"An Efficient Spam Detection Technique for IoT Devices using Machine Learning"

Guided By:

Prof. P. S. Gayke

Presented By:

1. Nikhil Bhor
2. Gaurav Bhise
3. Jagdish Bhagwat
4. Tanvi Alkute

Contents

- Problem Statement
- Abstract
- Introduction, Purpose, Scope, Objectives
- Literature Survey
- System Overview-Proposed System & Proposed Outcome
- Algorithm Details
- System Architecture Diagram & Design DFD Diagrams (Level 0, Level 1)
- System Requirements (H/W, S/W)
- References

Problem Statement

- To address the aforementioned challenges, we proposed a novel algorithm and build an web-based application for the detection of spam from different IoT devices dataset.
- In Proposed studies shows that the problem definition gets more specific for any attack type and includes an expanded definition of the attack and its behavior. Further, we confirmed that the performance of neural network increases with increase in accuracy and performance of algorithms.

Abstract

- Spam Detection System
- Information Security.
- Authentication, Verification
- Data Security and Privacy.
- Machine Learning Technology.
- Multilevel Security.
- This makes the data secure.

Introduction

- The Internet and computer networks have become an important part of our organizations and everyday life. With the increase in our dependence on computers and communication networks, malicious activities have become increasingly prevalent.
- Spam Detection are an important problem in today’s communication environments. The network traffic must be monitored and analyzed to detect malicious activities and attacks to ensure reliable functionality of the networks and security of users’ information.
- Recently, machine learning techniques have been applied toward the detection of network attacks or spam. Machine learning models are able to extract similarities and patterns in the network traffic.

Purpose

- As part of the recommended approach, the spammy characteristics are detected. ML models are used in Internet of things. This is the IoT data. it is pre-processed with the aid of pattern development method. By playing around with the structure, each IoT device is rewarded with ML models. The amount of spamming that has been detected As a result, the criteria for success have been refined. IoT equipment operating in a smart house As we go forward, will take into account meteorological conditions as well as the environment IoT devices more secured and reliable.

Scope of Project

- We propose the security of IoT devices by detecting spam using machine learning. To achieve this objective, Spam Detection in IoT using a Machine Learning framework is proposed. In this framework, machine learning models are evaluated using various metrics with a large collection of inputs features sets.

Objectives

- The proposed scheme of spam detection is validated using five different machine learning models.
- An algorithm is proposed to compute the spamicity score of each model which is then used for detection and intelligent decision making.
- Based upon the spamicity score computed in previous step, the reliability of IoT devices is analyzed using different evaluation metrics.
- To detect network attacks by applying machine learning methods.
- To reduce operational time.
- To increase accuracy and reliability.
- To increase operational efficiency.
- To provide data security.

Literature Survey

Sr. No.	Title	Publication & Year	Authors	Findings
01	Blockchain and Smart Contract for Digital Certificate.	*IEEE ICASI 2018*	Jiin-Chiou Chen, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen	In this paper study on how digital certificate validation & verification.
02	Security Applications and Challenges in Blockchain.	*IEEE 2019*	Austin Draper, Aryan Familrouhani, Devin Cao, Tevisophea Heng, Wenlin Han	In this paper, we study popular security applications in Blockchain
03	Certificate Validation through Public Ledgers and Blockchain.	*ITASEC 2017*	Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni and Luca Spalazzi	In this paper we stuied the issues and challenges of Certificate Validation through Public Ledgers and Blockchains.

Literature Survey

Sr. No	Title	Publication & Year	Authors	Findings
04	BlockSIM: A practical simulation tool for optimal network design, stability and planning.	*IEEE 2019*	Santosh Pandey, Gopal ojha, Rohit Kumar and Bikesh Shresha	Here a comprehensive and open source blockchain system simulation tool which can assist blockchain architects better evaluate the performance of planned private blockchain networks.
05	Proof-of-Propert y - A Lightweight and Scalable Blockchain Protocol.	*IEEE 2018*	Christopher Ehmke, Florian, Christoph M. Friedrich	In this paper is based on the idea of Ethereum to keep the state of the system explicitly in the current block.

Existing System

- The safety measures of IoT devices depends upon the size and type of organization in which it is imposed. The behavior of users forces the security gateways to cooperate. In other words, we can say that the location, nature, application of IoT devices decides the security measures.
- For instance, the smart IoT security cameras in the smart organization can capture the different parameters for analysis and intelligent decision making. The maximum care to be taken is with web based devices as maximum number of IoT devices are web dependent. It is common at the workplace that the IoT devices installed in an organization can be used to implement security and privacy features efficiently.

Disadvantages of Existing System

- Low Data Accessibility.
- Server Un-Available.
- Server not found.
- Server Issues.
- When hit number of node at time then load on server.
- Server accept and process only one node at a time.

Proposed System

- The proposed scheme of spam detection is validated using five different machine learning models.
- An algorithm is proposed to compute the spamicity score of each model which is then used for detection and intelligent decision making.
- Based upon the spamicity score computed in previous step, the reliability of IoT devices is analyzed using different evaluation metrics.
- Our main goal is that the task of finding spams is fundamentally different from these other applications, making it significantly harder for the intrusion detection community to employ machine learning effectively.
- Hence, efficient adaptive methods like various techniques of machine learning can result in higher detection rates, lower false alarm rates and reasonable computation and communication costs..

Proposed Outcome

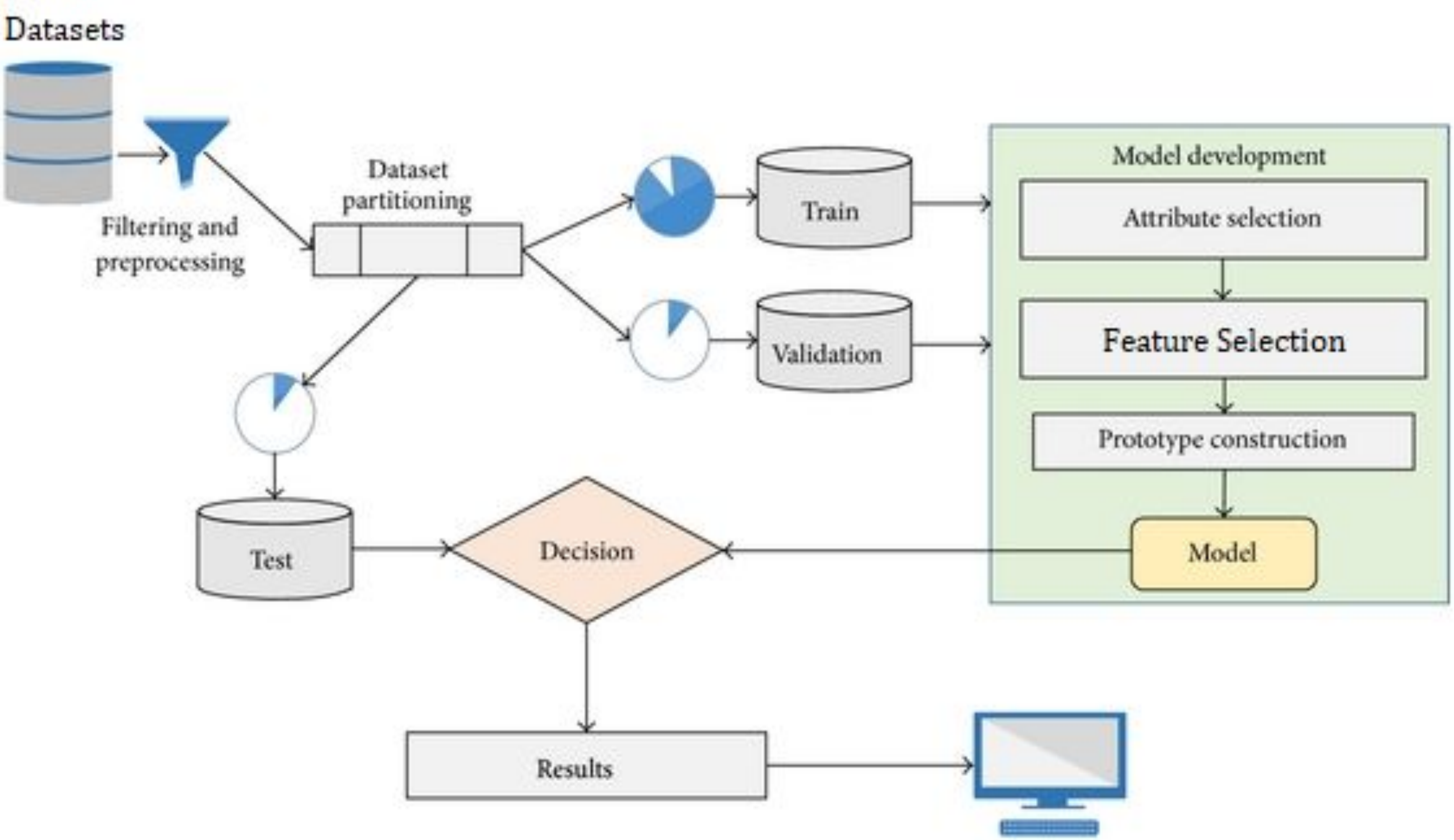
- We propose the security of IoT devices by detecting spam using machine learning.
- To achieve this objective, Spam Detection in IoT using a Machine Learning framework is proposed.
- In this framework, machine learning models are evaluated using various metrics with a large collection of inputs features sets.

Algorithm

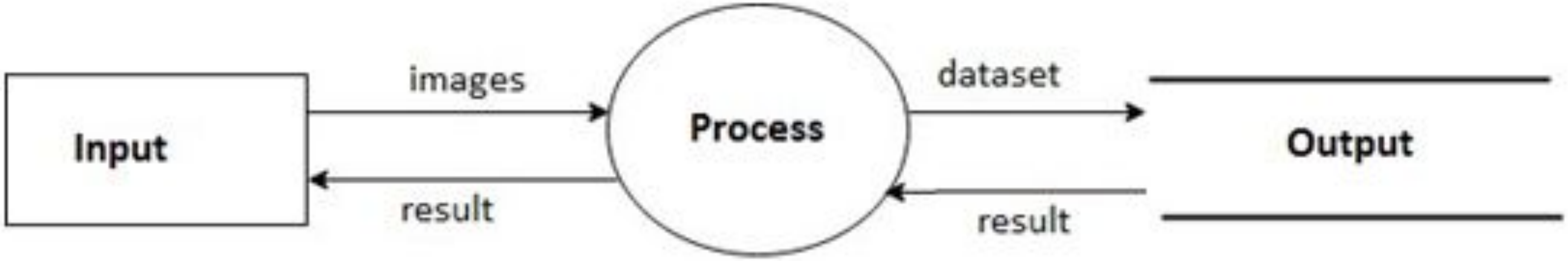
Here we design and develop An Efficient Spam Detection Technique for IoT Devices using Machine Learning.

- Novel Classification Algorithm
- Feature Selection
- Feature Extraction

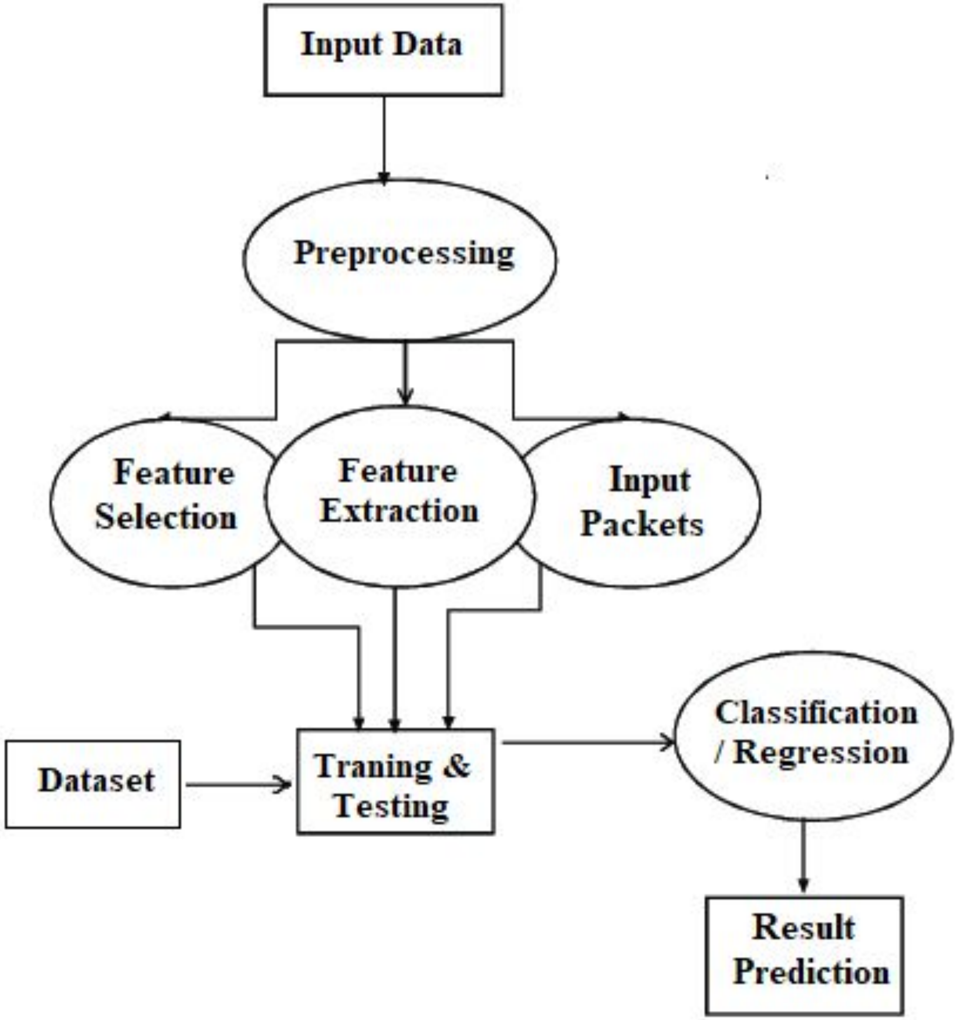
System Architecture Diagram



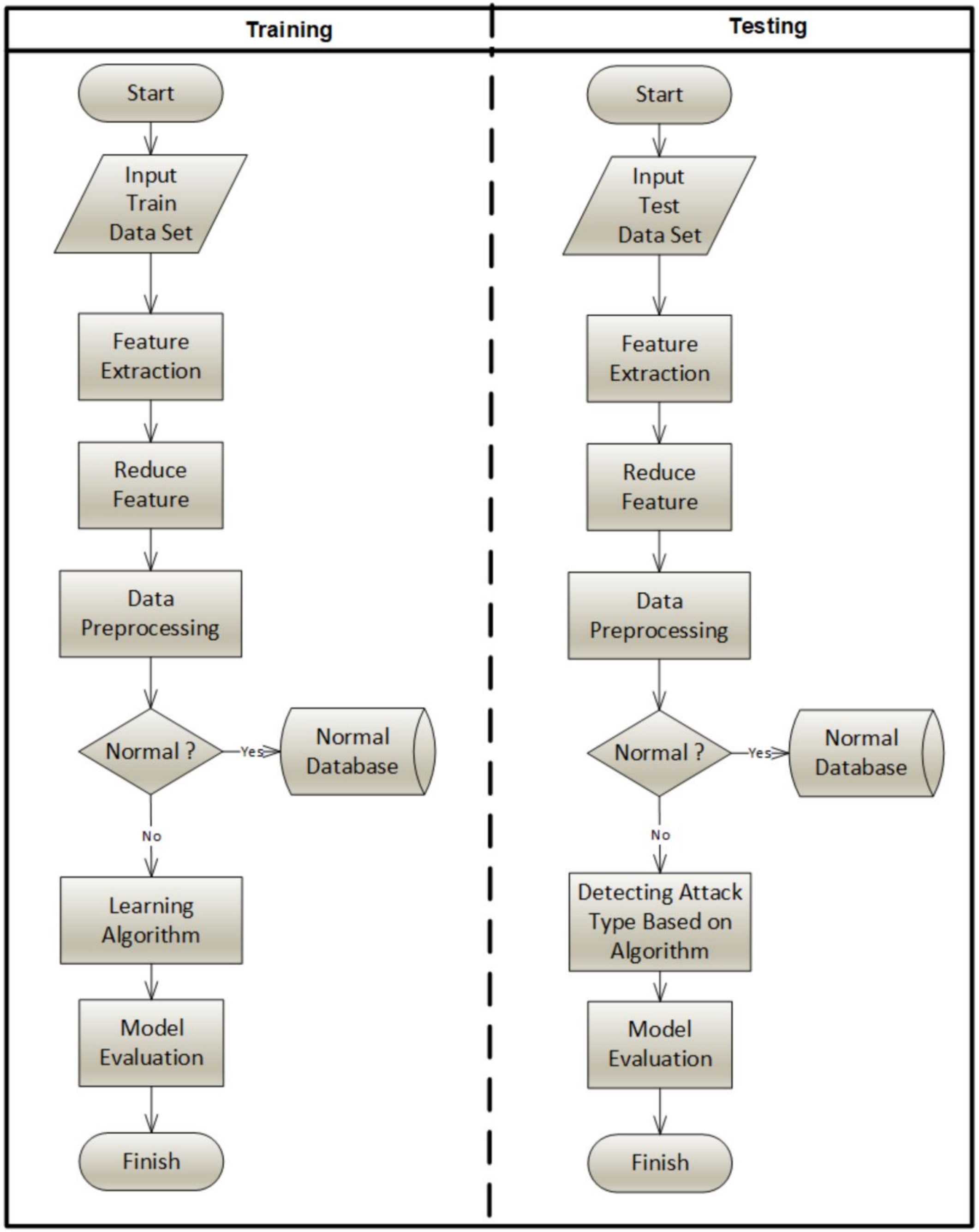
Design DFD Diagrams – Level 0



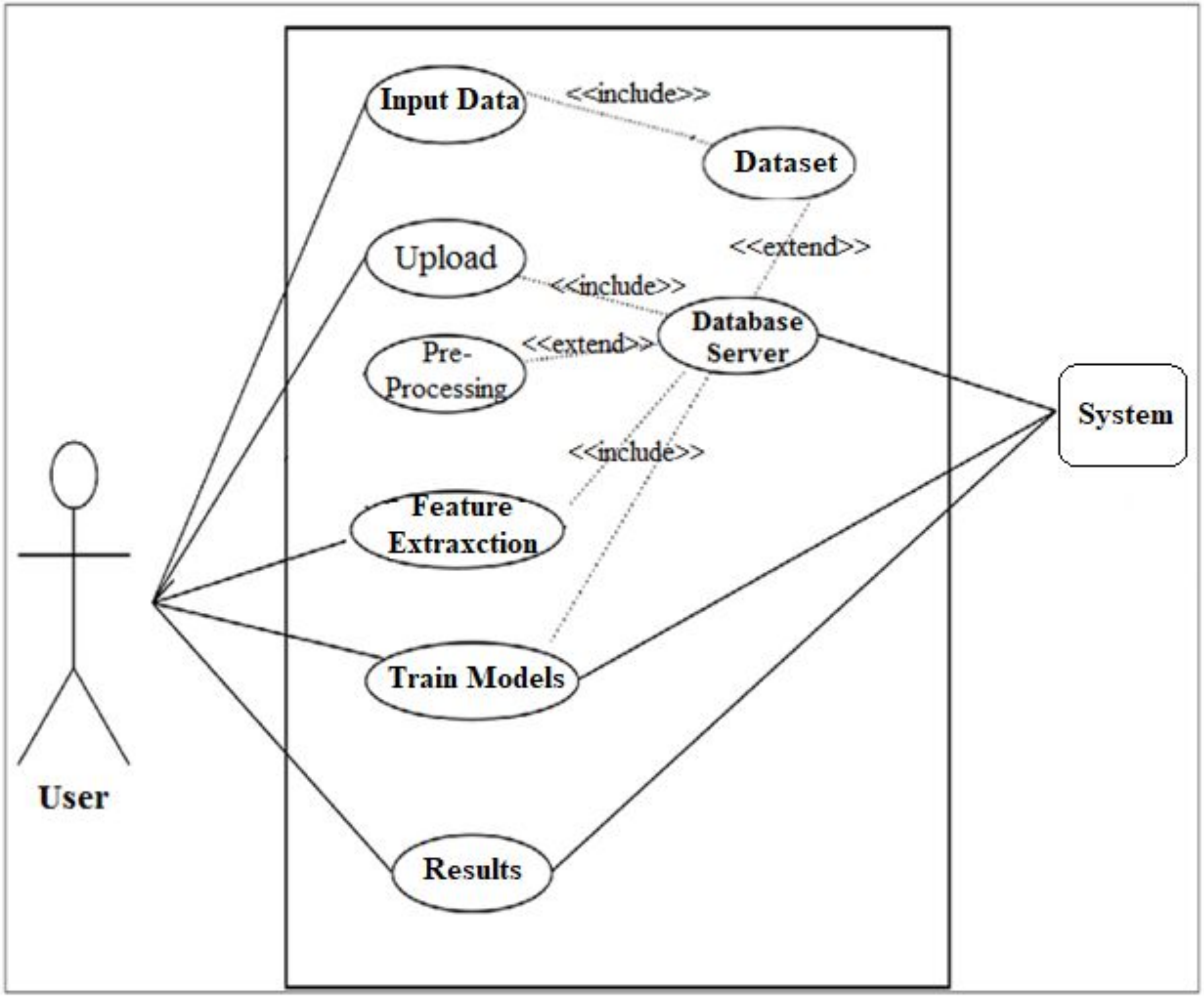
Design DFD Diagrams – Level 1



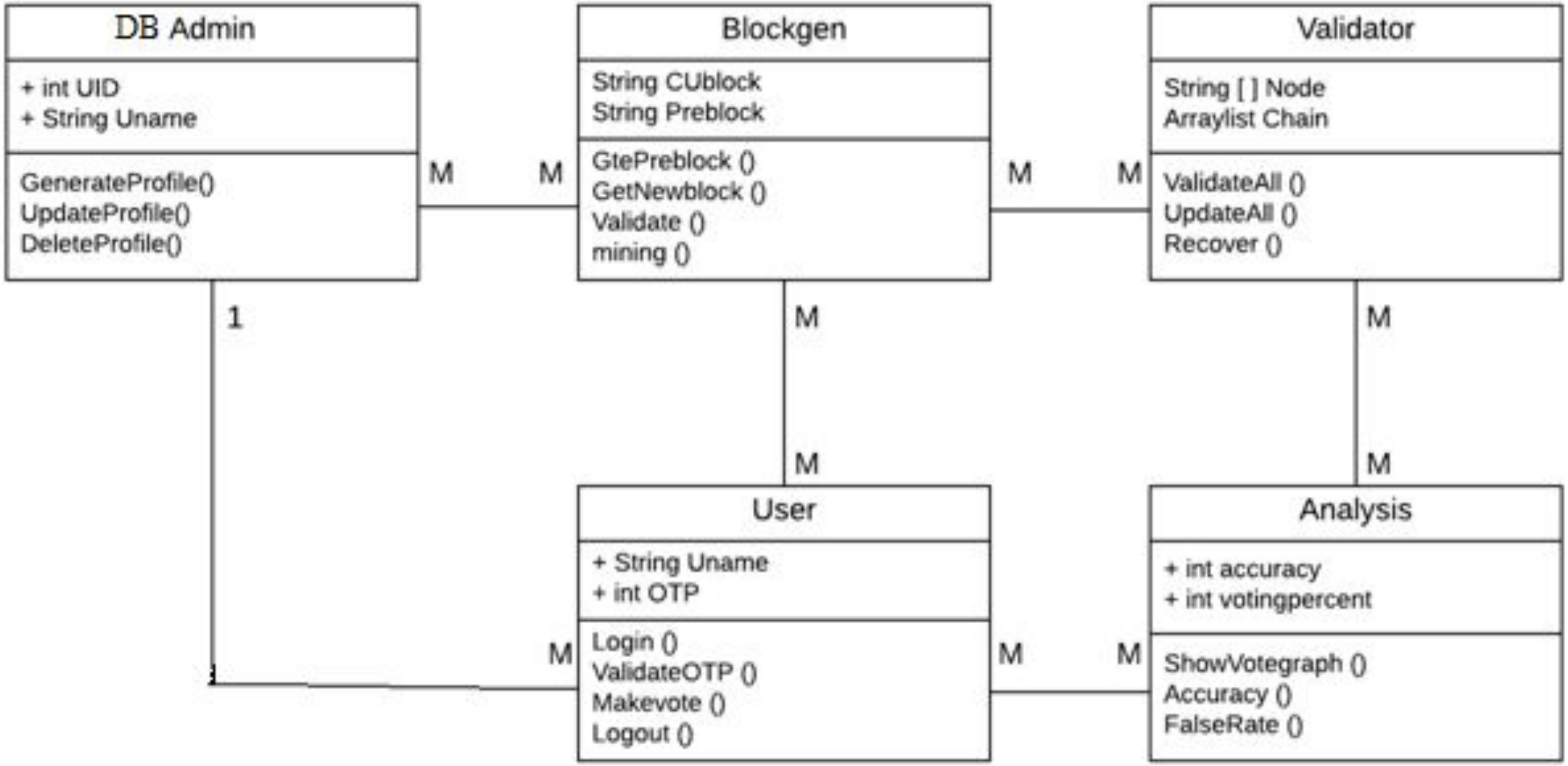
Activity Diagrams



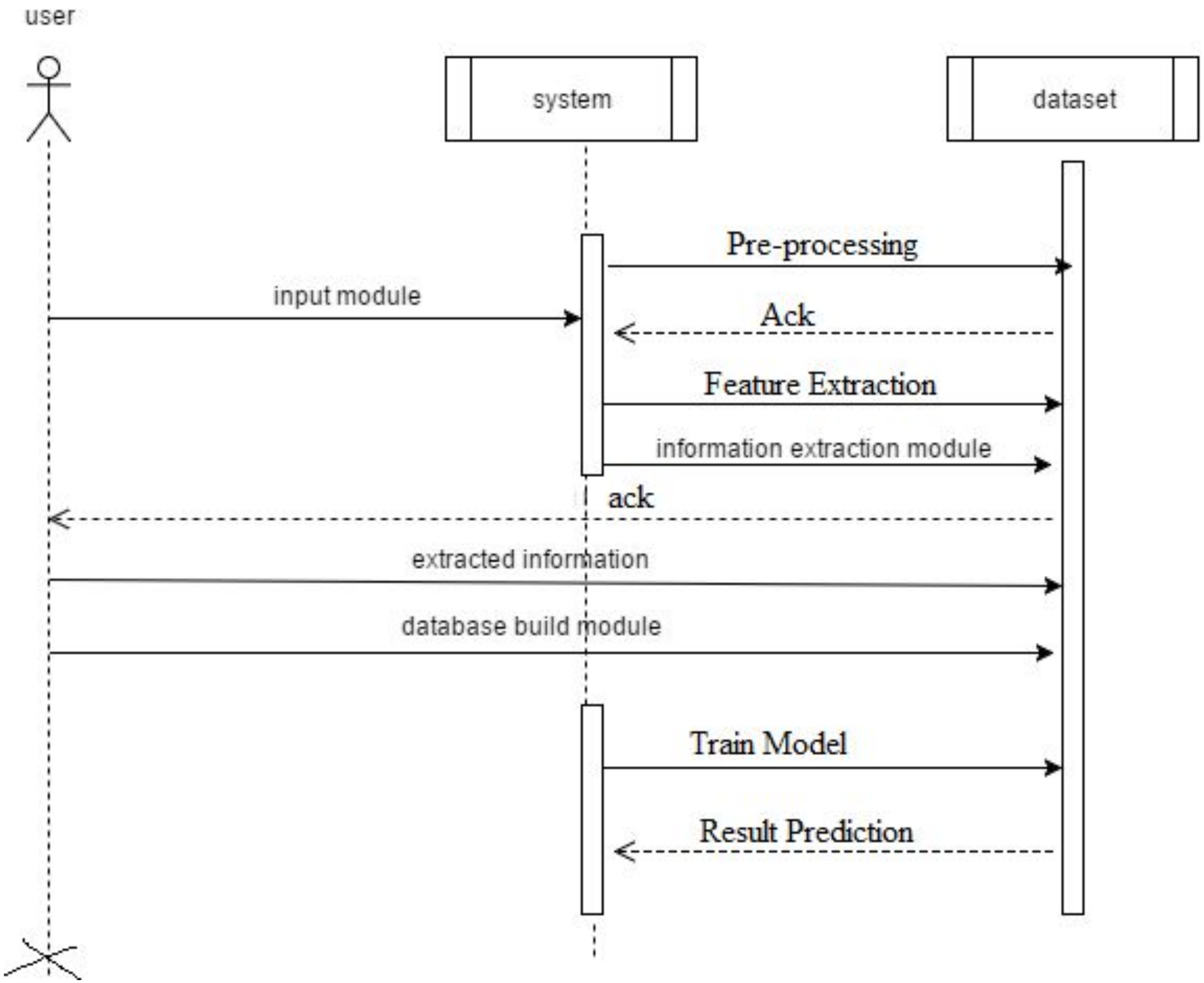
Use case Diagrams



Class Diagrams



Sequence Diagrams



System Requirements

Hardware Requirements:

- System : Intel Core i3 2.40GHz.
- Hard Disk : 256 GB (Min)
- IO Devices : Mouse, Keyboard.
- Device Type : Laptop or Computer
- Ram : 4 GB (Min).

System Requirements

Software Requirements:

- Operating system : Windows XP/7/8\9\10\11LINUX.
- Front End : .jsp (.html, .css, .js)
- Back End : MySQL 5.5 if required
- Tool/IDE : Eclipse Oxygen
- Server : Web Server (Tomcat 8.5)
- Development Kit : jdk 64 bit

Conclusion

- The proposed framework, detects the spam parameters of IoT devices using machine learning models.
- The IoT dataset used for experiments, is pre-processed by using feature engineering procedure.
- By experimenting the framework with machine learning models, each IoT appliance is awarded with a spam score.
- This refines the conditions to be taken for successful working of IoT devices in a smart home.
- In future, we are planning to consider the climatic and surrounding features of IoT device to make them more secure and trustworthy.

References

- [1] K. Graves, Ceh: Official certified ethical hacker review guide: Exam 312-50. John Wiley Sons, 2007.
- [2] R. Christopher, “Port scanning techniques and the defense against them,” SANS Institute, 2001.
- [3] M. Baykara, R. Das, , and I. Karado ?gan, “Bilgi g ¨uvenli ?gisistemlerindekullanilanarac, larinincelenmesi,” in 1st International Symposium on Digital Forensics and Security (ISDFS13), 2013, pp. 231–239.
- [4] S. Staniford, J. A. Hoagland, and J. M. McAlerney, “Practical automated detection of stealthy portscans,” Journal of Computer Security, vol. 10, no. 1-2, pp. 105–136, 2002.
- S. Robertson, E. V. Siegel, M. Miller, and S. J. Stolfo, “Surveillance detection in high bandwidth environments,” in DARPA Information Survivability Conference and Exposition, 2003.Proceedings, vol. 1. IEEE, 2003, pp. 130–138.

References (Cont….)

- [6] Z.-K. Zhang, M. C. Y. Cho, C.-W.Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "Iot security: ongoing challenges and research opportunities," in 2014 IEEE 7th international conference on service-oriented computing and applications. IEEE, 2014, pp. 230–234.
- [7] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops). IEEE, 2017, pp. 618–623.
- [8] E. Bertino and N. Islam, "Botnets and internet of things security," Computer, no. 2, pp. 76–79, 2017.
- [9] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," Soft Computing, vol. 20, no. 1, pp. 343–357, 2016.

Thank you