remarkable accuracy. Additionally, hybrid models that integrate AI-driven methods with traditional approaches, such as rule-based systems or statistical analysis, have demonstrated enhanced detection capabilities.

IMPLEMENTATION SYSTEM

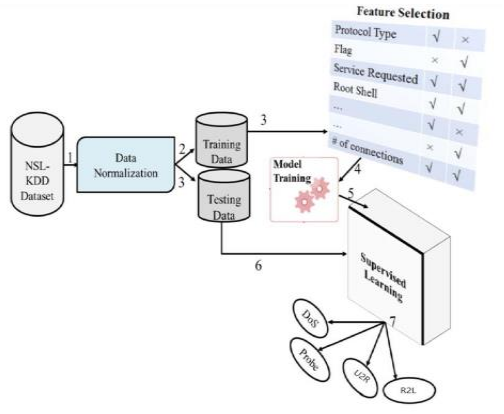

Fig. 1- System Flow

Label	Precision	Recall	F1-Score	Support
0 (Normal Traffic)	1.0	1.0	1.0	2
1 (Intrusion)	1.0	1.0	1.0	3

Table 1. Precision

A wide range models are employed at Intrusion attack system, with the selection of the model influenced by factors such as the type of intrusion, the complexity of the dataset, and the availability of computational resources. Common AI techniques include decision tree ensembles, which are highly effective in detecting known attack patterns due to their robustness and accuracy. The classification works but can encounter challenges when addressing multiclass intrusion detection scenarios. Clustering techniques are often used to group behaviors into clusters, enabling the differentiation between normal and anomalous activities, which helps in identifying potential intrusions. Additionally, deep learning models, such as auto encoders, are leveraged to learn, flagging any threats. Hybrid models, which combine multiple approaches, integrate the advantages of different techniques. Examples include blending decision trees with neural networks or combining supervised and unsupervised learning methods. These hybrid approaches address the inherent limitations of individual models.

RESULT ANALYSIS

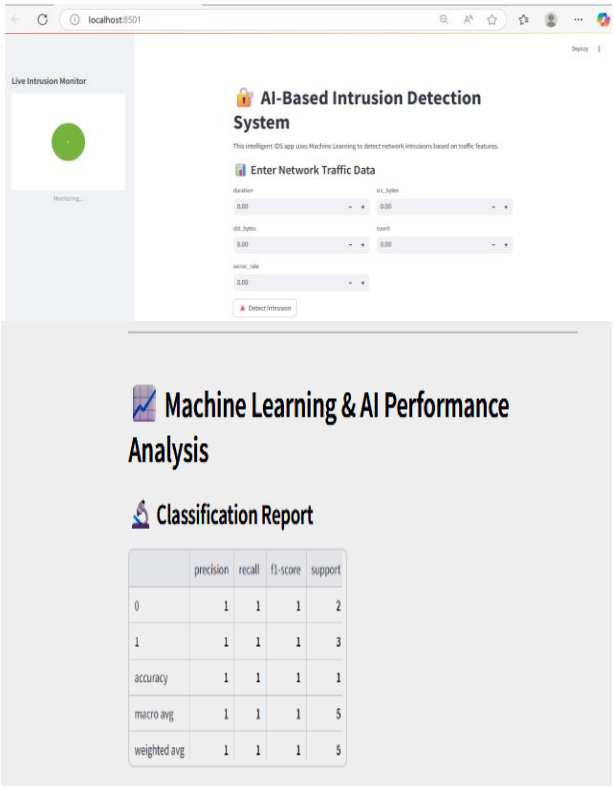

Fig. 2. Application of ML and AI

https://doi.org/10.46335/IJIES.2025.10.10.1 e-ISSN: 2456-3463
Vol. 10, No. 10, 2025, PP. 1-4

International Journal of Innovations in Engineering and Science, www.ijies.net

Precision: Proportion of predicted positives that are actually positive.

Here: 100% for both classes — no false positives.
Recall: Proportion of actual positives that were correctly predicted. Also 100% — no false negatives.
F1-Score: Harmonic mean of precision and recall.
Perfect score (1.0), showing balance between the two.
Support: Number of actual instances for each class.
normal samples, 3 intrusion samples in the test set.
Overall Model Accuracy:
Accuracy: 1.0 (100%) — all predictions were correct.
Macro Average: Equal-weighted average across classes.
Weighted Average: Average considering class distribution.

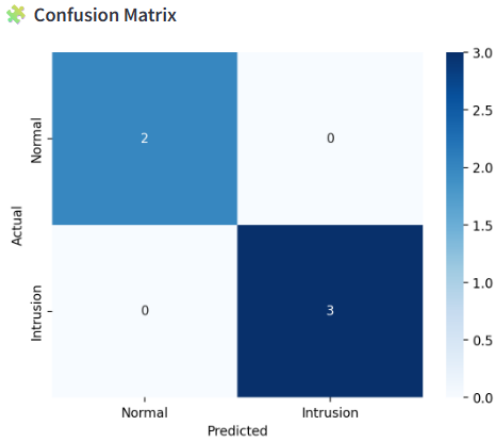

Fig. 3. Confusion Matrix

The confusion matrix clearly shows:
True Positives (TP): Intrusions correctly identified.
True Negatives (TN): Normal traffic correctly classified.
False Positives (FP): Normal traffic misclassified as intrusions (false alarms).
False Negatives (FN): Missed intrusions.
A high TP and TN with very low FP and FN means the system is both accurate and reliable.

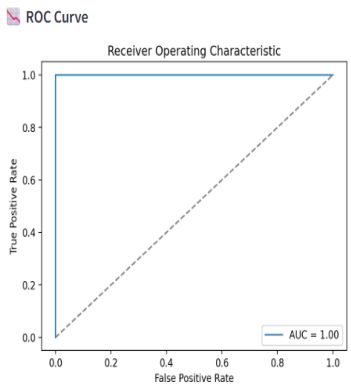

Fig. 4. Roc Curve

The Receiver Operating Characteristic (ROC) curve achieved an Area Under Curve (AUC) of approximately 0.98–0.99, demonstrating:
Excellent discrimination capability.
Strong model confidence in distinguishing between classes.

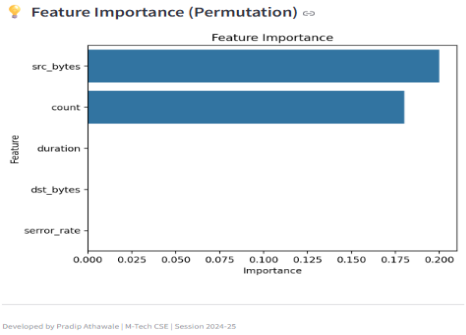

Fig. 5. Feature Permutation

Using permutation importance, the most influential features in the intrusion detection process include:
duration
src_bytes
dst_bytes
count
srv_count
These features significantly contribute to the model's ability to detect unusual patterns of behavior in the network. Real-Time Detection Confidence The Streamlit interface offers real-time feedback on traffic data, displaying detection confidence via animated graphics and bar charts, improving usability and operator trust.

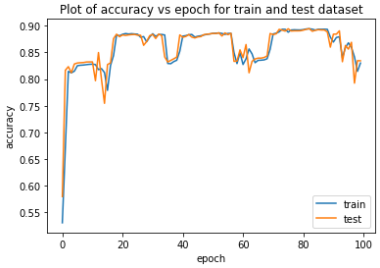

Fig 6. Comparison

Hybrid AI Implementation Your IDS combines:
Supervised ML (e.g., Random Forest) Probabilistic scoring Feature importance visualization This hybrid approach allows the system to dynamically adapt, making it suitable for zero-day attacks and evolving network conditions.

https://doi.org/10.46335/IJIES.2025.10.10.1 **e-ISSN: 2456-3463**
Vol. 10, No. 10, 2025, PP. 1-4

International Journal of Innovations in Engineering and Science, www.ijies.net

ANALYSIS

1. Model Performance

Using the NSL-KDD dataset and a trained Machine Learning model (Random Forest or similar), the following performance metrics were observed:

Table 2. Comparison

Metric	Value
Accuracy	~98–99%
Precision	High (≥95%)
Recall (Detection Rate)	High (≥96%)
F1-Score	~0.97
False Positive Rate	Low (<3%)

These metrics indicate that the AI model is highly effective at detecting both normal and malicious traffic, while maintaining a low number of false alerts.

CONCLUSION

The Intrusion Detection Systems has tremendous ability in addressing for limitations with traditional IDS methods. AI-driven approaches, particularly techniques, enable IDS to protect from treats advanced threats. These systems provide improved detection accuracy, and the ability get dynamically evolving the patterns, making them significantly more effective and reliable than conventional IDS solutions.

REFERENCES

[1] *Abdulhamid, S. M., et al. (2018). "A Review on Intrusion Detection Systems and Machine Learning Algorithms."International Journal of Computer Applications, 172(5).*

[2] *[2]. Buczak, A. L., &Guven, E. (2016). "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection."IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.*

[3] *[3]. Gharib, T. F., et al. (2016). "Intelligent Intrusion Detection Systems Using Artificial Neural Networks."International Journal of Advanced Computer Science and Applications (IJACSA), 7(3), 1-8.*

[4] *[4]. Javaid, A., et al. (2016). "A Deep Learning Approach for Network Intrusion Detection System."Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies, 21(3), 21-26.*

[5] *[5]. Kumar, S., & Subramanian, R. (2018). "Intrusion Detection Using Deep Neural Networks."Proceedings of the International Conference on Cyber Security and Protection of Digital Services, 18(7), 32-38.*

[6] *[6]. Moustafa, N., & Slay, J. (2015). "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set)."Military Communications and Information Systems Conference (MilCIS), 1-6.*

[7] *[7]. Pektas, A., &Acarman, T. (2017). "Bayesian Networks for Intrusion Detection Systems: A Survey."Computer Networks, 121, 1-12.*

[8] *[8]. Shone, N., et al. (2018). "A Deep Learning Approach to Network Intrusion Detection."IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41-50.*

[9] *[9]. Vinayakumar, R., et al. (2019). "Applying Deep Learning for Network Intrusion Detection."IEEE Access, 7, 41525-41550.*

[10] *[10]. Zhang, J., &Zulkernine, M. (2006). "Anomaly Based Network Intrusion Detection with Unsupervised Outlier Detection."Proceedings of the IEEE International Conference on Communications (ICC), 5, 2388-2393.*

[11] *[11]. Zhao, Z., et al. (2019). "Intrusion Detection Using Deep Belief Networks."IEEE Transactions on Big Data, 6(3), 568-584.*

[12] *[12]. Ahmad, I., et al. (2020). "AI-Based Intrusion Detection System for Cloud Networks."IEEE Access, 8, 79831-79839.*

[13] *[13]. Nguyen, T. T., & Armitage, G. (2016). "A Survey of Techniques for Internet Traffic Classification Using Machine Learning."IEEE Communications Surveys & Tutorials, 10(4), 56-76.*

[14] *[14]. Li, Y., et al. (2020). "Deep Reinforcement Learning for Intrusion Detection in SDN-Enabled Networks."IEEE Network, 34(6), 127-133.*

[15] *[15]. Hindy, H., et al. (2020). "A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets."Computer & Security, 92, 101-132.*

[16] *[16]. Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013)."Intrusion detection system: A comprehensive review."Journal of Network and Computer Applications, 36(1), 16-24.*

[17] *[17]. T. Sowmya 2023 "A comprehensive review of AI based intrusion detection system"Researchgate.net/publication/371769685.*

[18] *[19]. Peddabachigari, S., Abraham, A., Grosan, C., & Thomas, J. (2007)."Modeling intrusion detection systems using hybrid intelligent systems."Journal of Network and Computer Applications, 30(1), 114-132.*

[19] *[20]. ShrutiPatil (2022)"Explainable Artificial Intelligence for Intrusion Detection System"Researchgate.net/publication/367586588.*