

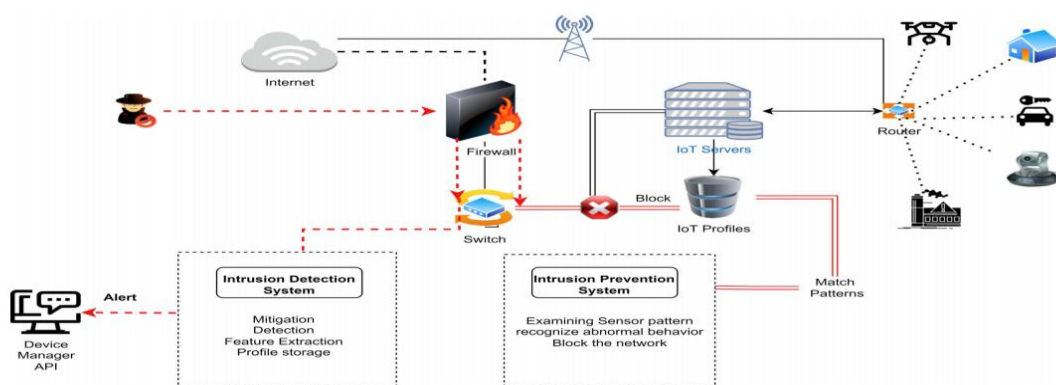
# ENSEMBLE-LEARNING FRAMEWORK FOR INTRUSION DETECTION TO ENHANCE INTERNET OF THINGS' DEVICES SECURITY

**Project Reference No.:** 47S\_BE\_3215

**College** : Sapthagiri College of Engineering  
**Branch** : Computer Science & Engineering  
**Guide(s)** : Prof. Chaitra P  
**Student(S)** : Ms. Poornima T  
Ms. S Mehak Afreen  
Ms. Sahana N  
Ms. Shreya Shetty S

## Introduction:

The Internet of Things (IoT) has grown exponentially due to technology's evolution. The IoT facilitates people's lives by providing and enhancing connectivity that supports the automation aspect of several human services. Millions of interconnected devices use the IoT to communicate, transfer, share, collect, and analyze data from several domains. While involving the internet as the main factor in the technology's fields, it opens a new platform for cybercriminals. Therefore, enhancing security and employing artificial intelligence innovations and technologies led to a protected and reliable IoT infrastructure. In addition, the IoT architecture contains three main layers: the application, network, and user experience levels. The Perception layer has responsibility for every task, from utilizing the sensors to gathering the information, but it is also susceptible to multiple attacks due to its central role. Physical attacks on sensor-equipped equipment, unauthorized entry into the infrastructure, and other forms of physical attack are prevalent. The Network layer allows the devices fitted with sensors to communicate and exchange data with the gateways and other IoT devices via wireless technologies such as Wi-Fi, 3G, and 4G. The most common attacks faced by the Network layer are distributed denial-of-service (DDoS), denial-of-service (DOS), Man of the Middle, information theft, and gateways attacks.



IDS Architecture

The major contributions of the project are summarized as follows:

- Proposing a binary classification of IoT device network traffic as normal or abnormal.
- Applying feature selection methods to improve the IDS performance of IoT network devices. Hence, we examined multiple ML algorithms to determine the most accurate and efficient learners for building an efficient IDS to detect attacks on IoT devices within IoT network data.
- Constructing and assessing four supervised models using data preprocessing and feature selection methods. This group of models consists of Naive Bayes, SVM, Random Forest, Adaboost. In addition, by combining the four supervised ML models, we employ ensemble methods to improve the efficiency of the proposed model. The performance evaluation includes accuracy, precision, recall, and F1-score metrics.
- The model we constructed improved the performance of the detection technique compared with the most recent study that used the same dataset.

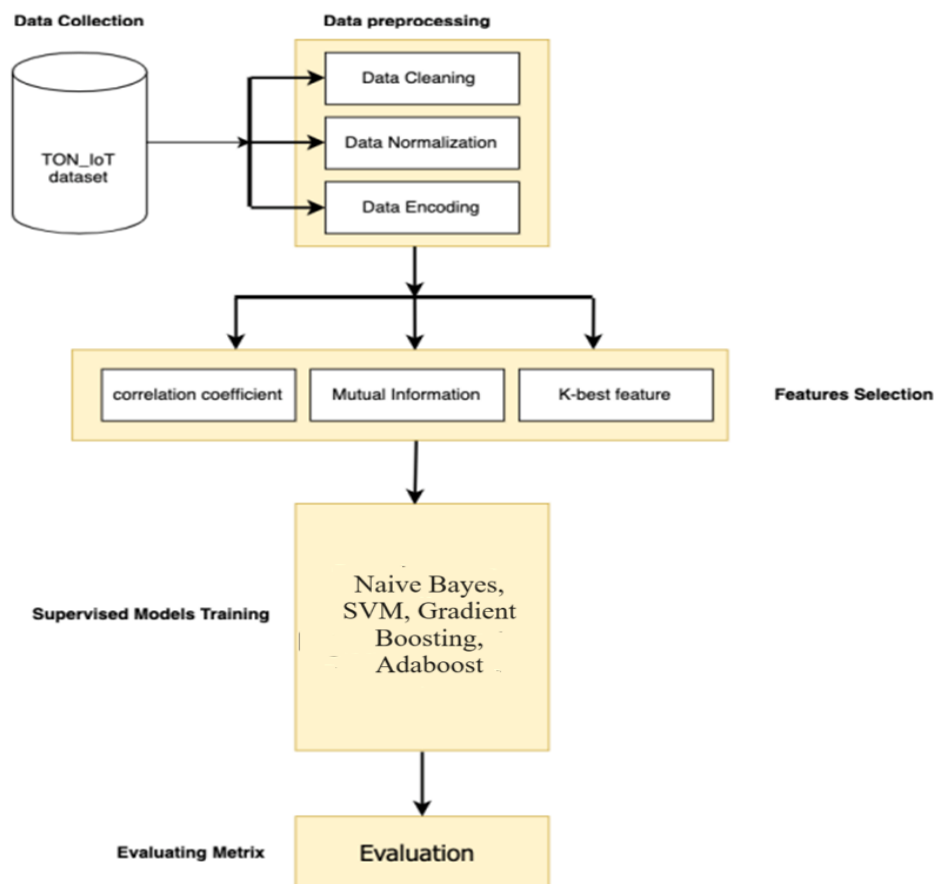
### **Objectives:**

- To implement an efficient network intrusion detection system in IOT network.
- Utilize real-world IoT network traffic datasets for comprehensive testing and validation.
- Enhance data reliability through rigorous testing and authentication procedures.
- Implement data preprocessing techniques to clean and prepare the dataset for analysis.
- Explore feature extraction methods to identify and prioritize relevant network traffic attributes. To Design and implement multi-class classification algorithms for efficient intrusion detection.
- Investigate the efficacy of different feature selection algorithms to optimize model performance.
- Evaluate the performance of the NIDS using standard metrics such as F1-score, recall, accuracy, and precision.
- Compare the performance of various machine learning algorithms to identify the most effective approach.
- Provide insights into network security by analyzing and interpreting the results of intrusion detection experiments.
- To identify different types of attacks.

### **Methodology:**

This project propose a binary classification of network traffic from the Internet of Things devices as normal or abnormal. We implemented feature selection algorithms to enhance the IDS performance in the IoT devices. Therefore, since our goal is to construct an effective IDS that can detect attacks on Internet of Things devices within the IoT network dataset, we examined a variety of machine learning algorithms to choose which models were the most accurate and efficient learner. Using the scaling of the data and the selection of features, we construct and evaluate four supervised models. Naive Bayes, SVM, Random Forest, Adaboost are the models that are included in the proposed model. In addition, to improve the effectiveness of our method for attack detection, we employ two ensemble methods to

improve the efficiency of the proposed model. The performance evaluation includes accuracy, precision, recall, and F1-score metrics.



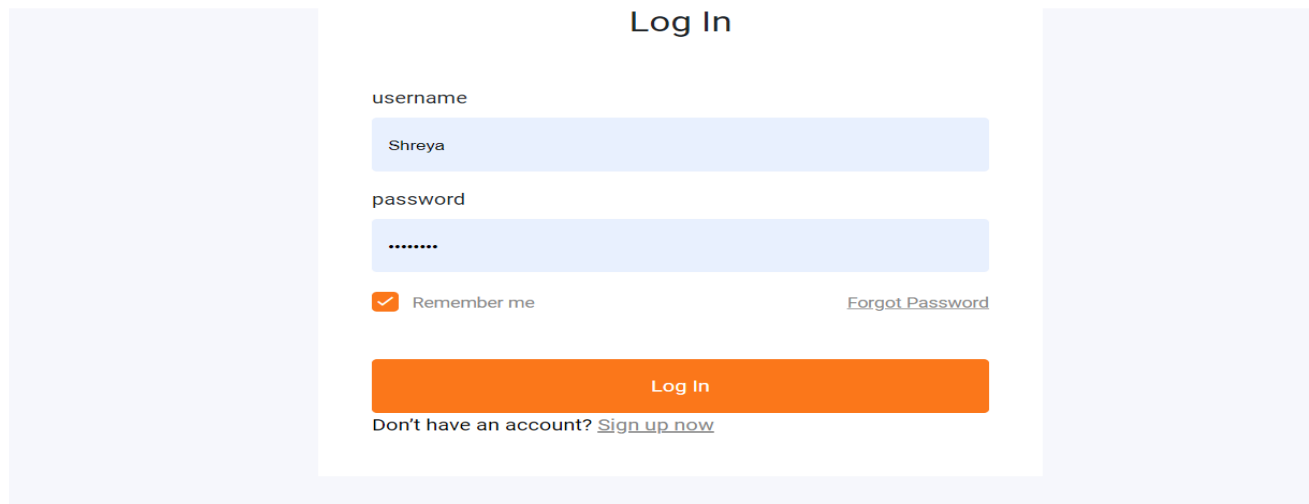
1.Data Preparation: The TON IoT network traffic dataset originates from real-world IoT scenarios at UNSW Canberra Cyber lab, tested and authenticated for reliability. Collected from multiple IoT devices, it's suitable for machine learning applications.

2. Data Preprocessing: Removing random data like '-' and replacing missing values with medians for robustness. Categorical features were encoded using Label Encoding. Standardization and normalization were applied to handle wide-ranging attribute values, with min-max scaling used for several features.

3. Feature Extraction: Various feature selection algorithms such as Mutual Information, Pearson Coefficient Correlation, and K-Best were evaluated to simplify the training process by eliminating irrelevant or redundant data points, aiding in anomaly detection.

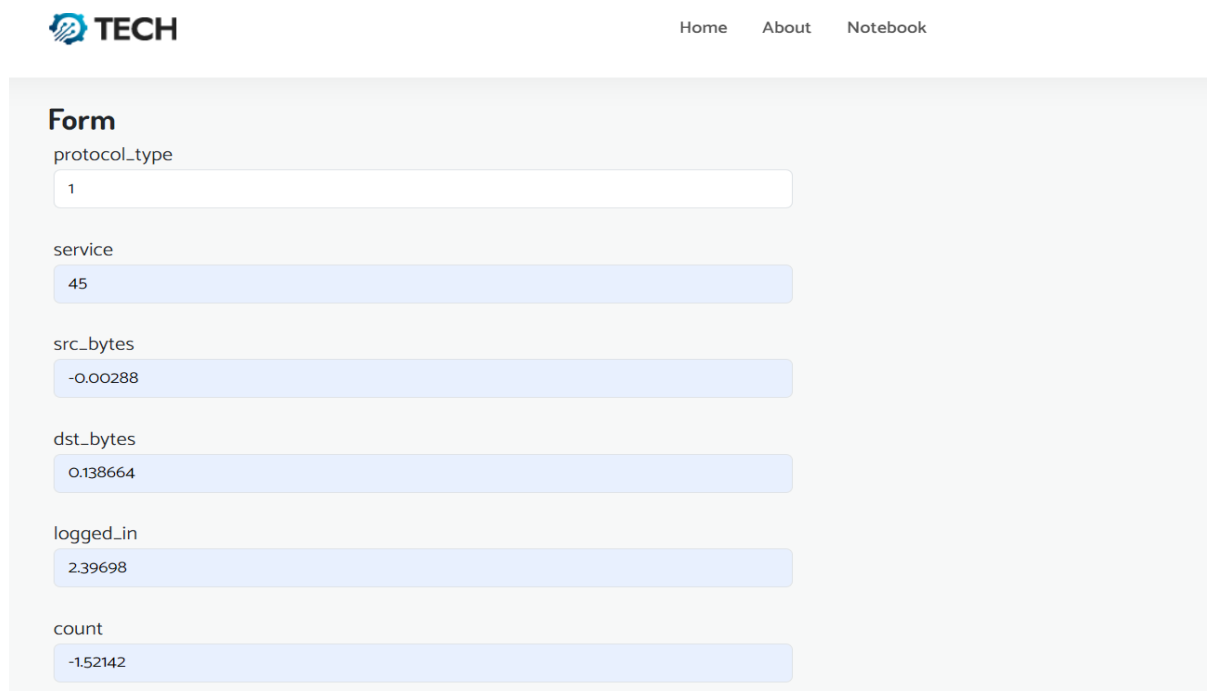
4. IDS Detection: Learning models are compared based on traditional performance metrics like F1-score, recall, accuracy, and precision. Models trained using machine learning bias algorithms are evaluated against standard evaluation parameters.

## Results:



A screenshot of a web application's login page. The page has a light gray background with a white central container. At the top of the container, the text "Log In" is centered. Below it, there are two input fields: "username" with the value "Shreya" and "password" with masked characters ".....". To the left of the password field is a checked checkbox labeled "Remember me". To the right is a link "Forgot Password". Below these fields is a large orange button labeled "Log In". At the bottom, there is a link "Don't have an account? Sign up now".

Fig : Login Page



A screenshot of a web application's GUI. At the top left is a logo with a blue circular icon and the text "TECH". To the right are navigation links: "Home", "About", and "Notebook". Below the navigation is a section titled "Form" containing several input fields with numerical values: "protocol\_type" (1), "service" (45), "src\_bytes" (-0.00288), "dst\_bytes" (0.138664), "logged\_in" (2.39698), and "count" (-1.52142).

Fig: GUI

Result

Result: **There is an No Attack Detected, it is Normal!**

Fig: No Attack

Deep Learning based Anomaly Detection for Fog-Assisted IoT Network

Result

Result: **There is an Attack Detected, Attack Type is DDoS!**

Fig: Attack is DDoS

Result

**Result: There is an Attack Detected, Attack Type is R2L!**

Fig: Attack is R2L

Result

**Result: There is an Attack Detected, Attack Type is Probe!**

Fig: Attack is Probe

**Conclusion:**

Here we propose an architecture using the network IDS and machine learning to build an Intelligent Network Intrusion Detection and Prevention System with dynamic rule updation creating robust and secure system with reduced resource consumption which can be used in Domestic Networks. The objective of the proposed system, is to detect malicious patterns in real-time traffic data and take action by dynamically updating network rules. By deploying a machine learning models in parallel and dynamically enabling rules, resource consumption of network can be reduced and optimized.

**Scope for future work:**

- Address the challenge of imbalanced datasets in intrusion detection by employing techniques such as oversampling, undersampling, or using ensemble methods specifically designed for imbalanced data.
- Extend the framework to detect not only known attacks but also novel or zero-day attacks by focusing on anomaly detection techniques within the ensemble learning paradigm.
- Integrate the ensemble learning framework with existing IoT security protocols and standards to provide a comprehensive security solution for IoT ecosystems.
- Explore techniques to extract and select relevant features from IoT device data, considering both network traffic and device behavior patterns.