Mobile Activity Monitoring System Using Android Spy

[1]Vaishnavi Shardul, [2]Shubham Chaudhari, [3]Aniket Ozarkar, [4]Ankita Pendharkar, [5] Prof. Dr. N.R. Wankhede

Department of Computer Engineering
Late G.N. Sapkal College of Engineering
Anjineri, Nashik.

***Abstract*-. Android mobiles are everywhere in the world these days, but if we con- sider a field like the IT industry, Organization, education, business in these sectors are done by all employees with their Android mobile phones many activities. Each company, organization has its own policies, rules, future projects, so in such cases, an employee of the organization must maintain privacy, security and confidentiality. So it is very important monitor their mobile phones to see if they are leaking confidential data or if they are making bad calls, bad SMS, or crossing out the geographical area of the organization during working hours. Another thing is so many criminal cases it happens like child abduction, so to avoid all this, we have to track the location of the child's mobile. After considering all these factors, we implemented the "Mobile Activity Monitoring System Using Android Spy" This system is im- plemented to monitor the daily activity of users with their android mobiles. The information like missed call, incoming call, outgoing call, call duration, incoming SMS, outgoing SMS along with its date and time will be tracked and updated on the server this server will be monitored by the administra- tor. This information may be maintained for organizational security purposes such as leakage of confidential data and maintaining the organization's poli- cies. Another thing that this system consists of is a location alert if any of the users cross the specified geographical area the organization will be im- mediately sent a notification to the manager's mobile phone in the form of an e-mail. This is very useful system administrators to track any user in the organization using their personal information and where they exist via GPS. By tracking such information, an organization can improve its performance at work.**

***Key Words*: Android, GPS, SMS, Tracking**

Published in IJIRMPS (E-ISSN: 2349-7300), Volume 11, Issue 3, May-June 2023

INTRODUCTION

The system "Mobile Activity Monitoring System Using Android Spy" is im- plemented in Android as a Front-End and My SQL in the backend. Today there are mobile phones with Android everywhere especially in the orga- nization area the maximum user has android mobiles. Users have higher performance activity with their mobile phones in the organization during working hours, so the system is implemented to monitor over users, what activity they perform working hours in the organization. There will be in- formation track such as incoming and outgoing calls (with date, time, source and destination mobile number, call duration and type) information about incoming and outgoing SMS (with date, time, source and destination mo- bile number, duration and type of call). tracked and sent to the server and a notification will be sent administrator's mobile device as soon as activity occurs performed by the user through his android Mobile Phones. Tracking will be done in the background services running on the user's Android mobile device, apk file will be installed at the time of user registration. All necessary information about the user, such as the User id, username, user label, user department, user the mobile number will be managed by the administrator. The administrator has access to the user's location at any time point and if any user exceeds the specified geographic location organization area or re- stricted organization area a notification will be sent to the administrator's mobile phone done by

picking up latitude and longitude by a spy working in the user's mobile device. This system plays an important role for income notification of breaches of the organization's security through GPS on their mobile phones with employee details. An administrator can easily detect a security breach and leaking confidential data from one organization to an- other organization. This system brings awareness during working hours and increases work efficiency and provides high industry logical security level. This system is useful not only for the organization but also useful for track- ing the victim with their location, tracking students doing activity on their android mobile phones in the classroom, watching children performing un- necessary activity of parents on mobile phones and they can also get location alerts from their kid's government authorities to prevent data leakage.

LITURATURE SURVEY

• "A secure tracking mobile app development", Bharath Sai Pochampally; Jiangbo Liu In this paper, The explosive growth of the Android platform has been a significant win for consumers with respect to competition and features. To provide users with the security applications to manage the data in their personal smart phones is very important. In this paper we describe an Android app development that the user can use to keep in touch with the lost phone if the user has misplaced the mobile or forgot the mobile somewhere and wanted to know the call history, SMS, GPS locations etc. The security solution provided by this app requires the user to install the application with security codes for call logs, SMS and GPS tracking. User has to send an SMS with these secret codes to the mobile in order to retrieve the call logs, messages, GPS locations to the mobile from which the SMS was sent. User can also manage personal information such as delete the call logs or messages. If the SIM card has been changed, the user will receive a notification with that information to the alternate number. With this app, users can also manage the personal information remotely and securely. The process and coding created in this research can be used as the platform for other secured Android mobile app development. • "Enabling Trust and Privacy-Preserving e-KYC System Us- ing Block chain" Somchart Fugkeaw; The electronic know your customer is a system for the banking or iden- tity provider to establish a customer identity data verification process between relying parties. Due to the efficient resource consumption and the high degree of accessibility and availability of cloud computing, most banks implement their e-KYC system on the cloud. Essentially, the security and privacy of e-KYC related documents stored in the cloud becomes the crucial issue. Existing e-KYC platforms generally rely on strong authentication and apply traditional encryption to sup- port their security and privacy requirement. In this model, the KYC system owner encrypts the file with their host's key and uploads it to the cloud. This method induces encryption dependency and communi- cation and key management overheads. • "Data-in-use leakages from Android memory — Test and anal- ysis" Pasquale Stirparo; Igor Nai Fovino; Ioannis Kounelis Due to their increasing pervasiveness, smartphones and more in gen-
eral mobile devices are becoming the citizen's companions in the daily life activities. Smartphones are today the repositories of our secrets (photos, email), of our money (online e-commerce) and of our identi- ties (social networks accounts). Therefore mobile applications have the responsibility of handling such sensitive and personal information in a proper, secure way. This paper present the second phase of the Mo- biLeak project, analysing how mobile applications manage users data when these are loaded in the volatile memory of the device. Scope of this work is to raise the awareness of the research and development communities on the poor attention that is generally paid in the secure development of mobile applications. • "Mobile biometrics: Towards a comprehensive evaluation method- olog" Attaullah Buriro; Zahid Akhtar; Bruno Crispo; Sandeep Gupta in this paper described Smartphones have become the pervasive per- sonal computing platform. Recent years thus have witnessed exponen- tial growth in research and development for secure and usable authen- tication schemes for smartphones. Several explicit (e.g., PIN-based) and/or implicit (e.g., biometrics-based) authentication methods have been designed and published in the literature. In fact, some of them have been embedded in commercial mobile products as well. However, the published studies report only the brighter side of the proposed scheme(s), e.g., higher accuracy attained by the proposed mechanism. While other associated operational issues, such as computational over- head, robustness to different environmental conditions/attacks, usabil- ity, are intentionally or unintentionally ignored. More specifically, most publicly available frameworks did not discuss or explore any other eval- uation criterion, usability and environment-related measures except the accuracy under zero-effort. Thus, their baseline operations usu- ally give a false sense of progress. This paper, therefore, presents some guidelines to researchers for designing,

implementation, and evaluat- ing smartphone user authentication methods for a positive impact on future technological developments..

AIM & OBJECTIVES

- To implement the of which is to track the user's daily mobile activity and send all the status to the administrator and also log will be maintained to the centralized server where users belong to student, employee, officer, kids, and others.
- To increase the security, confidentiality and integrity of any organization with their employees.
- This system will not be misused as the one administrator will maintain all the logs of information and maintain confidentiality in it.

.

MOTIVATION

The motivation behind the implementation of Android user activity monitoring and security". Is to Retrieve call log, SMS history user location from content provider and to monitoring these above activity finally send to the android user and also log will be maintained if user in any emergency situation automatically call to programed number with location**.**

METHODOLOGY

Project Planning: Define the objectives and scope of the project. Identify the key functionalities and features of the monitoring system. Plan the overall project timeline, resource allocation, and deliverables.
Requirement Analysis: Gather the requirements for the monitoring system. Identify the specific activities, events, or behaviors that need to be tracked and monitored on the target Android device. Determine the data that needs to be collected, such as call logs, text messages, location information, app usage, etc.
Requirement Analysis: Gather the requirements for the monitoring system. Identify the specific Android Spy Application Development: Develop the Android application that will be installed on the target device to track and collect data. This application should run in the background without the user's knowledge and collect the required information. The application may use various techniques, such as hooking into system APIs, intercepting network traffic, or monitoring system events, to gather data., events, or behaviors that need to be tracked and monitored on the target Android device. Determine the data that needs to be collected, such as call logs, text messages, location information, app usage, etc.

PROBLEM STATEMENT

In existing system There are limitations on storage of call and message logs in mobile phone memory also it cannot see the records of deleted messages and cannot restore them same in case of images. If your data is corrupted then all of your messages may lost so there is need of an application that can keep records of all call logs, messages at storage another than phone. Another one is tracking of location can be done of user by using Bluetooth functions i.e. the location will be tracked within a specified range and alert will be send to the administrator's mobile device through Bluetooth.

SCOPE OF PROJECT

In this approach, requirements for "Mobile Activity Monitoring System Using Android Spy" is described. As per described in previous section for parameter we use Android programming because it is very easy to install app on android operating systems device on the other hand it provides several permission like internet permission, GPS permission, SMS permission, reading contact permission and several others therefore we used Android programming to add functions and flow to our system. Implement the "Mobile Activity Monitoring System Using Android Spy".

SYSTEM ARCHITECTURE

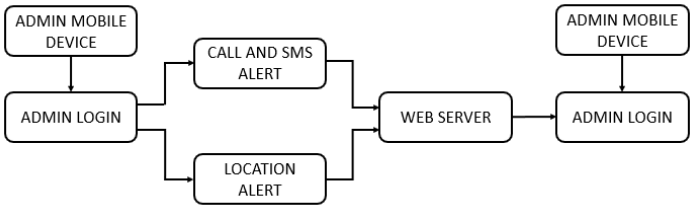
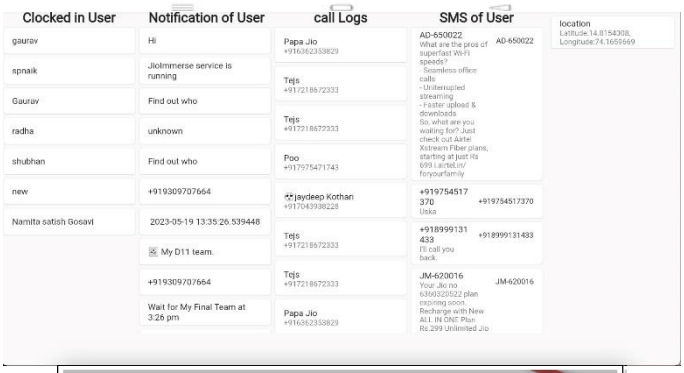


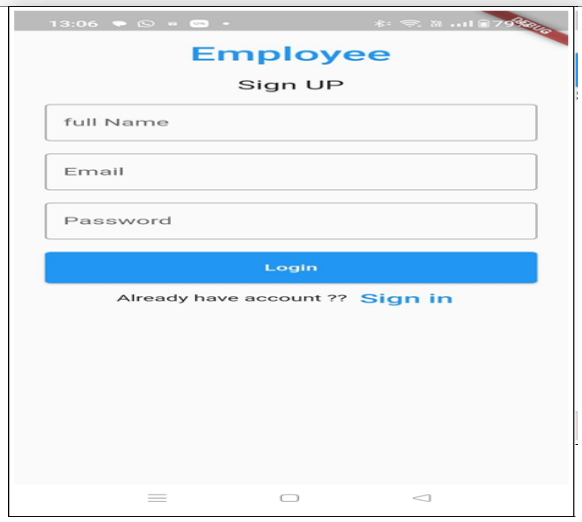
Fig -1: System Architecture Diagram

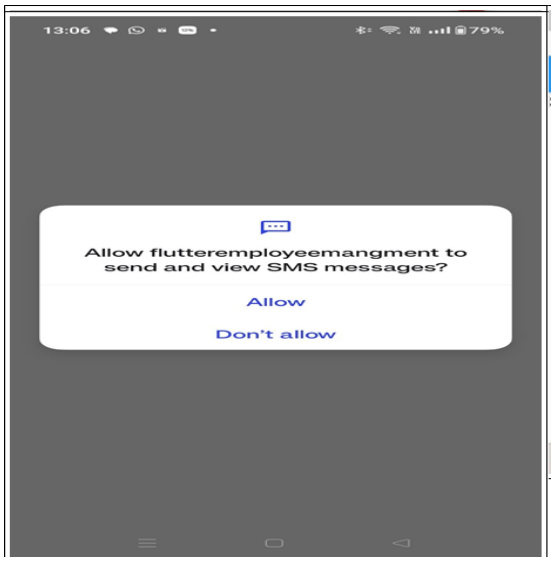
APPLICATION:

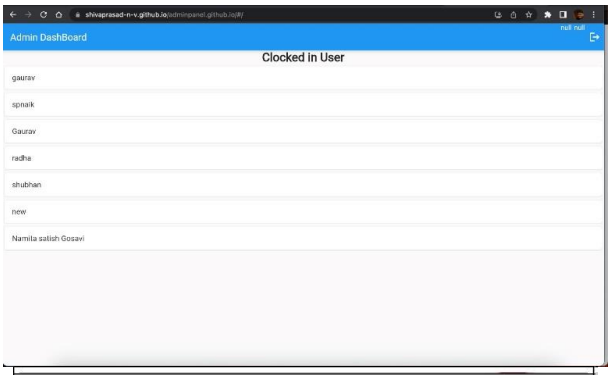
- Industry
- Security
- Public sector
- Government sector

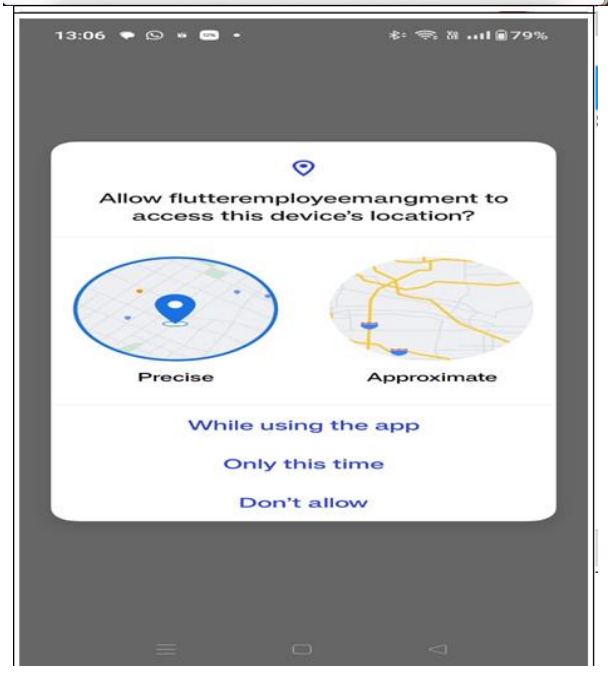
RESULT











CONCLUSION

In this system, the user activity monitor using spyware and their penetrations techniques are completely analyzed. The antimalware is categorized on the idea of detection strategies they use. an in-depth performance analysis of those antimalware Growth share techniques is additionally provided and therefore the edges and limitations of those antimalware is deduced comprehensively. At the end, a thought of hybrid antimalware is bestowed which can address the constraints of existing static and dynamic approaches. In future, it's aimed to implement the projected hybrid answer which can be a generic antimalware which will give higher security

for humanoid devices by foremost statically analyzing the humanoid applications on native device so it'll perform dynamic analysis on a foreign antimalware server

REFERENCES:

1. Abhishek Barve & Pragnesh shah ," Android based Remote Monitoring System", International Journal of Computer Applications, 2012.
2. Nitin P. Jagtap, Kanchan A. Patil, Shaziya Sayyed Shakil and Nitin S. Ingle, "Mobile Activity Monitoring System Using Android Spy", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 2, pp.158-162, 2015.
3. Adrian Dabrowski, Georg Merzdovnik, Nikolaus Kommenda and Edgar Weippl, "Browser History Stealing with Captive Wi-Fi Portals" , IEEE security and privacy workshops, 2016.
4. Available in, "Android Version History" , 17 August 2018 https://en.wikipedia.org/wiki/Android_version_history.
5. Jamil Khan and Sara Shahzad, "Android Architecture and Related Security Risks", Asian Journal of Technology & Management Research, Vol. 05 , Issue: 02, pp.14-18, 2015.
6. Xianhua Shu , Zhenjun Du and Rong Chen, "Research on Mobile Location Service Design Basedon Android ", IEEE, 2009. [14] Kiran Bala, Sumit Sharma ,and Gurpreet Kaur, " A Study on Smartphone based Operating System", International Journal of Computer Applications , Vol. 121 – No.1, pp.17-22, 2015.
7. Kusum Dalal, Prachi Chaudhary, and Dr. Pawan Dahiya, "Performance Evaluation of TCP and UDP Protocols in VANET Scenarios using NCTUns-6.0 Simulation Tool", International Journal of Computer Applications, Volume 36– No.6, 2011.
8. Andrew S. Tanenbaum and David J. Wetherall, "COMPUTER NETWORKS", Pearson Education, 2011.
9. Alaa O. Shama, "TCP/IP Protocol Suite (Internet Model)", The Islamic University of Gaza, 2017.
10. Ram Sundar G, "A Comparative Study of Mobile Operating Systems" , International Journal of Recent Trends in Engineering & Research (IJRTER), Vol. 02, Issue 02,pp. 57-61, 2016.