**Sinhgad College of Engineering**

**Proj. Gr. No.:** 27

Department of Computer Engineering Project Approval Form Year: 2019-20 (To be filled by students) **Review Committee Members:** Prof. M. R. Dhage, Prof. E. Jayanthi, Prof. A.S. Kalaskar

**Date:** 9/8/2019

**Title of Project:** Intrusion detection system for IOT devices

**Domain according to ACM-CCS Classification:** Network/ Cyber Security

**No. of IEEE / Equivalent Technical papers referred:** 6

**Title of Review Paper-1:** Anomaly based intrusion detection system through feature selection analysis and building hybrid efficient model

**Name of publication with Year:** Journal of computational science 25(2018) 152-160

**Seed Idea:** This paper proposes an anomaly based intrusion detection system using network transactions. It uses hybrid machine learning model on NSL-KDD dataset. It shows a high accuracy for intrusion detections; however, it is not implemented for IOT devices.

**Title of Review Paper-2:** Towards Machine Learning Based IoT Intrusion Detection Service

**Name of publication with Year:** Springer International Publishing AG, part of Springer Nature 2018

**Seed Idea**: This paper proposes an Intrusion Detection System for IOT devices based on machine learning techniques. They used Random forest as a classiﬁer to detect intrusions, then applied neural network classiﬁer to detect the categorization of the detected intrusion. As a downside, it uses cloud computing, which increases the resource requirements like connection to the internet and cloud services(which are payment based).

**Title of Review Paper-3:** Distributed attack detection scheme using deep learning approach for Internet of Things

**Name of publication with Year:** Future Generation Computer Systems (2017)

**Seed Idea:** When it comes to detecting intrusions in IOT devices, traditional machine learning models cannot guarantee accuracy. Hence, in this paper deep learning is used to train the IDS system as it is found to be more effective compared to its shallow counter parts. However, this system is signature based, meaning if a new attack occurs whose behavior is not previously classified as an attack, the system cannot recognize it.

**Project Approval Review Committee**

**Report Review Committee Members:** Prof. M. R. Dhage, Prof. E. Jayanthi, Prof. A.S. Kalaskar

**Date:**9/8/2019

**Names of modules for proposed system:**

1) IOT nodes – The components being attacked. Gathers and relays data to the Intrusion detection system.

2)Intrusion detection system – machine learning model which actually processes the data and decides if it is an attack or not

a) training module – train the model using the dataset

b) testing module – test the model, try to improve accuracy

c) processing module – process the data and decide whether it is normal or anomaly

3) Front end – for displaying detection notification and user interface

**Platforms and Tools planned to use for implementation:** Wireshark, Visual Studio Code, Python, Python libraries.

**Identification of Input Dataset:** DS2OS traffic traces dataset.

This datasets contains communications between different IoT nodes. It contains 358k rows with following 13 columns:

sourceID, sourceAddress, sourceType, sourceLocation, destinationServiceAddress, destinationServiceType, destinationLocation, accessedNodeAddress, accessedNodeType, operation, value, timestamp, normality

**Any other requirement:** IOT nodes for demonstration

**Abstract**

IoT devices are becoming popular day-by-day. Several vulnerabilities in IoT present the need for IoT security. The number of attacks on these devices keep increasing and most of them are slight variations of the previously known attacks, which can bypass the conventional firewall systems.

The existing systems are not suitable for IOT devices as IOT devices have low computational power. Those that use signature-based intrusion detection. It works only on known patterns and attacks, hence they cannot recognize newer attacks with unknown pattern. Also, many systems use cloud computing, which has a downfall that it needs access to internet at all times, also the cloud services are most often paid.

In the proposed system, we are planning to use anomaly-based detection system. The anomaly-based intrusion detection system comes into effect when detecting newer attacks, that are not filtered by the firewall. It is capable of handling newer/unknown attacks, which signature based cannot. Also we are setting up the IDS on a local higher powered device rather than on cloud. Machine learning ensemble model Random forest is used. The model will be trained on the DS2OS traffic traces dataset.

**System overview diagram**

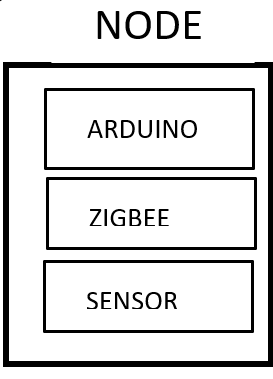
NODE

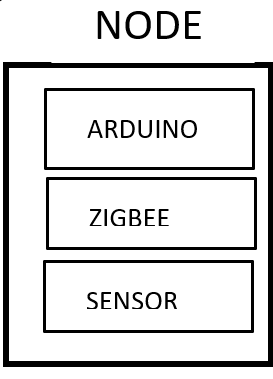
ARDUINO

INTERNET



GATEWAY





FRONTEND

DATABASE

IDS

ZIGBEE

SENSOR

FIREWALL