International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0249
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1694 - 1697

NIDS – Network Intrusion Detection System

Dr. S. S. Shriramwar[1], Siya Bhange[2], Tejashree Dravyakar[3], Mahesh Shinde[4], Lavanya Dongre[5]
[1]Centre of Examination, Priyadarshini College of Engg. Nagpur, 440019, India
[2,3,4,5] UG Scholar, Dept. of IIoT, Priyadarshini College of Engg. Nagpur, 440019, India
Emails: *sshriramwar2@gmail.com[1], siyabhange2002@gmail.com[2], tejashreedravyakar@gmail.com[3], maheshdileepshinde@gmail.com[4], lavanyadongre14@gmail.com[5]*

Abstract
The rapid expansion of Internet of Things (IoT) devices has transformed modern industries and everyday life. However, it has also introduced significant security challenges due to limited computational resources and weak built-in security mechanisms. To address these issues, this paper presents the design and implementation of a lightweight Network Intrusion Detection System (NIDS) specifically tailored for IoT environments. The proposed system continuously monitors network traffic and device behavior to detect unauthorized access, anomalies, and malicious activities with high accuracy while maintaining low computational overhead. The system utilizes machine learning-based techniques for efficient intrusion detection and ensures minimal resource consumption, making it suitable for resource-constrained IoT devices. Experimental results demonstrate the effectiveness of the proposed model in identifying various types of network attacks, thereby enhancing the overall security of IoT networks.

Keywords: *Anomaly Detection; Cybersecurity; IoT Security; Machine Learning; Network Intrusion Detection System*

1. Introduction
The rapid growth of the Internet of Things (IoT) across various sectors such as smart homes, healthcare, industrial systems, and critical infrastructure has significantly increased the demand for secure network communication. IoT devices are generally resource-constrained, with limited computational power, lightweight operating systems, and minimal built-in security features. These limitations make them highly vulnerable to a wide range of cyber threats, including unauthorized access, malware attacks, and denial-of-service (DoS) attacks. Traditional security solutions such as firewalls and antivirus systems are not sufficient to address the dynamic and complex nature of attacks in IoT environments. To overcome these challenges, Intrusion Detection Systems (IDS) have emerged as an effective security mechanism for monitoring network traffic and identifying malicious activities. Among them, Network Intrusion Detection Systems (NIDS) are widely used due to their ability to analyze network-level data and detect threats across multiple devices. NIDS can identify various types of attacks by continuously monitoring traffic patterns and generating alerts for suspicious behavior. Recent research has focused on enhancing intrusion detection systems using machine learning and deep learning techniques. An IoT-based NIDS utilizing machine learning techniques has been proposed in [1], which demonstrates the effectiveness of intelligent models in detecting both known and unknown attacks. A comprehensive survey in [2] highlights that machine learning approaches, including classification and anomaly detection techniques, significantly improve detection accuracy compared to traditional systems, although they introduce computational complexity. Furthermore, a study in [3] analyzed machine learning-based NIDS models across multiple datasets and found that model performance may vary depending on the dataset, emphasizing the challenge of generalization. Neural network-based intrusion detection systems have also been explored in [4], where artificial neural networks

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0249
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1694 - 1697

achieved high detection accuracy but required higher computational resources. These studies indicate that while machine learning and deep learning techniques enhance intrusion detection performance, challenges such as resource constraints, model generalization, and computational overhead still exist. Therefore, there is a need for a lightweight and efficient intrusion detection system suitable for IoT environments. In this work, a lightweight Network Intrusion Detection System (NIDS) tailored for IoT environments is proposed. The system is implemented using Raspberry Pi 4 Model B along with network monitoring tools such as Snort and Wireshark. The proposed system aims to provide real-time intrusion detection with low computational overhead, making it suitable for deployment in resource-constrained IoT networks. Recent research [1]–[4], [11]–[13] has focused on enhancing intrusion detection systems using machine learning and deep learning techniques.

2. Method

The methodology of the proposed system focuses on designing and implementing a lightweight Network Intrusion Detection System (NIDS) for IoT environments. The system is developed to monitor network traffic, analyze data packets, and detect malicious activities in real time. Initially, network traffic is captured using Wireshark, which provides detailed insights into packet-level information such as source and destination addresses, protocols, and traffic patterns. The captured data is then processed to identify relevant features required for intrusion detection. The detection process is carried out using Snort, an open-source intrusion detection system that applies predefined and custom rule sets to identify various types of attacks such as denial-of-service (DoS), port scanning, and unauthorized access attempts. The system continuously monitors incoming traffic and compares it against known attack signatures. The entire system is deployed on Raspberry Pi 4 Model B, which serves as a lightweight and cost-effective platform. Once a threat is detected, alerts are generated and logged for further analysis. This methodology ensures real-time detection with minimal computational overhead, making it suitable for resource-constrained IoT environments. The above table summarizes the key components used in the proposed system. Figure 1 shows Ids Block Diagram. Table 1.

Table 1 System Components and Description

Process	Description
Data Collection	Network traffic is captured using Wireshark
Data Processing	Relevant features are extracted from packets
Intrusion Detection	Snort applies rules to detect malicious traffic
Alert Generation	Alerts are generated for detected threats

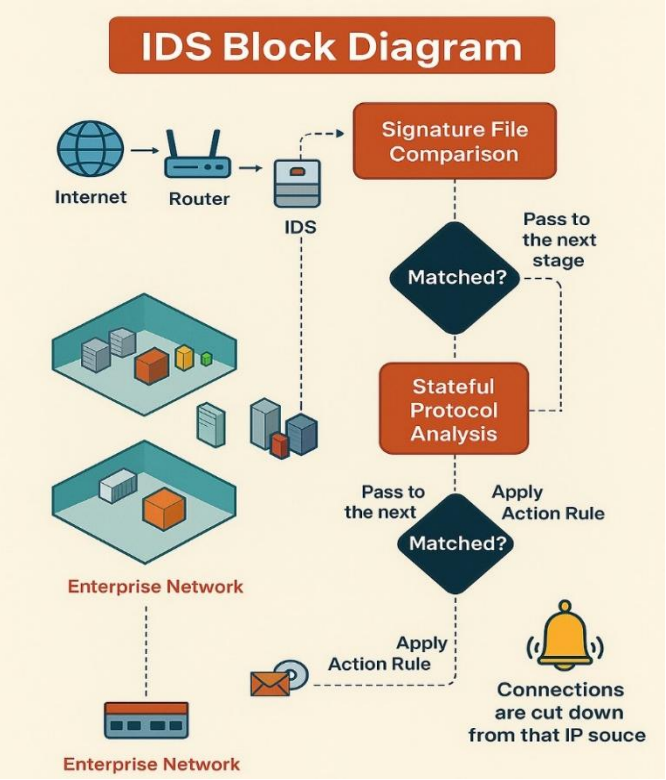

Figure 1 IDS Block Diagram

3. Results and Discussion

3.1.Results

The proposed Network Intrusion Detection System (NIDS) was evaluated in a controlled network

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0249
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1694 - 1697

environment by simulating various types of cyberattacks, including denial-of-service (DoS) attacks, port scanning, and unauthorized access attempts. The system successfully captured and analyzed network traffic using Wireshark, while Snort effectively identified malicious activities based on predefined rule sets. The performance of the system was analyzed using key parameters such as detection accuracy, response time, and system efficiency. The results indicate that the proposed NIDS can detect a majority of common network attacks with high accuracy while maintaining low computational overhead on the Raspberry Pi platform. Furthermore, the system demonstrated real-time alert generation with minimal delay, making it suitable for practical deployment in IoT environments. However, it was observed that signature-based detection techniques may have limitations in identifying unknown or zero-day attacks, indicating the need for further enhancement using machine learning approaches. Overall, the results confirm that the proposed system provides an effective and lightweight solution for intrusion detection in resource-constrained IoT networks.

3.2.Discussion

The experimental results demonstrate that the proposed NIDS effectively detects various network attacks in IoT environments with satisfactory accuracy. The system is capable of real-time monitoring and alert generation while maintaining low computational overhead on resource-constrained hardware such as Raspberry Pi. However, reliance on signature-based detection limits its ability to identify unknown or zero-day attacks. Therefore, integrating machine learning techniques can further enhance the system's detection capability and overall performance.

Conclusion

This paper presented a lightweight Network Intrusion Detection System (NIDS) designed for IoT environments using Raspberry Pi, Snort, and Wireshark. The system effectively monitors network traffic and detects various types of cyber-attacks in real time with low computational overhead. The results demonstrate that the proposed approach is suitable for resource-constrained IoT devices while maintaining reliable detection performance. Future work can focus on integrating machine learning techniques to enhance the detection of unknown and advanced threats.

Acknowledgements

The authors would like to express their sincere gratitude to our project guide for their continuous guidance, support, and valuable suggestions throughout the development of this project. We also thank the Department of Industrial Internet of Things, Priyadarshini College of Engineering, Nagpur, for providing the necessary resources and environment to successfully complete this work.

References

[1]. M. Roopak, G. Y. Tian, and J. Chambers, "Deep learning models for cyber security in IoT networks," IEEE Access, vol. 7, pp. 41525–41550, 2019.
[2]. S. M. Kasongo and Y. Sun, "A deep learning method with filter-based feature engineering for wireless intrusion detection system," IEEE Access, vol. 7, pp. 38597–38607, 2019.
[3]. H. Hindy et al., "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," IEEE Access, vol. 8, pp. 104650–104675, 2020.
[4]. A. Verma and S. Ranga, "Machine learning based intrusion detection systems for IoT applications," Procedia Computer Science, vol. 167, pp. 449–457, 2020.
[5]. K. Zhao and L. Ge, "A survey on the Internet of Things security," in Proc. IEEE Int. Conf. Comput. Sci. Electron. Eng., 2013, pp. 663–667.
[6]. D. E. Denning, "An intrusion-detection model," IEEE Trans. Softw. Eng., vol. 13, no. 2, pp. 222–232, 1987.
[7]. G. Creech and J. Hu, "A semantic approach to host-based intrusion detection systems using system call patterns," IEEE Trans. Comput., vol. 63, no. 4, pp. 807–819, 2014.
[8]. I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0249
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1694 - 1697

wireless sensor networks," IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 266–282, 2014.

[9]. [9] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in Proc. Mil. Commun. Inf. Syst. Conf., 2015, pp. 1–6.

[10]. T. Shon and J. Moon, "A hybrid machine learning approach to network anomaly detection," Inf. Sci., vol. 177, no. 18, pp. 3799–3821, 2007.

[11]. J. Kim et al., "Long short term memory recurrent neural network classifier for intrusion detection," in Proc. Int. Conf. Platform Technol. Service, 2016, pp. 1–5.

[12]. M. A. Ferrag et al., "A systematic review of data mining and machine learning for cyber security intrusion detection," IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 1416–1447, 2020.

[13]. Y. Xin et al., "Machine learning and deep learning methods for cybersecurity," IEEE Access, vol. 6, pp. 35365–35381, 2018.

[14]. S. Dua and X. Du, Data Mining and Machine Learning in Cybersecurity. Boca Raton, FL, USA: CRC Press, 2016.

[15]. R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in Proc. IEEE Symp. Security Privacy, 2010, pp. 305–316.