A PASSWORD SAVER APP WITH SECURITY AND RESTORING MEASURES

Vasanth Nayak[1], Divyashree D.K.[2], Deekshitha Rai[3], Shweta S[4], Aishwarya Kamath[5]
[1]Assistant Prof, [2,34,5]Student., Dept. of ISE,CEC Benjanapadavu, Mangalore, India,

Abstract

Password saver app has been used for storing and viewing password of wide variety of accounts. The number of smart phone users and mobile applications are growing rapidly. Though smart phones are expected to have PC-like functionality, hardware resources such as CPU's, memory and batteries are still limited. To solve this resource problem, many researchers have proposed architectures to use server resources in the cloud for mobile devices. Here we propose a conceptual architecture of Android as a Server Platform, which enables multiple user Android applications on server via network and backup and restore approach for mobile devices, which helps to reduce the effort in saving and restoring personal data Everyday data is shared, transmitted, stored for many purpose like banking, production, research and development. Hence, security is needed for storing the confidential data and Encryption can provide security. This application allows user to run this application on android platform to encrypt the file before it is transmitted over the network.

Keywords-encryption, android platform, SQLite database, data synchronization, remote server

I. INTRODUCTION

One primary, concern with password authentication is the cognitive burden of choosing secure, random passwords across all the sites that rely on password authentication. A Password Manager is one of the best ways to keep track of each unique password or passphrase that have created for various online accounts without writing them down on a piece of paper and risking that others will see them. The number of smart phones users and mobile applications are growing rapidly [1]. Though smart phones are expected to PC-like functionality, hardware resources such as CPU's, memory, and batteries are still limited. To solve this resource problem, some researchers have proposed using server resources in the cloud for smart phones. From this background, Android as a Server Platform [5] is proposed that enables many users to use resources on remote cloud servers. Backup is a crucial task, since hardware faults and software or human errors can lead to the loss of important information. As smart phones tend to be always connected to the Internet, it seems natural to move the information online and to provide backup and restore services based on the cloud computing paradigm, which is considered to be more reliable and less expensive by end users. Due to increasing use of smart phone, tablet, computer, growth of internet, information security has become the most critical problem. An unauthorized person can read and change the information while transmission occurs. Hence, protection of these sensitive data is very important. Encryption technique is used to protect the sensitive data from the unauthorized person.

Here, Advanced Encryption Standard algorithm is used to overcome above problems [2]. AES algorithm is not only security but also for great speed. It can be implemented on various platforms especially in small devices like mobile phone. It is used for all type of file encryption such as text, docx, pdf and image encryption [4]. AES algorithm is used for encryption and decryption. Apart from this the password recovery technique is also done in case if the use forgets the main password while logging in.

II.PROBLEM STATEMENT

A problem has arisen where people have many accounts and they tend to forget the password of those accounts. Every day hundreds and thousands of people interact electronically, whether it is through emails, e-commerce, etc. through internet. Sending sensitive messages over the Internet is very dangerous. If you need to send sensitive messages over the Internet, you should send it in the encrypted form.

In the current system configuration, password will be stored inside the Mobile phone in SQLite Database [3]. But, with the SQLite database there are many problems such as access to the database, security problem, memory problem, OS support problems come into picture. The need for storing Information in remote server exists because even if the mobile is lost or stolen you can get back all the passwords stored inside the phone.

III.PROPOSED SYSTEM

Here, proposed conceptual architecture of Android has a Server Platform**,** which enables multiple user Android applications on cloud server via network and backup and restore approach for mobile devices, which helps to reduce the effort in saving and restoring personal data. Encryption and Decryption allows user to easily encrypt and decrypt the passwords.

IV.SYSTEM DESIGN

The system has a client-server architecture with an Android client, and remote server. The Android app communicates with the central server through the Internet. The server handles functionality for managing and storing data in a database. The app is developed to run on Android versions 4.0 or greater as shown in fig.1. The Activity is the starting point of the app. It is a self contained process with the possibility to display a user interface to the user. To access the different part s of the app, it was decided to use a navigation drawer.

The app consists of mainly 4 features such as Add password, View password, Upload and Download as shown in

Fig.1.Through upload option user can store the passwords into the remote server. The app is designed with the ability to synchronize data to the server. The server is the system backend and is responsible for permanently storing data and providing it to the user on demand. User can fetch the data through Download option.

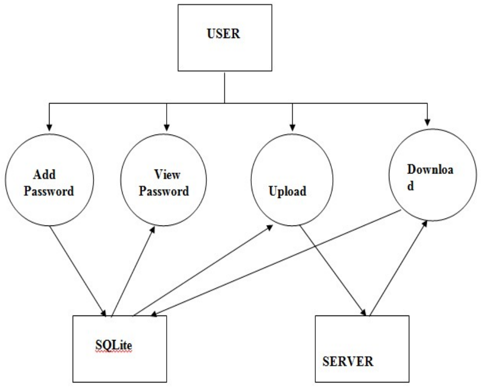


Fig.1 System Architecture

V. METHODOLOGY

A. To store data in a local database:

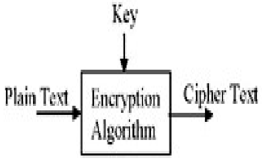
Android mobile system consists of SQLite database, which is concurrent database system. SQLite database is backend of the mobile application. That is all passwords that are entered by user are stored in this local database. Operations like insert, selection of columns, updating the data are performed on the SQLite database tables. All these operations are performed to store the passwords by category and account wise. The data and server information are stored in the SQLite database to use the stored information while retrieving the file from the server.

B. UploadPswd

The data present in the local SQLite database will be synced with the remote server in order to perform statistical operations at the server end, maintain backup of the offline data etc. in such cases offline data will be synced with remote server when user explicitly hits ‘Upload’ button when internet connectivity is available[7] and the data is uploaded into the server[1].

C. Encrypt and Decrypt

In this class, the selected data is divided into chunks. Each chunk is encrypted using AES encryption algorithm. The encrypted chunk is stored on the distributed file server. Along with this, the file and server information and number of chunks are saved on the local SQLite database table of the Android device**.**Symmetric key cryptography is generally used to encrypt the data having large sizes[2]. In symmetric cryptography, there is a single key (called secret key or private key) that is used to encrypt as well as decrypt the data. The parties that need to communicate with each other must have same secret key. Proposed system is performing in the following procedures: Fig.2.a shows the encryption and Fig.2.b shows decryption process of plaintext file. Encryption takes place at sender side. The input of encryption process is plaintext file and that of decryption process is the cipher text file. First, passwords that are stored in local database are encrypted into cypher text through AES encryption algorithm and is stored in the remote server. Whenever the user demands the data from the server, the cypher text is decrypted and stored in the local SQLite database.



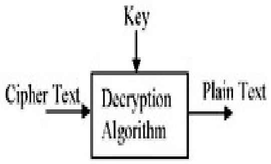


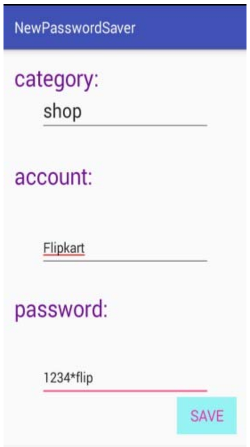
Fig.2.a Encryption of passwords **Fig.2.b Decryption of passwords**

D. *DownloadPswd:*

This activity is loaded when the user wants to download the data from the distributed file server using the information stored on the SQLite database. When the user clicks the “Download” button OTP is generated. A common technology used for the delivery of OTPs is text messaging. Because text messaging is a ubiquitous communication channel, being directly available in nearly all mobile handsets After downloading all the file chunks, the original file is constructed and stored in the SQLite database [1].

VI. EXPERIMENTAL RESULTS

Whenever the user wants to enter the new passwords, he must enter the category to which it belongs and as well as its account name as shown in Fig.3.a. Entered password can be viewed by selecting view either by Category option or by Account option as shown in Fig.3.b.



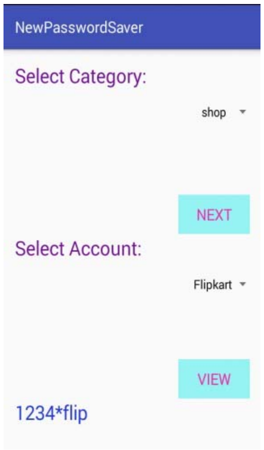
NewPasswordSaver

category:
shop

account:
Flipkart

password:
1234*flip

Fig.3.a Add Password



NewPasswordSaver

Select Category:
shop

Select Account:
Flipkart

1234*flip

Fig.3.b View Password

VII. CONCLUSION

Here we proposed Android as a server platform system that enables the use of saving, recovering and sharing personal information like password into closed groups of smart phones. We plan to develop a prototype system about proposed multitenant Android architecture. We believe that proposed architecture shows high performance on virtual image based virtualization for mobile applications. It shows successful implementation of data encryption as well as decryption. The user experiences faster file encryption and decryption. This shows that the AES encryption and decryption algorithm run faster in android phone. It gives better security of mobile from unauthorized access. This application guarantees secure end to end transfer of data without any corrupt data. In future the work may be extended by developing a stronger encryption algorithm with high speed and less memory usage.

VIII. ACKNOWLEDGMENT

We would like to express our sincere gratitude to Prof. Vasanth Nayak for his guidance and valuable support. Besides that, big thank we address to all the authors of the papers those we referred and for providing the necessary opportunities for the preparation of the paper.

REFERENCES

[1] “A Secured Mobile-Based Password Manager” by S. Agholor, A.S.Sodia, A.T.Akinwale, O.J.Adiniran Dept of Computer Science, *Dept of Mathematics, Federal University of Agriculture, Abeokuta, Nigeria,2016

[2] Suchit Tayde,“File Encryption, Decryption Using AES Algorithm in Android Phone” ,Volume 5, Issue 5, May 2015.

[3] Kiran Dhokale1, Namdeo Bange2, Shelke Pradip3, Sachin Malave,” Implementation Of Sql Server Based On Sqlite Engine On Android Platform”, Volume: 03 Issue: 04 Apr-2014 .

[4] "3 Different Data Encryption Methods," 04 June 2013.

[5] Pawade P.P and Kathalkar A.A, “ Android based server for sharing backup and restoring data”,2012.

[6] “Data synchronizatiom between mobile divices and server side databases” by Abdullahi Abubakar Imam, Shuib Basri, Rohiza Ahmad Dept of Computer Science and Information Science,2011.

[7] Sowmya Kukkadapu, “Android application for file storage and retrieval secured and distributed file servers”2010 .