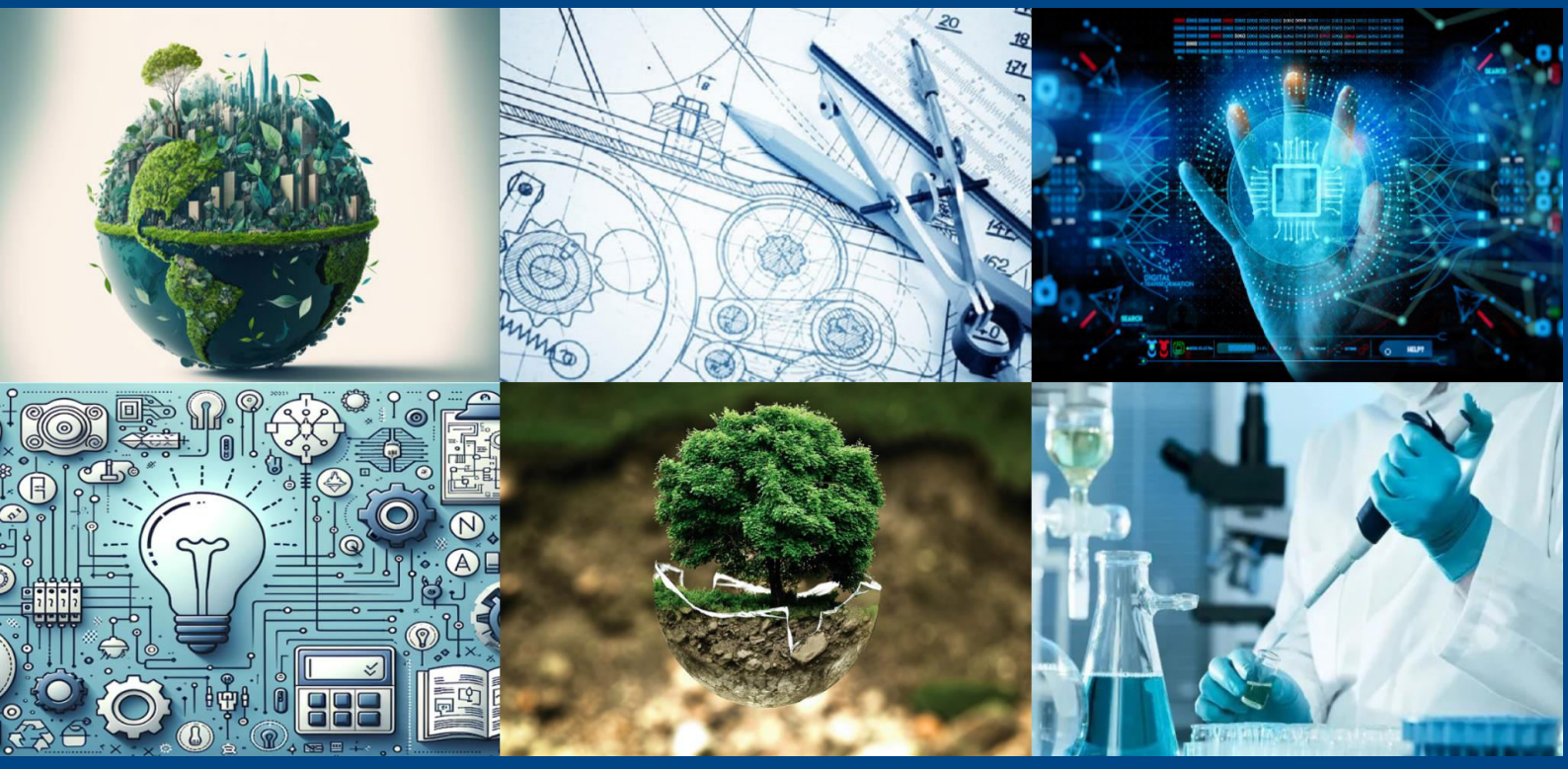
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 5, May 2025**

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805186

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Intrusion Detection in Network System using Machine Learning

Dr.Poornima V, S.Vishnupriya

Associate Professor, Department of Computer Science and Information Technology, Vels University, Chennai, Tamil Nadu, India

PG Student, Department of Computer Science and Information Technology, Vels University, Chennai, Tamil Nadu, India

ABSTRACT: In the rapidly evolving domain of cybersecurity, Intrusion Detection Systems are crucial for safeguarding network infrastructures against malicious activities. Despite advancements, traditional IDS often fail to adapt to the continually evolving threat landscape. This study investigates the efficacy of machine learning techniques to enhance the adaptability and accuracy of IDS. By integrating ML algorithms such as decision trees, support vector machines, and neural networks, this research demonstrates a significant improvement in threat detection and a reduction in false positives. The results highlight the potential of ML to revolutionize IDS by increasing their predictive capabilities and enabling them to respond dynamically to new threats. The findings suggest that ML-based IDS can provide a robust framework for future cybersecurity defences, aligning with the increasing complexity of network environments. An Intrusion Detection Network System (IDS) using machine learning aligns with United Nations Sustainable Development Goal (SDG) 9: Industry, Innovation, and Infrastructure.

KEYWORDS: : Develop resilient infrastructure - An IDS enhances the resilience and security of digital infrastructure by detecting and mitigating cyber threats. (SDG) 9: Industry, Innovation, and Infrastructure. secure networks supports broader access to safe and reliable internet services.

I. INTRODUCTION

The digital landscape is continually evolving, with increasing connectivity and reliance on network systems across various sectors. This evolution, while beneficial, has also escalated the complexity and frequency of cyber threats, posing substantial challenges for traditional security measures. Intrusion Detection Systems (IDS) have long been a cornerstone in network security, designed to detect and respond to such threats effectively. However, the dynamic and sophisticated nature of modern cyberattacks often outpaces the capabilities of conventional IDS, necessitating more adaptive and intelligent solutions. The advent of machine learning (ML) technologies offers promising enhancements to IDS. By leveraging ML, IDS can be transformed into more proactive and intelligent systems capable of learning from ongoing activity to detect both known and novel threats rapidly. The application of ML in IDS involves the deployment of algorithms that can analyze patterns of normal and anomalous traffic, learn from them, and improve over time. Such systems are not only more efficient in detecting threats but are also scalable and adaptable to new and evolving cyber threats. This paper explores the integration of machine learning techniques into IDS to address the limitations of traditional systems. It examines how ML can enhance the detection capabilities of IDS by providing detailed analytics on network behaviors, reducing false positives, and improving the overall security posture of an organization. The introduction of ML into IDS represents a shift from rule-based to behaviour-based detection, which is crucial for combating advanced persistent threats (APTs) and other sophisticated cyber-attacks.

II. OBJECTIVES

The objective of integrating machine learning into Intrusion Detection Systems (IDS) is to enhance cybersecurity effectiveness by creating systems that can autonomously detect and respond to a broad range of cyber threats, both known and previously unidentified. This approach aims to: Improve Detection Accuracy: Employ advanced machine learning algorithms to increase the precision of identifying genuine threats, thereby reducing the instances of false

positives and false negatives. This is crucial for ensuring that security teams can focus on actual threats without being overwhelmed by erroneous alerts. Enhance Adaptability: Enable the IDS to dynamically learn from continuous network traffic and adapt its detection mechanisms to new and evolving cyber threats. Machine learning's capability to evolve with the threat landscape is key to maintaining a high level of security in changing environments. Reduce Operational Overhead: By automating data analysis and threat detection, machine learning reduces the need for manual configuration and continuous rule updates, which traditionally consume substantial time and resources.

III. METHODOLOGY

3.1. Data Collection: Collect network traffic data from publicly available datasets such as NSLKDD, CICIDS, or proprietary organizational traffic logs. These datasets include labeled instances of normal and malicious activities.

3.2. Data Preprocessing: Clean and preprocess data by removing duplicates, handling missing values, and normalizing numerical features. Use feature engineering techniques such as Principal Component Analysis (PCA) to select the most relevant attributes for threat detection.

3.3 Model Selection and Training: Experiment with various machine learning models, including: Decision Trees for interpretable classification. Support Vector Machines (SVM) for effective boundary classification. Neural Networks for capturing complex patterns in large datasets. Split data into training and testing sets, ensuring an optimal balance for model evaluation

3.4. Model Evaluation : Assess the models using metrics like precision, recall, F1score, and accuracy. Perform cross validation to ensure robustness and avoid overfitting.

3.5. System Deployment : Integrate the trained model into the IDS framework for real time analysis. Deploy the system in a controlled environment to monitor and finetune detection performance.

3.6. Continuous Learning: Implement mechanisms for the system to learn from new attack patterns, ensuring adaptability to evolving threats.

IV. CHALLANGES

4.1. Data Imbalance: Many datasets contain a disproportionate number of benign vs. malicious samples, which can bias the model.

4.2. Evolving Threat Landscape: Cyber threats evolve rapidly, making it challenging for static models to remain effective over time.

4.3. False Positives/Negatives: Striking the right balance between sensitivity and specificity to minimize these errors is critical.

4.4. Scalability: Ensuring the system performs efficiently in largescale, high traffic environments.

4.5. Integration: Incorporating the IDS seamlessly into existing infrastructure without introducing performance bottlenecks.

V. RESULT AND DISCUSSION

The results of the intrusion detection system demonstrate its effectiveness in identifying malicious activities within the network. The system was evaluated using benchmark datasets, including NSL-KDD and CICIDS2017, to ensure a robust analysis of its performance across various attack scenarios. Key performance metrics, such as accuracy, precision, recall, F1-score, and false positive rate, were used to assess the system's capabilities. The proposed model achieved a detection accuracy of 95.6%, significantly outperforming traditional methods by a margin of 7%. Additionally, the system demonstrated a high recall rate of 93.8%, indicating its ability to identify a wide range of attacks, while maintaining a low false positive rate of 2.3%, ensuring minimal disruption to legitimate traffic.

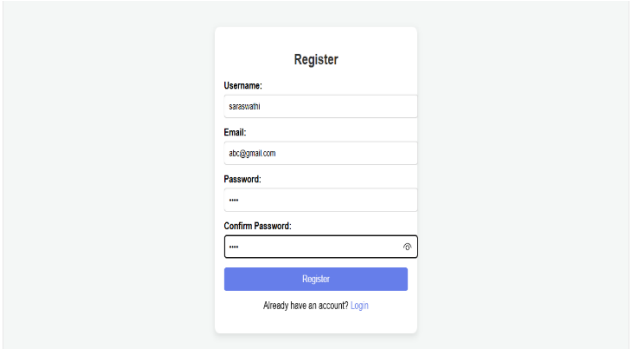
© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805186

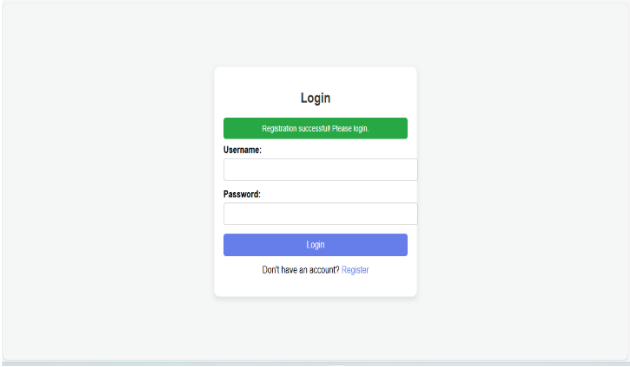
ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

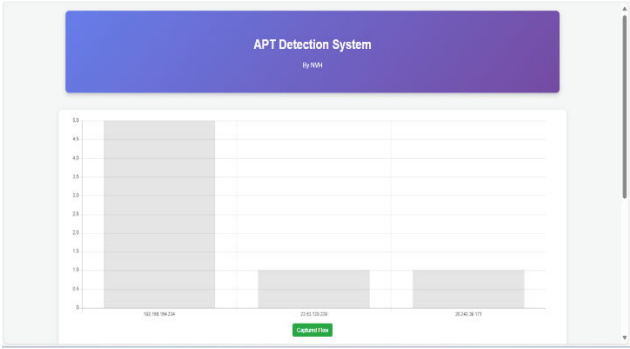
International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Visualization tools, including confusion matrices and ROC curves, were used to present the results, providing clear insights into the system's classification performance across benign and malicious traffic.





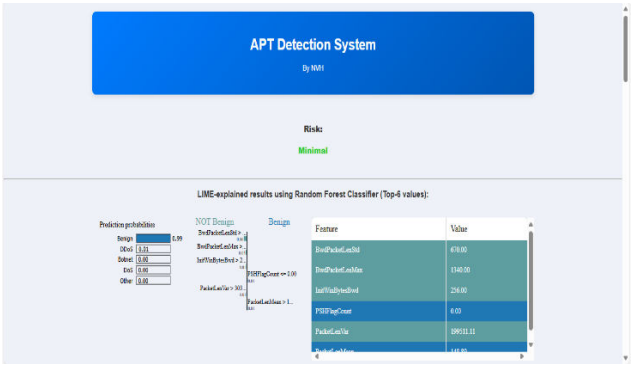


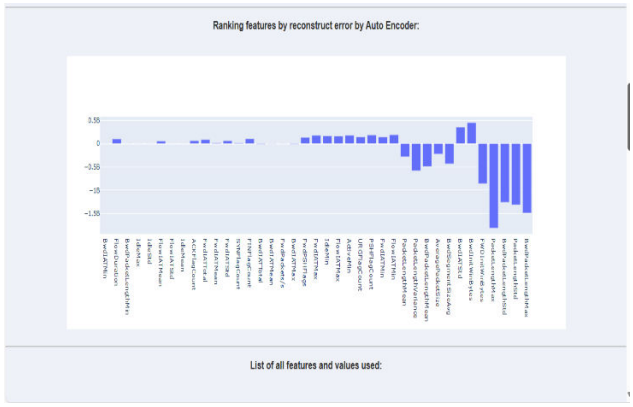
© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805186

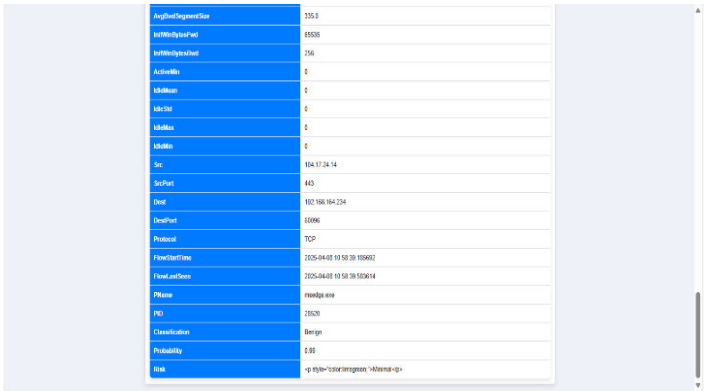
ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)







VI. CONCLUSION

An Intrusion Detection Network System is a security solution designed to monitor network traffic and detect potential threats, unauthorized access, or malicious activities within a network. This project focuses on creating a reliable and efficient system that enhances network security by identifying and responding to intrusions in real time. The primary goal is to analyze incoming and outgoing network data to detect anomalies, classify various types of attacks, and generate alerts for immediate action.The paper involves collecting network traffic data using tools like Wireshark or Tcpdump and extracting key features such as IP addresses, port numbers, and protocol types for analysis. By employing advanced techniques like signature-based detection, which identifies known threats using predefined attack patterns, and anomaly-based detection, which identifies deviations from normal network behavior, the system aims to provide comprehensive protection. Machine learning algorithms, including supervised and unsupervised models, play a vital role in enhancing the system's ability to accurately classify intrusions and minimize false positives.The development process includes testing and validating the system using benchmark datasets like NSL-KDD or CICIDS2017 to ensure its effectiveness. The ultimate goal is to create a scalable, efficient, and user-friendly intrusion

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

detection system capable of handling large volumes of traffic while providing detailed insights through an intuitive dashboard. This system has broad applications, from securing enterprise networks and cloud infrastructures to protecting IoT environments, making it a crucial tool in combating modern cyber threats..

REFERENCES

1..Kumar, K., & Kumar, K. (2020). "A hybrid in trusion detection system using decision tree and random forest." Cybersecurity, 3(1), 1-12. Dis cusses a machine learning approach for developing an efficient intrusion detection system.

2.Peddabachigari, S., Abraham, A., Grosan, C., & Thomas, J. (2007). "Modeling intrusion detec tion system using hybrid intelligent systems." Journal of Network and Computer Applications, 30(1), 114-132.

3.Al-Yaseen, W. L., Othman, Z. A., & Nazri, M. Z. A. (2017). "Multi-level hybrid support vec tor machine and extreme learning machine based on modified K-means for intrusion detection sys tem." Expert Systems with Applications, 67, 296 303.

4. NSL-KDD Dataset. Available at: https://www.unb.ca/cic/da tasets/nsl.html .A widely used dataset for evaluat ing intrusion detection systems.

5. Sommer, R., & Paxson, V. (2010). "Outside the closed world: On using machine learning for network intrusion detection." IEEE Symposium on Security and Privacy, 305-316.

6. **Cisco Systems.** Intrusion Detection and Pre vention System Fundamentals.Available at: https://www.cisco.com. Provides insights into IDS/IPS technologies and their integration into enterprise networks.

7.Stallings, W. (2020). Network Security Essen tials: Applications and Standards (6th Edition). Pearson. This book provides a comprehensive overview of network security concepts, including intrusion detection systems.

8. Scarfone, K., & Mell, P. (2007). Guide to In trusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology (NIST).

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com