PROJECT REFERENCE NO : 46S_BE_5080

VISVESVARAYA TECHNOLOGICAL UNIVERSITY
BELAGAVI-590018

Project Report on

“DETECTION OF ANOMALOUS BEHAVIOUR OF SMARTPHONE DEVICES USING CHANGEPOINT ANALYSIS & MACHINE LEARNING”

For the Academic year 2022 -2023

Department of Computer Science & Engineering
KARAVALIINSTITUTE OF TECHNOLOGY
NERUMARGA, MANGALURU-574142

PROJECT GUIDE

Project Guide:

Ms. Dhanya Jayan, M.Tech

Assistant Professor

Department of Computer Science & Engineering

Email id: dhanyajayan4u@gmail.com

Contact No: 7975053965

Team:

NAME	USN	EMAIL
SHARAN S	4KM19CS057	sharanssharan9535@gmail.com
VINITHA M	4KM19CS068	vinithavinim4@gmail.com
RIDHIN P V	4KM19CS048	Ridhinridhin03@gmail.com
PUNITH M	4KM19CS044	Punith80800@gmail.com

KEYWORDS

1. AdaBoost Classifier
2. Decision Tree Classifier
3. XGBoosting Classifier
4. Support Vector Classifier
5. Confusion Matrix

INTRODUCTION

In recent years, the Internet of Things (IoT) market is witnessing an explosion in the number of devices connected and to be connected. It is expected that by 2020 the number of devices will reach ~50 billion. A significant percentage of these devices are smartphones. According to Statista in 2019, there are approximately 2.7 billion smartphone users around the world. A common characteristic of IoT devices and smartphones is the continuous necessity for Internet access through wireless communication systems to transmit sensitive and private information of users. For this reason, these devices have been of interest to cybercriminals who have developed applications with malicious code to steal passwords, emails, contacts, photos, recordings, health insights, or another valuable user information. Furthermore, other cybercriminals have focused their efforts to degrade and harm the performance of the infrastructure of cellular, private, and public networks converting IoT devices into botnets to provoke denial of service of these networks. To counter such malicious activities, researchers, companies, and even governments have been developing different methodologies. Most of these approaches are based on analyzing the static characteristics of the applications' source code. A disadvantage of this strategy is that these methods are susceptible to obfuscation and modification of the code to avoid being detected. Thus, other researchers have been developing methodologies in which they analyze the dynamic characteristics of the device such as network traffic, power consumption, Central Processing Unit (CPU) activity, and temperature while applications are running. This analysis can be done in real time (on-line) or offline (analysis of measurements obtained beforehand). Other researchers have used hybrid techniques which are combinations of static and dynamic characteristics to do more effective recognition.

The present work proposes a novel methodology to decide if a smartphone is running a malicious application using the power consumption of the device. The hypothesis is that the power consumed by a device contains encoded and useful information that can be used to identify the presence of malwares. That is due to the fact that when a malware is installed in a device, it must perform some activities that depicts the combination of the energy consumed for each of the hardware component of the device such as CPU, network components, screen, Global Positioning System (GPS), accelerometers, or other components. This methodology uses offline processing technique and off-device measurement in which an external device is used to collect the power consumption to improve the resolution of the power traces assuming that important features can be embedded in very short periods of time. Furthermore, we use the theory of changepoint detection to extract features of a non-stationary time series signal. The features extracted by this theory have been used as the input to a classifier to define a binary classification problem applying different machine learning techniques.

OBJECTIVES

Develop a system to detect anomalous behaviour in smartphone devices using a combination of changepoint analysis and machine learning techniques.

The objectives of detecting anomalous behaviour in smartphone devices using changepoint analysis are multi-fold and encompass various aspects related to performance, security, and user experience. The following objectives highlight the key areas of focus:

1. Performance Optimization: One objective is to identify unusual patterns in smartphone device metrics, such as CPU usage, memory consumption, battery usage, and network activity. By detecting significant changes and shifts in these metrics, the goal is to identify performance bottlenecks, resource-intensive processes, or abnormal resource utilization. This information can then be utilized to optimize the device's performance, enhance responsiveness, and improve overall efficiency.

2. Fault Diagnosis and Troubleshooting: Another objective is to detect anomalous behavior that may indicate device malfunctions, software bugs, or compatibility issues. By analyzing time series data and identifying changepoints, it becomes possible to pinpoint the occurrence of unusual events or patterns that may lead to system instabilities or crashes. Early detection of such anomalies enables prompt fault diagnosis and efficient troubleshooting, thereby reducing downtime and minimizing the impact on the user.

3. Security Breach Detection: Detecting anomalous behavior can play a vital role in enhancing smartphone device security. By monitoring various metrics and analyzing changepoints, it becomes possible to identify suspicious activities, unauthorized access attempts, or abnormal network behavior that may indicate security breaches or malware infections. Timely detection of such anomalies enables the implementation of security measures, such as notifying the user, initiating remediation actions, or blocking malicious activities, thus safeguarding the user's data and privacy.

4. User Experience Enhancement: An important objective is to improve the overall user experience by proactively addressing abnormal behaviour in smartphone devices. By detecting and analysing

changepoints, it becomes possible to identify patterns that may cause user dissatisfaction, such as sudden performance degradation, excessive battery drain, or connectivity issues. By taking timely actions based on the detected anomalies, such as generating alerts, offering recommendations, or optimizing device settings, the objective is to ensure a smooth and satisfactory user experience.

5. Proactive Maintenance and Predictive Analytics: Detecting anomalous behavior using changepoint analysis facilitates proactive device maintenance and predictive analytics. By continuously monitoring and analyzing device metrics, patterns, and anomalies, it becomes possible to predict potential issues, anticipate failures, and schedule preventive maintenance tasks. This proactive approach helps in minimizing device downtime, reducing maintenance costs, and maximizing the lifespan of the smartphone.

In summary, the objectives of detecting anomalous behaviour of smartphone devices using changepoint analysis encompass performance optimization, fault diagnosis, security breach detection, user experience enhancement, and proactive maintenance. By leveraging the power of machine learning and statistical analysis, these objectives aim to ensure optimal device performance, enhance security, and provide a seamless user experience.

METHODOLOGY

Modules

1.1 User

1.1.1 View Home page:

Here user view the home page of the anomalous behaviour web application.

1.2 View Upload page:

In the about page, users can learn more about the anomalous behaviour prediction.

1.3 Input Model:

The user must provide input values for the certain fields in order to get results.

1.4 View Results:

User view's the generated results from the model.

1.5 View score: Here user have ability to view the score in % .

System

2.1 Working on dataset:

System checks for data whether it is available or not and load the data in csv files.

2.2 Pre-processing:

Data must be pre-processed in line with the models. By doing so, the model's accuracy and data information are improved.

2.3 Training the data:

After pre-processing the data will split into two parts as train & test data before training with the given algorithm.

2.4 Model building:

To create a model that predicts the personality with better accuracy this module will help us.

2.5 Generated score:

Here user view the score in %.

Algorithms	**Accuracy**
Decision Tree Classifier	90.29%
Support Vector Classifier	83.24%
XGBoost Classifier	90.02%
AdaBoost Classifier	84.3%

2.6 Generated result:

We train the machine learning algorithm and predict the anomalous behaviour.

Workflow

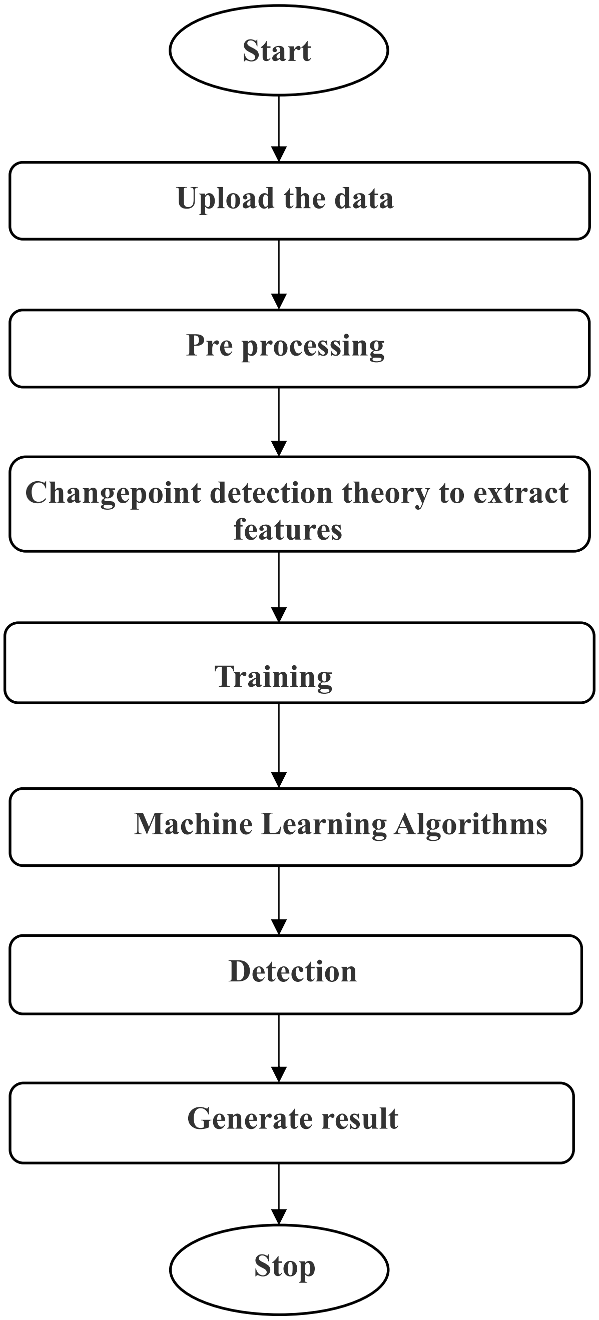
Start
Upload the data
Pre processing
Changepoint detection theory to extract features
Training
Machine Learning Algorithms
Detection
Generate result
Stop

Fig 3.1 : Block Diagram

RESULT & CONCLUSION

In this paper, we proposed a new methodology to identify when smartphone applications behave anomalously. The work considers the use of a changepoint detection theory to extract features and three machine learning techniques to train a classifier from the power consumed by the smartphone. We can conclude that the proposed methodology performs better in terms of F1-measure accuracy comparing it with three other methodologies. We got a best score of 92.28 % accuracy through Decision Tree Classifier comparing it with three other methodologies. In confusion matrix we got the True Positives is 1189, True Negative is 2577, False Positive is 84 & False Negative is 79. We can emphasize that our methodology can recognize malware acting in short periods of time which it was a disadvantage of the other methodologies.

FUTURE SCOPE

The future scope for the project of detecting anomalous behaviour of smartphone devices using changepoint analysis:

1. Edge Computing and Real-time Detection: The future scope involves leveraging edge computing capabilities to perform real-time anomaly detection directly on the smartphone devices. By deploying lightweight machine learning models or rule-based systems on the device itself, it would be possible to detect anomalies in real-time without relying heavily on cloud-based processing. This approach can enable immediate feedback, faster response times, and enhanced privacy by keeping sensitive data locally.

2. Multi-modal Anomaly Detection: Smartphone devices capture data from various sensors such as accelerometers, gyroscopes, cameras, and microphones. Future research can focus on developing multi-modal anomaly detection techniques that integrate information from different sensor modalities. This can provide a more comprehensive understanding of the device behaviour and enable the detection of complex anomalies that involve multiple data sources.

3. Self-learning and Adaptive Systems: Developing self-learning systems that can adapt and evolve based on changing device usage patterns and user preferences is an exciting future direction. By continuously analysing and learning from historical data, these systems can refine their anomaly detection algorithms and improve their accuracy over time. This adaptive capability can help in handling evolving threats, adapting to user behaviour changes, and reducing false positives.

4. Anomaly Interpretability and Explain ability: Providing explanations and interpretable insights about detected anomalies is an important future scope. By employing techniques such as feature importance analysis, visualizations, or rule extraction methods, it becomes possible to explain why a certain behaviour is flagged as anomalous. This would assist in understanding the underlying causes, aiding in troubleshooting, and building user trust in the anomaly detection system.

5. Integration with IoT and Smart Home Environments: As smartphones increasingly serve as central hubs for Internet of Things (IoT) devices and smart home environments, extending the anomaly detection scope to include these interconnected systems presents an opportunity. By analyzing data from various devices and sensors within the IoT ecosystem, it becomes possible to detect anomalies that span across multiple devices, enabling holistic monitoring and management.

6. Predictive Maintenance and Predictive Analytics: Expanding the project's scope to include predictive maintenance and predictive analytics can be beneficial. By leveraging historical data and analyzing patterns, it becomes possible to predict potential anomalies, system failures, or performance issues before they occur. This proactive approach can lead to more effective maintenance scheduling, reduced downtime, and improved device reliability.

7. Collaborative Anomaly Detection: Collaboration between multiple smartphone devices can enhance the anomaly detection process. By sharing aggregated and anonymized device data, it becomes possible to identify global anomalies, detect coordinated attacks, or identify widespread software bugs affecting multiple devices. Collaborative anomaly detection can provide a collective defense mechanism and enhance the overall security posture.

In summary, the future scope for the project of detecting anomalous behaviour of smartphone devices using changepoint analysis encompasses areas such as edge computing, real-time detection, multi-modal detection, self-learning systems, interpretability, integration with IoT, and predictive analytics. Exploring these directions can further improve the accuracy, efficiency, and usability of anomaly detection systems for smartphone devices.

REFERENCES

[1] D. Evans, “The internet of things: How the next evolution of the internet is changing everything,” CISCO white paper, Tech. Rep.

[2] Statista, “Number of mobile phone users worldwide at 2020 (in billions).” [Online]. Available: https://www.statista.com/statistics/274774/forecast-ofmobile-phone-users-worldwide

[3] A. Arabo and B. Pranggono, “Mobile malware and smart device security: Trends, challenges and solutions,” in 19th International Conference on Control Systems and Computer Science, pp. 526–531.

[4] T. Kim, B. Kang, M. Rho, and et. all, “A multimodal deep learning method for android malware detection using various features,” IEEE Trans. on Info. Forensics and Security, vol. 14, no. 3, 2019.

[5] Y.-S. Yen and H.-M. Sun, “An android mutation malware detection based on deep learning using visualization of importance from codes,” Microelectronics Reliability, vol. 93, pp. 109–114, 2019.

[6] D. Arp, M. Spreitzenbarth, M. Hubner, H. Gascon, K. Rieck, and C. Siemens, “Drebin: Effective and explainable detection of android malware in your pocket.” in Ndss, vol., pp. 23–26.

[7] P. Faruki, A. Bharmal, V. Laxmi, and et. all, “Android security: A survey of issues, malware penetration, and defenses,” IEEE Communications Surveys Tutorials, vol. 17, no. 2, pp. 998–1022, Second quarter.

[8] K. Ariyapala, H. G. Do, H. N. Anh, and et. all, “A host and network based intrusion detection for android smartphones,” in 30th Int. Conf. on Advanced Info. Net. and Apps Workshops (WAINA).