# Proposal _Guoyachao.pdf

*by* yachao guo

**Submission date:** 18-Apr-2025 11:05AM (UTC-0700)
**Submission ID:** 2649972448
**File name:** Proposal__Guoyachao.pdf (225.5K)
**Word count:** 722
**Character count:** 4171

UTM UNIVERSITI TEKNOLOGI MALAYSIA

SCHOOL OF COMPUTING
Faculty of Engineering

Project Proposal Form MCST1043
Sem: 2 Session: 2024/25

## SECTION A: Project Information.

Program Name: **Masters of Science (Data Science)**

Subject Name: **Project 1 (MCST1043)**

Student Name: Guo Yachao

Metric Number: MCS241039

Student Email & Phone: guoyachao@graduate.utm.my & +601116787971

Project Title: Detection of network anomalies in smart home Internet of Things

Supervisor 1:

Supervisor 2 / Industry Advisor(if any):

## SECTION B: Project Proposal

**Introduction**:

The modern technological era has been completely changed by the Interne to provide daily conveniences at our fingertips. The Internet of Things --IoT is a technology that has transformed modern development concepts. The Internet of Things has been applied to agriculture, catering, roads, and our homes. Applications which is based on IoT are called as smart applications. Smart homes are equipped with IoT devices which can capture and utilize smart sensors and controllers to manage various areas of the home. These sensors communicate via internet connections. These devices share data with specific tasks and objectives, including recognition, perception, communication,service, and semantics.

**Problem Background**:

In this technological modern era , the Internet of Things has permeated every aspect of life that includes smart scenarios, smart homes, and even intelligent spaces. Smart homes are equipped with plenty of continuously operating IoT devices, without any interruptions. A peaceful living environment can be provided by these smart devices with the security and authentication. Monitoring the activities by smart IoT devices is crucial for ensuring their trouble-free operation.

**Problem Statement**:

The increasing number of IoT applications has made smart devices low cost, energy saving, and even compact. Though the rise in the use about IoT devices adds the risk factors and threats to the network as well. Ensuring

the security and threat-free use of these devices is crucial,therefore people can safely employ these networks in smart homes.

**Aim of the Project**:
This project proposes a machine learning that is based on smart home anomaly detection method and that is Detecting the abnormal and normal behaviors about IoT device traffic, so as to identify malicious activities such as external attacks and attempts.

**Objectives of the Project**:
1.To collect data sets that contain more types of malicious behavior characteristics.
2.To preprocess the data by data cleaning, feature selection and even data balancing.
3.To convert the data into feature vectors through label coding.
4. To select a variety of machine learning methods.
5.To detect network anomalies in the Internet of Things by using Multiple machine learning methods.

**Scopes of the Project**:
In this study,the data set collected is a refined UNSW BoT IoT data set that has been widely used by researchers, and various machine learning methods such as AdaBoost, decision tree, random forest, autoencoder and artificial neural network are used.

**Expected Contribution of the Project**:
This research work is to use machine learning methods based on feature selection to identify malicious patterns in traffic, so as to provide an important contribution for iot devices to resist external attacks. So, user security , privacy and even security can be safeguard.

**Project Requirements**:

Software: Python, TensorFlow, PyTorch, Scikit-learn, Jupyter Notebook

Hardware: CPU: Minimum Intel i6 or AMD Ryzen 6;Storage≥ 256GB SSD
GPU (Optional):Minimum NVIDIA GTX 1050 Ti

Technology/Technique/ Methodology/Algorithm: AdaBoost, Ada Boost, Auto Encoder, and Random Forest, Artificial Neural Network,Decision Tree

**Type of Project (Focusing on Data Science)**:

[ √ ] Data Preparation and Modeling
[ √ ] Data Analysis and Visualization
[ ] Business Intelligence and Analytics
[ √ ] Machine Learning and Prediction
[ ] Data Science Application in Business Domain

**Status of Project**:

[ √ ] New

[ ] Continued

If continued, what is the previous title?

## SECTION C: Declaration

**I declare that this project is proposed by**:

[ √ ] Myself

[ ] Supervisor/Industry Advisor ( )

Student Name: Guo Yachao

April 17, 2025

**Signature** **Date**

## SECTION D: Supervisor Acknowledgement

The Supervisor(s) shall complete this section.

**I/We agree to become the supervisor(s) for this student under aforesaid proposed title.**

2

Name of Supervisor 1:

**Signature** **Date**

Name of Supervisor 2 (if any):

**Signature** **Date**

## SECTION E: Evaluation Panel Approval

The Evaluator(s) shall complete this section.

**Result:**

[ ] FULL APPROVAL [ ] CONDITIONAL APPROVAL (Major)*

[ ] CONDITIONAL APPROVAL (Minor) [ ] FAIL*

***** Student has to submit new proposal form considering the evaluators' comments.

1

**Comments:**

Name of Evaluator 1: .....

**Signature** ..... **Date** .....

Name of Evaluator 2: .....

**Signature** ..... **Date** .....

# Proposal _Guoyachao.pdf

ORIGINALITY REPORT

| 5% | 3% | 1% | 3% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | Submitted to The Chartered Institute of Procurement & Supply<br>Student Paper | 2% |
| 2 | www.coursehero.com<br>Internet Source | 2% |
| 3 | Dutta, Indira Kalyan. "A High-Performance Lightweight Polymorphic Encryption System for Constrained Internet of Things (IoT) Devices", University of Louisiana at Lafayette, 2024<br>Publication | 1% |

| | | | |
|---|---|---|---|
| Exclude quotes | On | Exclude matches | Off |
| Exclude bibliography | On | | |