Quick Sec- Android Application For Security Informant

K.Navaneethakrishnan[1], P.Nisha[2], P.Palanikumar[3], R.Karthiyayini[4]
[1, 2, 3]Dept of Computer applications
[4]Assistant Professor, Dept of Computer applications
[1, 2, 3, 4] University College of Engineering (BIT Campus), Trichy, India

Abstract*- In a recent modern world among the existence of plenty of technologies, android applications are a rapidly growing segment of the global market because etoday's human routine life is influenced by smart cellular phone. Android applications are evolving at a meteor pace to give users a rich and fast user experience. In The paper, Android security platform for the android application development, layered approach and the details of security information for Android is discussed and suspicious applications is also discussed. As such, graphical passwords have been introduced as an alternative to the traditional authentication process. The dynamic password schemes provide a way of making more user friendly passwords, also increasing the level of security. In general, session passwords are those that can be used only once and for every new session on, new password is generated. The generated one time password is valid for only a short user defined period of time. The SMS based mechanism is implemented as both a backup mechanism for retrieving the password and as a possible mean of synchronization.*

Keywords- Android app,Dynamic password, SMS (Short Messaging Service), Security.

I. INTRODUCTION

The log-in of any application today requires user to enter the username and passwords in textual format. We have experienced situations where the textual passwords are easily cracked and hackers can breaks in to the system's vital information section. As a result, private data becomes accessible and modification of these data causes great harm and financial losses to business. Authentication scheme of this application provides one additional level of protection in the form of comparing the passwords. This provides enhanced security to a machine and makes it difficult for the attacker to gain access to system's resources. This application provides to generate the dynamic passwords. Whenever client have trying to sign in get the new password via the application. New password also send it to the corresponding Mail address for the client.

1.1. ANDROID

Android Operating System Android is a Linux-based operating system. Designed primarily for touch screen mobile devices such as smart phones and tablet computers. Initially developed by Android, Inc., which Google backed financially and later bought in 2005. Android was unveiled in 2007 along with the founding of the Open Handset Alliance: a consortium of hardware, software, and telecommunication companies devoted to advancing open standards for mobile devices[10].The first Android-powered phone was sold in October 2008.

Android is open source and Google releases the code under the Apache License. This open-source code and permissive licensing allows the software to be freely modified and distributed by device manufacturers, wireless carriers and enthusiast developers. Android has a large community of developers writing application ("apps") that programming language. In October 2012, there were approximately 700,000 apps available for Android, and the estimated number of application downloaded from Google Play, Android primary app store, was 25 billion. These factors have contributed towards making Android the world's most widely used Smartphone platform, overtaking Symbian in the fourth quarter of 2010, and the software of choice for technology companies with require a low-cost, customizable, lightweight operating system for high tech devices without developing one for scratch.

As a result, despite being primarily designed for phones and tablets, it has seen additional applications on televisions games consoles, digital camera sand other electronics. Android's open nature has further encouraged a large community of developers and enthusiasts to use the open source code as a foundation for community-driven projects, which add new features for advanced user or bring Android to devices which were officially released running other operating system. Android had a worldwide Smartphone market share of 75% during the third quarter of 2012, with 750 million devices activated in total and 1.5 million activations per day.

The operating system's success has made it a target for patent litigation as part of the so-called "Smartphone wars" between technology companies. As per may 2013, a total of 900 million Android devices have been activated and 48 billion apps have been installed from the Google Play Store. The currently leading platforms on the market are Android, IPhone, Symbian, BlackBerry, Windows Mobile and Palm Web. But Android OS is now days mostly use as compare to other OS. Android is user friendly OS and easy to access. If any user wants to create application base on android then process is easy as compare to other OS. Patented for application is also low cost as compare to other OS.

II. LITERATURE SURVEY

Thepaper [1]seeks to better understand smartphone application security by studying 1,100 popular free Android applications. We introduce the compilation, which recovers Android application source code directly from its installation image. Our analysis uncovered pervasive use/misuse of personal phone identifiers, and deep penetration of advertising and analytics networks.

The paper [2], Android brings the developers and users a wide range of convenience but simultaneously it increases the security issues. The major threat of Android users is Malware infection via Android Application Market which is targeting some loopholes in the architecture mainly on the end-users part. The paper presents the current state of Android security mechanisms and their limitations also identify certain security requirements.

The paper [3], the information of women position provided by the device can be viewed on Google maps using Internet or specialized software. The IT companies are looking for-ward to the security problem and requires a system that will efficiently evaluate the problem of women security working in night shifts, traveling alone. We focuses on the proposed model that can be used to deal with the problem of security issue of women using GPS and GSM based tracking system.

The paper [4], the information of women position provided by the device can be viewed on Google maps using Internet or specialized software. The IT companies are looking for-ward to the security problem and requires a system that will efficiently evaluate the problem of women security working in night shifts, traveling alone. We focuses on the proposed model that can be used to deal with the problem of security issue of women using GPS and GSM based tracking system. It focuses on the proposed model that can be used to deal with the problem of security issue of women using GPS and GSM based tracking system.

The paper [6], A highly severe menace to any computing device is the impersonation of an authenticate user. The most frequent computer authentication scheme is to use alphanumerical usernames and passwords. But the textual passwords are prone to dictionary attacks, eves dropping, shoulder surfing and social engineering. As such, graphical passwords have been introduced as an alternative to the traditional authentication process. Though the graphical password schemes provide a way of making more user friendly passwords, while increasing the level of security, they are vulnerable to shoulder surfing. To address this problem, text can be used in combination with the colors and images to generate the session passwords, thereby making a stronger authentication means. In general, session passwords are those that can be used only once and for every new session, a new password is engendered.

The paper [8], The Existing system of android like plenty of security based system. Distributed home automation system, consists of server, sensors. Server controls and monitors the various sensors, and can be easily configured to handle more hardware interface module (sensors).smart phone based vehicle alarm system .those security based system should communicate along with smart phone.

III. PROPOSED SYSTEM

To ensure the user data is not abused by the unauthorized users and all request for access must be approved by the account holder. Access control has two components authentication and authorization Authentication ensures that a valid user is logged-in, based on an ID and password provided by the user.

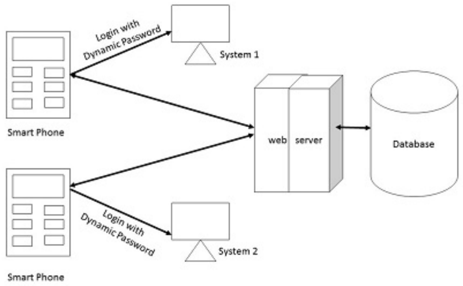
To avoid the inconvenient and security issues. In The paper will gives us the solution for maintaining logs and monitoring actions of the person.

As a part of a solution to the above identified pitfalls in the android security model, we propose a reputation based security trust model to evaluate and validate the application prior to installation. We have also analyzed the consequences of a malicious application that has managed to get installed with the full consent of the end user to ensure the end-user Data security.

This application will provides the client can know about complete setup and procedure for the security access. Sign in category also have biometric (Finger print) based security System and also face detection security System also have the details about the previous session sign in history. Each time Client has dynamic passwords and its gives high security for the event. Organization will know about the customer prospections and what it happening around. Each session get the requesting from client to the server. Server can provide the Dynamic password bases on time priority, and its consequent actions.

After getting the password sign in the required computer system then its corresponding IP address will send over the Server. And Server will monitoring the details what is it happening and surfing to store the back end Database.

IV. ARCHITECTURE



V. REQUIREMENTS

Java:

It is a general-purpose computer programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere",Without java couldn't develop android application.

Android Studio:

Android Studio is the official Integrated Development Environment (IDE) for Android app development, based on Intelligence. On top of Intelligence powerful code editor and developer tools, Android Studio offers even more features that enhance your productivity when building Android apps, such as

- A flexible Griddle-based build system
- A fast and feature-rich emulator
- A unified environment where you can develop for all Android devices
- Instant Run to push changes to your running app without building a new APK
- Code templates and GitHub integration to help you build common app features and import sample code
- Extensive testing tools and frameworks
- Lint tools to catch performance, usability, version compatibility, and other problems
- C++ and NDK support
- Built-in support for Google Cloud Platform, making it easy to integrate Google Cloud Messaging and App Engine

Database/SQLite:

SQLite is an open source Database which is embedded into Android. SQLite supports standard relation database features like SQL syntax, transaction and prepared statement. In addition it requires only little memory at runtime (approx.250 Kbyte). SQLite supports the data types TEXT, INTEGER, REAL. All other types must be converted into o0ne of these fields before saving them in the database. SQLite itself does not validate if the types written to the columns are actually of the defined type, e.g. you can write integer into string column vice versa

Android's Components

Android composed of basic four components. ICC is used for communication between components.

Activity: Activity provides GUI for interaction of user with the application. Depends upon design, an application may consists of one or more activities

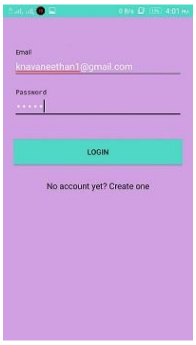
Service: Service is a background process that fetches data from the network.

Broadcast Receiver: Broadcast receiver receive broadcast announcements and response to them according to the situation.

Content Provider: Content provider is a SQLite database, which supports the sharing and accessing of data among applications.

VI. RESULTS& DISCUSSIONS

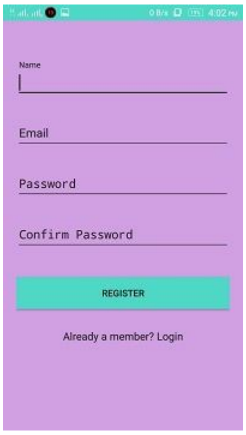
Log in module will have user name and passwords. Enter the email id and password.

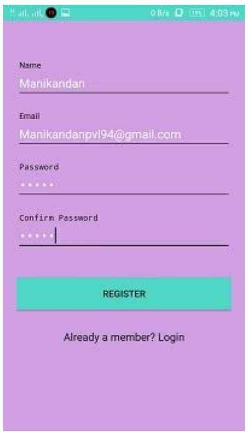


Email
knavaneethan1@gmail.com
Password
•••••

Client/User doesn’t have account to register the new account. Clients gives his details like Name, Email, Password, and Phone Number.

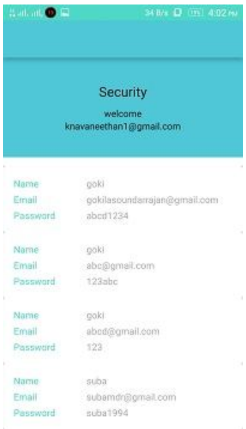
Required Field have validating condition applied on the events.





Name
Manikandan
Email
Manikandanpvl94@gmail.com
Password
•••••
Confirm Password
•••••

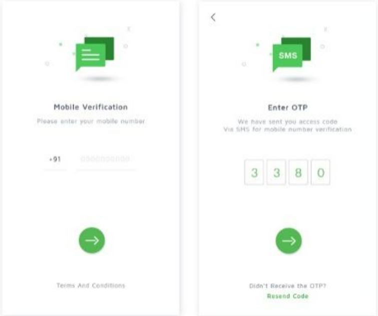
Details about who are the actors to involve the action which defined us to persons are monitor by the server and maintaining its logs.



Security
welcome
knavaneethan1@gmail.com

Name	goki
Email	gokilasoundarrajan@gmail.com
Password	abcd1234
Name	goki
Email	abc@gmail.com
Password	123abc
Name	goki
Email	abcd@gmail.com
Password	123
Name	suba
Email	subamdr@gmail.com
Password	suba1994

Dynamic One Time Password has been generated for every session, and sign in process for the application can be proceeded.



Mobile Verification
Please enter your mobile number
+91

Enter OTP
We have sent you access code
Via SMS for mobile number verification
3 3 8 0

VII. CONCLUSION

Authentication is critical for security of computer systems. Without the knowledge of the identity of a principal requesting an operation, it is difficult to decide whether the operation should be allowed. Traditional authentication methods are not suitable for use in computer networks where attacker monitor network traffic to intercept passwords. The use of strong authentication method that do not disclose password is imperative. This authentication system is well suited for authentication of user in such environments. Access control is concerned with limiting the activity of legitimate users. Access control assumes that the authentication of the user has been successfully verified prior to enforcement of access control via a reference monitor as correctly establishing the identity of the user is the responsibility of the authentication service.

REFERENCES

[1] A studyof android application security- Williamenck, Damienocteau, PatrickMcDaniel,andSwaratchaudhuri.

[2] Security in android based smartphones – mr.sumedhp.ingale,prof.sunilR.Gupta.

[3] [Android application for women security system-kavithasharma,anandh more.

[4] Android Based Intelligent mobile home automation security system - Niraj R Chauhan profpranjaliDeshmukh.

[5] Home Automation systems-Sathishpalaniappan,Naveenhariharan,naren t kesh,vidhyalakshimi

[6] Android based total security for system authentication by mithilvasaani,bhaveshpandya,charmichaniyara

[7] Android protection system Jonathan D. Stueckle, Capt, USAF.

[8] Development Techniques for Android Platform Mobile Device Application Ivan Njunjic.

[9] Application Security framework for Mobile App Development in Enterprise setup SubhamoyChakraborti, D. P. Acharjya, SugataSanyal

[10] Android Based Mobile Application Development and its SecurityT.S.Nirmala1., M.Sathya2

[11] Android Based Mobile Application Development for Web Login Authentication Using Fingerprint Recognition FeatureNilayYildirim

[12] Language-Based Security on Android-AvikChaudhuri

[13] Survey on Android Security Framework-SwapnilPowarDr.B.B.Meshram

[14] Place Reminder- An Android APPMiss. Minal S. Mahure

[15] Authenucatorfor Android application: https://en.wikipedia.org/wiki/Google_Authenticator

[16] Android Development tutorial: https://www.javatpoint.com/android-tutorial

[17] TOOLS: https://developer.android.com/studio/index.html