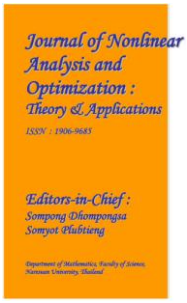
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1, No.1 : 2025
ISSN : **1906-9685**



COMPACT AND EFFICIENT IOT INTRUSION DETECTION FRAMEWORK

G.UMA DEVI Assistant Professor in Department of CSE, Raghu Engineering College, Visakhapatnam.
D.HITESH NAIDU B. Tech Computer Science and Engineering (AI-ML) in Raghu Institute of Technology, Visakhapatnam.
P. PRANATHI B. Tech Computer Science and Engineering (AI-ML) in Raghu Institute of Technology, Visakhapatnam.
B.SAI KRISHNA B. Tech Computer Science and Engineering (AI-ML) in Raghu Institute of Technology, Visakhapatnam.
D.SURESH B. Tech Computer Science and Engineering (AI-ML) in Raghu Institute of Technology, Visakhapatnam.

Abstract_ The growing prevalence of low-powered devices on the Internet of Things (IoT) ecosystem has significantly increased its vulnerability to security threats. This study focuses on enhancing IoT security by developing a lightweight Intrusion Detection System (IDS) that incorporates machine learning techniques for efficient feature selection and classification. A filter-based feature selection method was employed to reduce computational overhead, ensuring suitability for resource-constrained IoT environments.
To classify features, multiple machine learning algorithms were evaluated, including Naïve Bayes (NB), Decision Tree (DT), Random Forest (RF), k-Nearest Neighbor (KNN), Support Vector Machine (SVM), and Multilayer Perceptron (MLP). Among these, the Decision Tree (DT) demonstrated superior performance across diverse datasets and was chosen as the optimal model for the IDS.
This work contributes to IoT security by presenting a framework that is both computationally efficient and effective in identifying potential intrusions. The findings provide a benchmark for evaluating future feature selection and machine learning methodologies aimed at improving the resilience of IoT systems against emerging threats.

.

.**Keywords:**
- IoT (Internet of Things)
- IDS (Intrusion Detection System)
- Anomaly detection
- Feature selection.

1.INTRODUCTION

The Internet of Things (IoT) has revolutionized the way devices interact, creating interconnected ecosystems that enable automation, data sharing, and enhanced functionalities in various sectors. From smart homes to industrial automation, IoT devices have become integral to modern infrastructure. However, the growing reliance on these devices has also introduced significant security challenges. The resource-constrained nature of IoT devices, coupled with their widespread use, makes them highly susceptible to cyberattacks such as unauthorized access, data breaches, and network intrusions. To address these challenges, this project focuses on developing a **Compact and Efficient IoT Intrusion Detection Framework**. The goal is to design a lightweight yet robust Intrusion Detection System (IDS) capable of identifying and mitigating threats in real-time without overburdening the limited computational and energy resources of IoT devices. By leveraging advanced machine learning techniques for feature selection and classification, the proposed framework ensures a balance between accuracy, speed, and resource efficiency.

The framework incorporates a filter-based feature selection method to reduce computational overhead and explores various machine learning algorithms, including Decision Tree (DT), Random Forest (RF), and Support Vector Machine (SVM), to determine the most effective model for intrusion detection. This project emphasizes scalability, adaptability, and compatibility with diverse IoT environments, ensuring its practical application across different use cases.

Through this work, the project aims to contribute to the advancement of IoT security by offering a solution that enhances the resilience of IoT networks while maintaining their operational efficiency.

2. LITERATURE SURVEY

Atzori et al. This paper provides a comprehensive survey on the Internet of Things (IoT), covering its key technologies, applications, and challenges. The authors explore RFID, wireless sensor networks, and cloud computing as core enablers of IoT. Security and scalability concerns are discussed, emphasizing the need for efficient threat detection mechanisms. The study highlights how IoT introduces new attack vectors, requiring advanced security solutions like intrusion detection systems (IDS).

Weiser et al. This paper introduces the concept of ubiquitous computing, predicting a future where technology seamlessly integrates into daily life. Weiser envisions smart environments with interconnected devices, paving the way for modern IoT systems. The study highlights how contextaware computing can improve automation but also increases security risks. As IoT adoption grows, so does the need for efficient security frameworks, such as lightweight intrusion detection for real-time threat monitoring.

Sedjelmaci et al. This paper proposes a game-theoretic anomaly detection method tailored for lowresource IoT devices. The authors design a framework that balances detection accuracy and computational efficiency, making it ideal for power-constrained environments. The approach effectively identifies malicious activities while minimizing false alarms. By leveraging lightweight security mechanisms, the study demonstrates how intrusion detection can be optimized for IoT networks without compromising performance.

Raza et al. This paper presents SVELTE, a lightweight intrusion detection system (IDS) designed for IPv6-based IoT networks. The system focuses on detecting routing attacks using real-time anomaly detection techniques. The authors evaluate SVELTE's efficiency, showing that it reduces false positives while maintaining high detection accuracy. The study emphasizes the importance of low-power IDS solutions that can operate effectively in resource-constrained IoT environments.

Anand & Patel et al. This paper provides an overview of intrusion detection systems (IDS), categorizing different attack types and detection mechanisms. The authors analyze network-based and host-based IDS, highlighting their strengths and weaknesses. The study also explores how machine learning techniques can enhance intrusion detection capabilities. By classifying common IoT security threats, the paper reinforces the need for advanced feature selection and preprocessing techniques to improve detection accuracy.

3. PROPOSED SYSTEM

The proposed system introduces a lightweight Intrusion Detection System (IDS) specifically designed to address the unique security challenges of IoT networks. This system leverages machine learning techniques to provide efficient, accurate, and scalable intrusion detection, making it suitable for resource-constrained IoT devices.

The framework adopts a structured workflow comprising several stages:

- **Dataset Collection and Preprocessing:** Relevant datasets containing network traffic data are collected and preprocessed to remove noise and ensure the quality of input data.
- **Feature Selection:** A filter-based feature selection method is employed to identify and retain only the most relevant features for intrusion detection. This approach reduces computational overhead, optimizing the system for the limited resources of IoT devices.
- **Classification:** Various machine learning algorithms, including Naïve Bayes (NB), Decision Tree (DT), Random Forest (RF), K-Nearest Neighbor (KNN), Support Vector Machine (SVM), and Multilayer Perceptron (MLP), are evaluated for their performance. Among these, the

Decision Tree (DT) model is selected for its superior accuracy, low computational requirements, and ability to handle diverse datasets effectively.

- **Training and Validation:** The selected model is trained using labeled datasets and validated using performance metrics such as accuracy, precision, recall, and F1-score. This ensures the IDS is robust and capable of reliably detecting threats in real-world scenarios.

Real-Time Detection: The trained IDS is integrated into an interactive framework built with Gradio. This interface allows users to input network traffic parameters for real-time analysis. The system predicts potential threats and provides a confidence score, offering actionable insights for securing IoT networks To implement this project author has used 3 datasets such as KDDCUP, NSLKDD and the UNSW_NB15 dataset includes various types of attacks, such as Denial of Service (DoS), R2L, U2R, Probe, and others. Additional details can be found in the corresponding research paper.
Figure 2 illustrates the activity diagram of our Lightweight Intrusion Detection System (LIDS), which identifies intrusions by analyzing current behavior and comparing it to normal patterns. If any deviation is detected, an alarm is triggered.
It is composed of three phases:

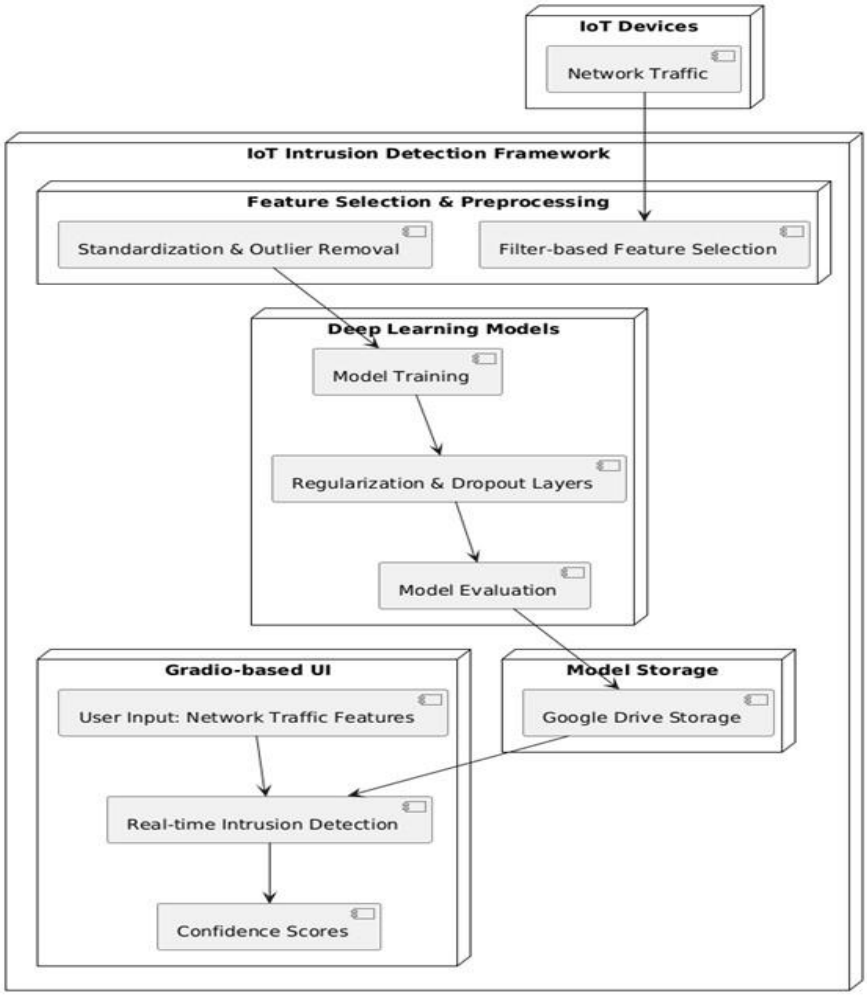


Fig 1:SYSTEM ARCHITECTURE

4. RESULTS AND DISCUSSIONS

The primary objective of this project is to develop a **Compact and Efficient Intrusion Detection System (IDS)** tailored specifically for IoT environments. The system aims to address the challenges posed by resource-constrained devices and evolving cyber threats by achieving the following:

- **Design a Lightweight IDS:** Develop a computationally efficient framework capable of operating on low-powered IoT devices without compromising their performance.
- **Leverage Machine Learning for Intrusion Detection:** Utilize advanced machine learning techniques to improve the accuracy and efficiency of intrusion detection, ensuring timely and reliable identification of threats.

- **Implement Feature Selection for Optimization:** Employ a filter-based feature selection method to reduce data dimensionality and computational overhead while retaining critical features for effective classification.
- **Evaluate and Optimize Classifiers:** Explore and compare multiple machine learning algorithms, such as Decision Tree (DT), Naïve Bayes (NB), and Support Vector Machine (SVM), to select the best-performing model for real-time intrusion detection.
- **Develop a Real-Time Detection System:** Create an interactive framework that allows real-time analysis of network traffic, providing actionable insights to detect and mitigate intrusions proactively.
- **Ensure Scalability and Adaptability:** Design the IDS to scale with growing IoT networks and adapt to new and evolving security threats.

Methodology

The project employs a structured methodology to develop a **Compact and Efficient IoT Intrusion Detection Framework**. The system is divided into distinct modules, each contributing to the overall functionality of the Intrusion Detection System (IDS). These modules ensure an organized and systematic approach, enhancing the project's effectiveness and scalability.

A. Data Collection and Preprocessing

Objective: Gather and prepare high-quality data for training and testing the IDS.

- **Data Collection:**
  - Identify and obtain relevant datasets containing IoT network traffic information (e.g., normal and malicious traffic data).
  - Use publicly available IoT datasets, such as the UNSW-NB15 or CICIDS datasets, to ensure diverse and comprehensive threat coverage.
- **Data Preprocessing:**
  - Remove missing or irrelevant entries to ensure data quality.
  - Normalize and scale the data to make it suitable for machine learning algorithms. o Label data to distinguish between normal traffic and intrusions.

B. Feature Selection

Objective: Reduce computational overhead by selecting the most relevant features for intrusion detection.

- **Filter-Based Feature Selection:**
  - Employ statistical methods such as correlation, Chi-square tests, or Information Gain to rank features based on their relevance.
  - Eliminate irrelevant or redundant features to optimize data dimensionality.
- **Output:** A reduced set of key features that retain critical information for accurate classification while minimizing resource usage.

C. Model Selection and Training

Objective: Evaluate multiple machine learning algorithms to identify the best-performing classifier.

- **Algorithm Exploration:**
  - Compare the performance of various classifiers, including:
    - Naïve Bayes (NB)
    - Decision Tree (DT)
    - Random Forest (RF)
    - K-Nearest Neighbor (KNN)
    - Support Vector Machine (SVM)
    - Multilayer Perceptron (MLP)

- **Model Evaluation:**
  - Use metrics such as accuracy, precision, recall, F1-score, and computational efficiency to assess each model.
  - Select the Decision Tree (DT) model based on its balance of high accuracy and low computational requirements.
- **Training and Validation:**

- Divide the dataset into separate training and validation sets. o Train the selected model on the training set and validate its performance using the validation set.

D. Real-Time Detection Module

Objective: Integrate the trained model into a framework for real-time intrusion detection.

- **Interactive Framework:**
  - Utilize a user-friendly interface (e.g., Gradio) to allow real-time analysis of network traffic.
  - Enable users to input network traffic parameters for detection.
- **Detection Process:**
  - Analyze incoming traffic using the trained Decision Tree model.
  - Predict potential threats and display results with a confidence score.

E. Performance Evaluation and Optimization

Objective: Test the system under various conditions to ensure reliability and robustness.

- **Testing:**
  - Evaluate the IDS on real-world IoT datasets to simulate diverse scenarios.
  - Measure metrics such as detection rate, false positive rate, and system latency.
- **Optimization:**
  - Fine-tune hyperparameters and feature selection criteria to enhance detection accuracy and reduce false positives. o Ensure the system operates efficiently within the computational limits of IoT devices.

F. Deployment and Scalability

Objective: Deploy the system in IoT environments and ensure its adaptability.

- **Deployment:** o Install the IDS in simulated IoT environments to validate its functionality.
  - Test integration with existing IoT devices and communication protocols.
- **Scalability:**
  - Design the system to accommodate increasing numbers of IoT devices without performance degradation. o Ensure adaptability to new and evolving security threats through periodic updates.

This modular methodology ensures that each component of the IDS is systematically developed, evaluated, and optimized, resulting in a lightweight, efficient, and accurate intrusion detection framework

5. CONCLUSION

The development of a compact and efficient IoT Intrusion Detection System (IDS) addresses critical security challenges in IoT environments, particularly the need for lightweight and accurate intrusion detection tailored to resource-constrained devices. By leveraging a filterbased feature selection method and evaluating multiple machine learning algorithms, the system achieves a balance between computational efficiency and high detection accuracy. The decision tree classifier was identified as the optimal model due to its superior performance metrics, making it a practical choice for IoT networks.

The proposed system offers several advantages, including low computational overhead, realtime detection capabilities, scalability, and user-friendly implementation using an interactive Gradio framework. It provides a robust defense mechanism against evolving cyber threats by analyzing network traffic and accurately identifying potential intrusions. Furthermore, the system demonstrates versatility by being adaptable to various IoT environments, such as smart homes, healthcare, and industrial IoT applications.

This project lays the foundation for future research in enhancing IoT security through advanced machine learning models, distributed architectures, and blockchain integration. By addressing the limitations of traditional IDS systems, this work contributes to the development of secure and resilient IoT networks, ensuring safer and more reliable interactions in the connected world

FUTURE SCOPE

In Future Work we will find out about different characteristic resolution techniques blended with extra laptop getting to know algorithms utilized to real-time statistics from IoT devices.

REFERENCES

[1] Atzori, L., Iera, A., Morabito, G. (2010). The Internet ofThings: A survey. Computer Network, 54(15): 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010
[2] Weiser, M. (1991). The computer for the 21st century.Scientific American, 265(3): 94-105.
[3]Sedjelmaci, H., Senouci, S.M., Al-Bahri, M. (2016).Lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology.IEEE ICC - Mobile and Wireless NetworkingSymposium. https://doi.org/10.1109/ICC.2016.7510811
[4] Raza, S.,Wallgren, L., Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. Ad HocNetworks, 11(8):2661-2674.https://doi.org/10.1016/j.adhoc.2013.04.014
[5] Anand, A., Patel, B. (2012). An overview on intrusiondetection system and types of attacks it can detectconsidering different protocols. International Journal ofAdvanced Research in Computer Science and SoftwareEngineering, 2(8): 94-98.
[6] Rajasegarar, S., Leckie, C., Palaniswami M. (2008).Anomaly detection in wireless sensor networks. IEEEWireless Communications, 15(4): 34 40.https://doi.org/10.1109/MWC.2008.4599219 [7]Li, W.C., Yi, P., Wu, Y., Pan, L., Li, J.H. (2014). A newintrusion detection system based on KNN classificationalgorithm in wireless sensor network. Journal ofElectrical and Computer Engineering, 2014: 8 pages.http://dx.doi.org/10.1155/2014/240217
[8]Thanigaivelan, N.K., Nigussie, E., Kanth, R.K., Virtanen,S., Isoaho, J. (2016). Distributed internal anomaly detection system for Internet-of-Things. 13th IEEEAnnual Consumer Communications & Networking Conference (CCNC).https://doi.org/10.1109/CCNC.2016.7444797
[9]Summerville, D.H., Zach, K.M., Chen, Y. (2015). Ultra-lightweight deep packet anomaly detection for Internet ofThings devices. 2015 IEEE 34th InternationalPerformance Computing and CommunicationsConference (IPCCC).https://doi.org/10.1109/PCCC.2015.7410342
[10] Huang, S.H. (2003). Dimensionality reduction inautomatic knowledge acquisition: A simple greedysearch approach. IEEE Transactions on Knowledge andData Engineering, 15(6): 1364-1373.https://doi.org/10.1109/TKDE.2003.1245278
[11] Zhao, K., Ge, L. (2013). A survey on the Internet ofThings security. in Int'l Conf. on ComputationalIntelligence and Security (CIS), pp. 663-667.https://doi.org/10.1109/CIS.2013.145
[12]Leo, M., Battisti, F., Carli, M., Neri, A. (2014). Afederated architecture approach for internet of things security. in Euro Med Telco Conference (EMTC), pp. 1-5.https://doi.org/10.1109/ EMTC. 2014. 6996632

Author's Profiles

G.UMA DEVI working as Assistant Professor in Department of CSE, Raghu Engineering college,Visakhapatnam

D.HITESH NAIDU B. Tech Computer Science and Engineering (AI-ML) in Raghu Institute of Technology , Visakhapatnam.

P.PRANATHI B. Tech Computer Science and Engineering (AI-ML) in Raghu Institute of Technology , Visakhapatnam.

D.SURESH B. Tech Computer Science and Engineering (AI-ML) in Raghu Institute of Technology , Visakhapatnam.

B.SAI KRISHNA B. Tech Computer Science and Engineering (AI-ML) in Raghu Institute of Technology , Visakhapatnam.