CSC 544 Internet of Things

Final Project Proposal

Project Title: Anomaly Detection in IoT Networks

1. Introduction

Anomaly detection in cybersecurity, especially concerning IoT devices, has become increasingly crucial due to the rising number of interconnected devices and the growing threat landscape. The IoT-23 dataset, provided by the Stratosphere Laboratory, offers a unique opportunity to delve into anomaly detection challenges within IoT networks. This project is part of the research under “Machine Learning and Deep Learning Methods for Better Anomaly Detection in IoT-23 Dataset Cybersecurity”. The research paper proposed an anomaly detection system model for IoT security with the implementation of ML/DL methods, including Naïve Bayes, SVM, Decision Trees, and CNN. This proposal aims to address the existing problem of efficiently and accurately detecting anomalies in IoT network traffic.

1.1 Motivation and Problem Description:
The widespread adoption of IoT devices introduces new security challenges. These devices often have limited processing power and weak security protocols, making them vulnerable to attacks. Anomaly detection helps identify and prevent malicious activities within IoT networks by distinguishing normal network traffic patterns from abnormal ones.

1.2 Existing Solutions:
Several approaches exist for anomaly detection in IoT networks, including signature-based and anomaly-based methods. Signature-based techniques identify known attack patterns but are ineffective against novel attacks. Anomaly-based methods, utilizing machine learning and deep learning models, offer greater flexibility in detecting unknown threats. Existing research explores various models like Naive Bayes, SVM, and Decision Trees with promising results. However, there is a continuous effort to improve detection accuracy and efficiency.

1.3 Proposed Solution:
We propose to explore a hybrid approach combining convolutional neural networks (CNN), support vector machines (SVM), decision trees, and naïve Bayes classifiers for anomaly detection in IoT-23 dataset cybersecurity. Each model will be tailored and optimized for the specific characteristics of IoT network traffic.

2. Approaches

2.1 Framework and Algorithms:

We propose a framework that utilizes various machine learning and deep learning algorithms for anomaly detection on the IoT-23 dataset. The framework will involve the following stages:
- Data Preprocessing
- Model Training
- Model Evaluation
- Comparison and Analysis

The algorithmic framework involves preprocessing the IoT-23 dataset to handle missing values, normalize features, and extract relevant features for model training. Subsequently, the CNN model will be utilized to capture spatial dependencies within the network traffic data. SVM will focus on separating normal and anomalous instances in a high-dimensional feature space, while decision trees and naïve Bayes classifiers will provide interpretable and probabilistic anomaly scores, respectively.

Experiments will involve evaluating the performance of individual models and the hybrid approach using metrics such as accuracy, precision, recall, and F1-score. Additionally, comparative analysis with existing state-of-the-art methods will be conducted to showcase the effectiveness of our proposed solution.

2.2 Experiments:

We will conduct the following experiments:

- Individual Model Evaluation
- Comparative Analysis

3. Research Plan

Timeline:

- **Week 1:** Literature review on anomaly detection in IoT networks and machine learning/deep learning algorithms for anomaly detection.
- **Week 2:** Data preprocessing and exploration of the IoT-23 dataset.
- **Week 3:** Model implementation and training (Naive Bayes, SVM, Decision Tree, and CNN).
- **Week 4:** Model evaluation and performance analysis.
- **Week 5:** Comparative analysis and documentation.
- **Week 6**: Report writing and finalization.

4. References

1. A. Parmisano, S. Garcia, and M.J. Erquiaga, "IoT-23: A labeled dataset with malicious and benign IoT network traffic," Stratosphere IPS, Jan. 22, 2020, https://www.stratosphereips.org/datasets-iot23.
2. Li, Y., Lin, H., & Han, Z. (2020). "A Survey on Anomaly Detection in Internet of Things". IEEE Internet of Things Journal, 7(1), 696-706.
3. "Introduction to Anomaly Detection in IoT" by Towards Data Science.

Team Members:

Lalitha Priya Bijja – 101168225
Venkata Surya Deepak Lakshimpalli - 101143451