**Detection of Anomalous Behavior of Smartphone Devices using Change Point Analysis & Machine Learning**

**OBJECTIVE:**

The primary goal of this project is to determine the anomalous behaviour whether there is anomalous behaviour or not and to know this we have used Decision tree, XGBoosting and AdaBoost Classifiers and Support Vector Classifier to classify anomalous behaviour.

**ABSTRACT:**

Security, reliability, and availability have become three fundamental characteristics that smartphones and IoT (Internet of Things) devices have to possess to provide end-users a trustworthy experience. These properties can be degraded by extraneous events or anomalous behavior provoking damage in hardware, changes in software, theft of user information, and impact of device performance in terms of speed or availability. Considering these facts, this paper focuses on anomaly detection on smartphones using their power consumption signals. These signals represent the dynamic behavior of the device due to the action of different hardware components controlled by one or many applications at the same time. This behavior can be seen as a non-stationary process due to the changes in time of its statistical properties. Considering this assumption, our methodology uses a feature extraction technique that is based on changepoint detection theory. Then, it fits three machine learning classifiers to inject diversity and maximize the detection performance. The methodology was validated on a dataset of an emulated malware running in the background of a smartphone. Our results have been compared with several power signal based approaches demonstrating that the proposed technique performs better in terms of detection accuracy.

**Keywords:** Anomalous Behaviour, Decision tree, XGBoosting and AdaBoost Classifiers and Support Vector Classifier.

**Existing Method:**

In the existing system, implementation of machine learning algorithms is bit complex to build due to the lack of information about the data visualization. Mathematical calculations are used in existing system for model building this may takes the lot of time and complexity. To overcome all this, we use machine learning packages available in the scikit-learn library.

**Disadvantages:**

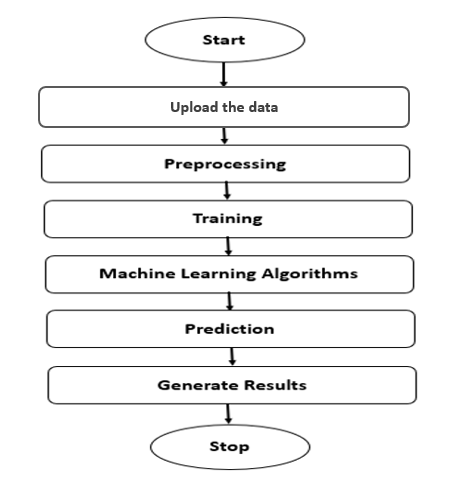
* High complexity.
* Time consuming.

**Proposed System:**

Proposed several machine learning models to classify whether there is anomalous behavior or not , but none have adequately addressed this misdiagnosis problem. Also, similar studies that have proposed models for evaluation of such performance classification mostly do not consider the heterogeneity and the size of the data Therefore, we propose a Decision tree, XGBoosting and AdaBoost Classifiers and Support Vector Classifier.

**Advantages**:

* Highest accuracy
* Reduces time complexity.
* Easy to use

**Block Diagram:**

**SOFTWARE AND HARDWARE REQUIREMENTS:**

**Hardware:**

Operating system : Windows 7 or 7+

RAM : 8 GB

Hard disc or SSD : More than 500 GB

Processor : Intel 3rd generation or high or Ryzen with 8 GB Ram

**Software:**

Software’s : Python 3.6 or high version

IDE : PyCharm.

Framework : Flask

**LEARNING OUTCOMES:**

* About Classification in machine learning.
* About pre-processing techniques.
* About ensemble algorithm.
* About flask framework.
* Knowledge on PyCharm Editor.