PHONEMITHRA

Rohith Raju[1]
Dept. of CSE
Mangalam College of Engineering,
Kerala, India.
reachrohit01@gmail.com

Linsa Mariam Binu[2]
Dept. of CSE
Mangalam College of Engineering,
Kerala, India.
linsabinu88@gmail.com

Nayana Anna Joshy[3]
Dept. of CSE
Mangalam College of Engineering,
Kerala, India
nayanaannajoshy@gmail.com

Maneesh Mathew K J[4]
Dept.of CSE
Mangalam College of Engineering,
Kerala, India
maneeshkj80@gmail.com

Nayana N Panicker[5]
Dept of CSE
Mangalam College of Engineering,
Kerala, India.
nayana.panicker@mangalam.in

Abstract-- **Mobile phones have become a very important aspect of human life. From making cellular calls to money transactions. Nowadays, people mostly use smart phones, which work very efficiently in the sense of network connectivity such as 4G, 5G, Bluetooth connectivity, WIFI, etc. Around 70% of people use Android-supported systems. Whereas Android is vulnerable to attacks, viruses, and other malicious contents compared to other OS's such as Apple's iOS, smartphones are vulnerable nowadays, as "security is a myth" in networks. Security is thus essential for Android systems. The proposed system is an SMS-based remote mobile recovery system. The system proposes an Android-based application that allows the client to retrieve contacts, locate the system that is misplaced, change the sound profile of the system, or lock the system if it is misplaced. This could be done using another cell phone, which does not require an internet connection.**

Keywords—SMS,recovery,smartphone,retrieval

I. INTRODUCTION

Nowadays, smartphones play an important role in one's life, as they control the most important aspects of a human being's life. It has multiple access points to one's daily life categories, such as personal life and banking aspects. So there are many important contents for a person stored in it, such as his or her banking credentials, valuable documents, etc. So it is very important to protect these users information. The proposed system is an SMS-based recovery system. That is, the system is an application for Android users. Most people use Android, as it has a much simpler interface and is also affordable also. But when it's compared with other OSes such as Apple's iOS, the security features of Android are pretty weak and breakable. And recovery features when an Android phone is lost are also not that good.

Consider that when someone misplaces his or her Android smart phone, we could send a specific message from any phone and easily recover the mobile phone's geographic location. Also, if someone forgot to take his or her phone with him or her, they could easily retrieve contacts. Likewise, they could also change the sound from silent to general and lock the system. This system allows the user to access his or her phone using another cell if the application has been installed on the user's Android device. This app doesn't require internet access for retrieving the smartphone. As it requires only a text message from a cell phone to the user's phone. The reply would include further details regarding the same. So it's an Android smartphone protection and recovery application which doesn't require internet connection once it's been installed on a system.

II. LITERATURE SURVEY

Ajay Joy, Ankitha K , Amritha P.A and Tintu Devasia[1] proposed a system which uses Firebase Cloud Messaging(FCM) technology and Global Positioning System(GPS) for the connection between the user's mobile phone and the other cellular device which is used to recover it. This system which uses Firebase Cloud Messaging (FCM) technology and Global Positioning System (GPS) for the connection between the user's mobile phone and the other cellular device which is used to recover it. The suggested device communicates between the client mobile phone and the external mobile phone using Firebase Cloud Messaging (FCM) and GPS technology. The application sends a SIM card alert message to the recovery mobile number when the SIM card is replaced. The user details are registered with a password, secret pin, and recovery mobile number. While the utility is receiving an SMS with the password and command call, the user can view the actions that can be taken. The program is made to

address a number of issues, including forgetting or losing a device, tracking its present location, and locking the device if someone else has it without authorization. The password is sent with a command from the user.

G. Divya Jyothi, and K. Navya[2] proposed an application to track a phone in silent mode and convert it to vibration and general mode is called "Phone Mode Conversion" in the paper. The mobile device's receiving side is where the application must be installed; once installed, it runs in the background until it is removed. To authenticate the message and switch from silent mode to general and vibrate mode, a predetermined code must be sent from another mobile device. The mobile device's mode will immediately switch from silent mode to general mode if the code is matched. Any type of computing that utilizes computer or online networks, as well as numerous communications channels, is considered mobile computing.

Oystein Sigholt, Besmir Tola, and Yuming Jiang[3] proposed a system. That is when the cellular networks go down, Wireless Direct is a potential technology that can be used to restore connectivity between consumer devices. Authentication, secrecy, and integrity of communications are all guaranteed by the proposed technique's mix of security layers. At registration, a central authentication entity issues certificates to each device. If the server component cannot be reached, the device will try to join a group over WIFI Direct with other nearby devices experiencing the same issue. A mobile social application using various mobile devices is implemented to validate the methodology. In-range wireless communication between devices is made possible by the radio interfaces found in modern smartphones. The proposed system consists of three components: the Authentication Component, the Server Component, and the Certificate Signing Request (CSR). The Authentication Component is the single mutually Trusted Third Party (TTP) with the sole responsibility of managing the identities of the users. The Certificate Signing Request (CSR) contains the public key and the identity (or Distinguished Name (DN) that the certificate is for. The Certificate Revocation List (CRL) can be maintained to revoke credentials after the fact. The server component is responsible for message forwarding to connected clients both over the Internet and during out-of-coverage operation.

Vishal Tambe, Dinesh Chauhan, Sudarshan Kulal and Snehal Sherkhane [4] proposes an offline Android application that can carry out various operations on distant mobile devices to help locate lost or stolen mobile devices. In order to be recognised, the user must enter a verification code and contact name. The software then operates in the background while it waits for incoming messages. In terms of topics, trustees, consistency, and correctness, this debate is valuable. Mobile security, offline security, and SMS gateways are the main topics of this project. The system operates in the background while it verifies. The app is triggered when a message is received in order to examine it and determine whether it was intended for the app. If so, the app will check the code and compare the requested name to the contact list.

Lappanitchayakul, Kreadtisak[5] conducted a survey and By using the ICMP Protocol (Ping), the created network monitoring system identified and informed the irregularity of equipment in the network of Rajamangala University of Technology Phra Nakhon. On a website, it showed the connection state of network equipment as well as a record of appliance connection. The system administrator received email and SMS warnings when the irregularity was discovered, letting him know where the problematic device was so he could rectify it. The system also made it possible for the system administrator to make a preventive plan by looking up the appliance's connection history in the system. The institution is having a difficulty with the main centre's lack of staff, which is causing an extended time of inspection.

NalinipriyaG.,Isravel, J., and Lokesh Kumar[6]discussed how the number of people using mobile phones is unexpectedly increasing while phone theft is on the rise.. Mobile devices save a variety of sensitive personal information about a person, such as images, demographic information about their schooling, government-related documents, and more. Therefore, losing smart phones results in an unrecoverable loss that might not be cheap. In this edition, the researcher tries to provide a solution to the problem of rehabilitating an unattended or stolen phone. The researcher supports a system that would remotely request authorization to access a cell phone from every other smartphone using an SMS. The remote device is able to determine the location of user device. The faraway device can trace the vicinity of the misplaced cell device. The person wants to register in order to have access to the area around the strange device. The user must send a key phrase as a message from the missing tool after registering while the tool is missing in order to activate the programme. As a result, the utility will send a message to the registered number containing the location of the stolen tool. Application parses each message as soon as it is received by the user in order to look for the keyword in the message. The location finding services are summoned as soon as the key phrase is located. The device may be located by using GPS.
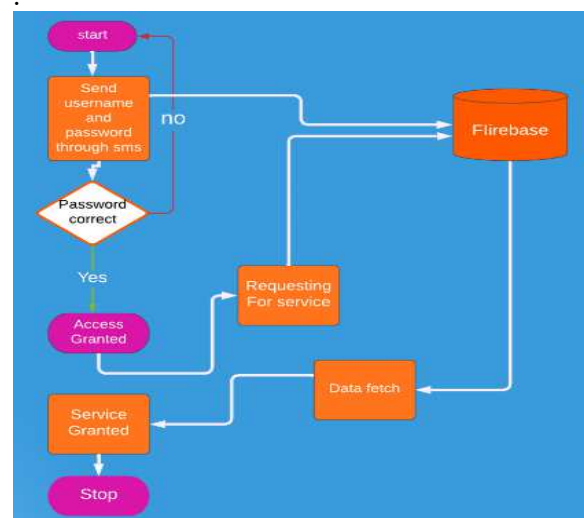
.

Fig.1 System Architecture

III. PROPOSED SYSTEM

The Fig 1 indicates the system Architecture of the proposed system. The connection between the user and the external mobile is done using the SMS. Once the installation of the application is done in the user's smartphone, then it could be accessed using the passcode and the certain message could be used to retrieve or to perform certain functions such as Access Contact, change sound profile, Access Location or to lock the Screen of the smartphone. And to work it out in this system, Global Positioning System are used. The user's information is required, along with a secret pin and a mobile phone recovery number. The individual could be able to operate the mobile device from another mobile device through SMS to this utility. Many of these actions are conducted by the system without an online connection because they are all done by SMS message. The device also has an additional layer of security in that it will automatically send the new SIM card number to the recovery mobile number.

This system features an Android application that runs offline. The user may be prompted to enter the user id which is the email id and the password which, the user assigned during the time of registration in the application.

The email and password are used to complete the registration. The given application has the ability to send a SIM card alert message to the recovery cell phone number on a regular basis when the SIM card is being swapped. By sending messages to the new cellphone number, the user will still be able to control his mobile device. Once the password has been properly configured, the user can view the moves that the utility can do while it waits for an SMS with the password and the command call for the appropriate movement to be completed. The utility may be hidden after the application has been closed so that no unauthorized user gains access to the smartphone.
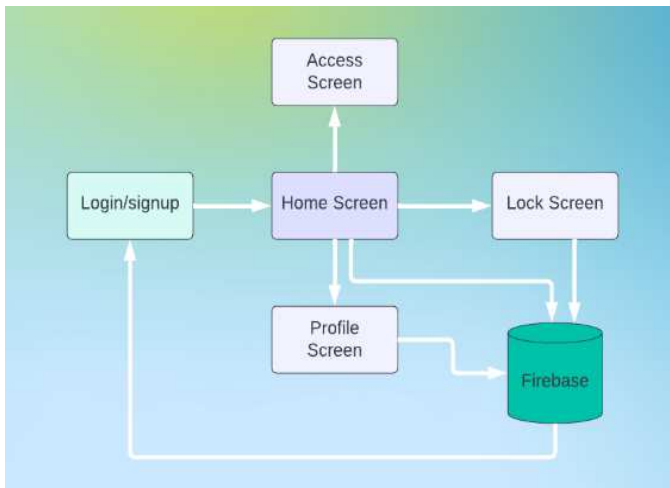

Fig.2. Application Architecture

The Fig.2 indicates the Application Architecture. That is the application consists of a user interface screens which are home interface and also a registration interface and there will be separate interfaces for each function modules.

Upon receiving the message, the user's mobile device checks the password. If it matches the password that the user has set,

the command is processed. The appropriate step is carried out. The information that the user requested is retrieved and given to the user after the procedure is completed in the user's mobile device. When the user's request is complete, they send the SUCCESS command, which halts the execution of any ensuing commands and kills the application. The app will always be travelling through history. As a result, the software can test every message sent or received on that phone since the utility was installed, and it will start by looking for the password.

The various functions performed through this Android Application are:

- If someone leaves their device at home and needs a contact number, they can remotely receive one from their cell phone.

- Locate the smartphone if it is lost or misplaced.

- Change sound profile from silent to general.

- Lock Screen of the Smart phone also.

A Success command is sent back if the requested functionality is fulfilled. Or if the working or execution of the functionality is done successfully then a success command is returned from the user's device as text message.
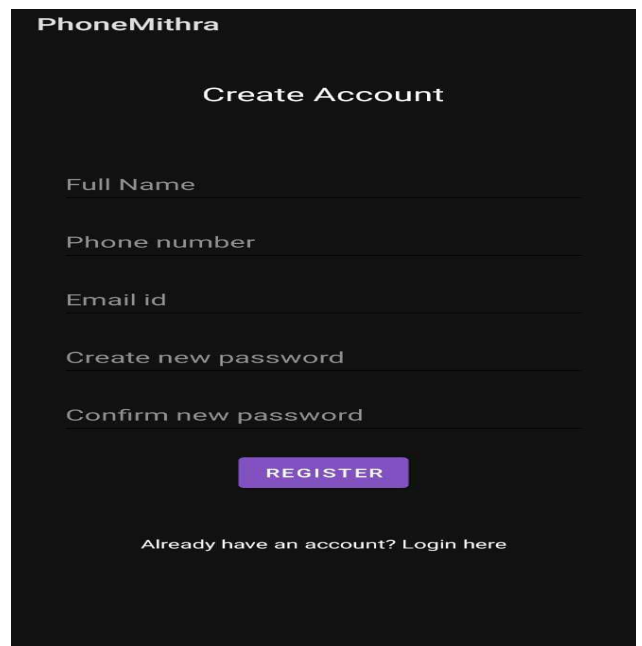

Fig.3 Registration Interface

Figure 3. shows the registration interface where the user should fill up the details and register himself for the application to start executing.
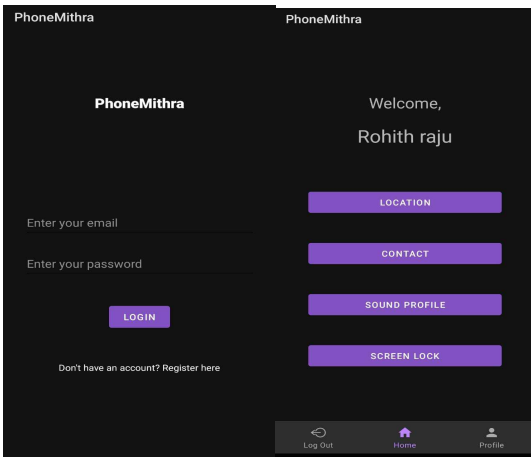
Fig. 4.   Fig.5.

Figure 4 shows the login interface where the user could login using the registered credentials.

Figure 5 shows the different functionality modules of the application.

IV. RESULT

A. Access Contact

The user could easily access the contact of a person using an external device by just sending the text message to the desired smartphone in the format as shown below in figure6.
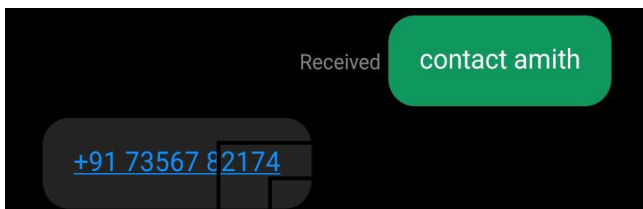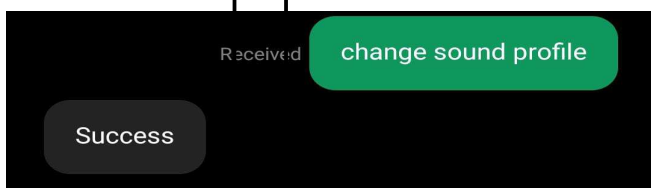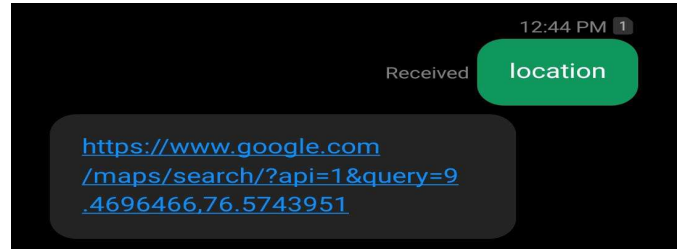

Fig . 6

Fig .7

B. Change Sound Profile

The sound profile could be changed as shown in the above figure7.

C. Access Location

The location could be accessed in the form of google location coordinates as it the most flexible location tracing application. Like shown in figure8.

D. Lock Screen

By using the corresponding operations stated above, the user could easily add the screen lock also when the text message is received.

V. CONCLUSION

As our co-dependency on mobile devices increase, the more we need to be concerned for its safety. The app will be beneficial in accessing restricted information from an end-user's phone without compromising on its safety and will also be able to reconfigure its security settings. It will also be able to inform a user of the exact location of the target phone without having the need to be in a place with internet connectivity. That is the SMS based recovery system is flexible as the application is of less storage size and this app will help in accessing restricted information from a user's phone without endangering its security and will be able to change the security settings on the device. A user won't need to be in an area with internet connectivity in order for it to tell them the precise location of the target phone.

References

[1] Ajay Joy, Ankitha K , Amritha P.A and Tintu Devasia "SMS based remote mobile phone data access system." 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT) | 978-1-6654-1005-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICICICT54557.2022.9917880

[2] G. Divya Jyothi and K. Navya. "Phone mode conversion". in 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA): volume 2. 2017, pages 193–195 doi: 10.1109/ICECA.2017.8212793.

[3] Oystein Sigholt, Besmir Tola and Yuming Jiang. "Keeping Con nected When the Mobile Social Network Goes Offline". in 2019 International Conference on Wireless and Mobile Computing, Net working and Communications (WiMob): 2019, pages 59–64. doi: 10.1109/WiMOB.2019.8923549

[4] Vishal Tambe andothers. "Offline Mobile Security". in 2018 Interna tional Conference on Smart City and Emerging Technology (ICSCET): 2018, pages 1–4. doi: 10.1109/ICSCET.2018.8537303

[5]] Kreadtisak Lappanitchayakul. "Development of Email and SMS Based Notification System to Detect Abnormal Network Conditions: A Case Study of Faculty of Business Administration, Rajamangala University of Technology Phra Nakhon, Thailand". in 2018 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS): volume 3. 2018, pages 98–105. doi: 10.1109/ICIIBMS.2018.8549920.

[6] G. Nalinipriya, J. Isravel and N. Lokesh Kumar. "A dynamic tracking system for smart phones - A secure approach". in2019 International Conference on Smart Structures and Systems (ICSSS): 2019, pages 1–4. doi: 10.1109/ICSSS.2019.888286

Special Issue - 2023

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
ICCIDT - 2023 Conference Proceedings