IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

Mobile Self Encryption

Ms. N.S.Gurdhalkar[1], Ms. S.S.Gurdhalkar[2], Ms.P.D.Belhekar[3], Ms.J.S.Mane[4], Prof. T.R.Shinde[5]

Student, Information Technology, Pimpri Chinchwad Polytechnic, Nigdi, India[1-4]

Lecturer, Information Technology, Pimpri Chinchwad Polytechnic, Nigdi, India[5]

Abstract: Day by day, the mobile user are rapidly increased that's why, the chances of mobile losses are also increased. Apple, Sony, OnePlus5, LG, Moto z having more security like face recognition, finger print, voice recognition. But they having high cost. Because of high cost middle class people cannot afford these phones. But some mobile have low cost. Due to low cost, it doesn't provide that much security as compare to high cost mobile phones. Mobile Self Encryption allows users to store sensitive data on their mobile phones without having to worry about is confidentiality even if the mobile is lost. This Application concentrates on securing data on mobile phones by storing it an encrypted form.User is install app on their phone and it performs various operations.If user mobile device is lost it login on portal and update status with lost for deleted secrete key.

KeyWords: Cloud, Encryption, Decryption, Confidentiality

1.INTRODUCTION

In traditional approach, Most of the user thinks that their personal mobile device is secure to store the confidential information. They simply store their data without providing any security to the data. But now a day's due to the rapidly growing mobile user population, so it challenging task to maintain privacy of our mobile data in this approach. In case if mobile device has stolen or lost it's very simple to access Confidential data without efforts. That's why we use this system. This system allows users to store sensitive data and confidential information on their mobile devices without having to worry about confidentiality even if the mobile is lost. This system is developed so that employees and other mobile users can store and operate on sensitive data on their mobile phones without having to worry of it being leaked. This software project concentrates on securing data on mobile devices by storing it in encrypted form. This data is encrypted with a stream cipher whose key is stored on a server. This system enables the user to store sensitive data on their android mobile phones. System will encrypt the data and store the data online. User can access the system data by login to the system using his user ID and password than the data will be displayed to the user. Other malicious user can't access the data. Even if malicious user access online database, data will be displayed in encrypted format which is not in understandable format. By using this system user is free from worrying about leakage of his confidential data. Even if user loses his mobile phone he can access his sensitive data by login to the system using other mobile phone. Since confidential data is stored in encrypted format other malicious would not able to access the data even if he accesses the data he won't able to understand. This application is used by many people who want to keep their confidential data secretly. This application is a web application developed in android. User can access this system anywhere at any time he just has to use his user ID and password to access the system. We use java technology for the coding of our system.

2.LITERATURE SURVEY

Self-Encryption Scheme for Data Security in Mobile Devices. Yu Chen and Wei-Shinn Ku[1].2009. This paper proposes a novel data encryption and storage scheme to address this challenge. Treating the data as a binary bit stream, our self-encryption (SE) scheme generates a keystream by randomly extracting bits from the stream. The length of the keystream depends on the user's security requirements. The bit stream is encrypted and the ciphertext is stored on the mobile device, whereas the keystream is stored separately. This makes it computationally not feasible to recover the original data\stream from the ciphertext alone. Stream Ciphers and the eSTREAM Project? Vincent Rijmen[2]. 2010. In this paper, we give an overview of the eSTREAM project and we describe some lessons learnt on the design of secure stream ciphers. The design of secure stream ciphers is one of the oldest problems in cryptography. Although there exists a nicely developed theory that answers several of the important questions, the question is not fully solved (and it will probably never be). After the completion of the Advanced Encryption Standard (AES) process, block

DOI 10.17148/IJARCCE.2018.7121

ciphers were firmly in the center of the cryptographic community's attention. Some people started wondering aloud whether there was still any practical application for stream ciphers or a reason to perform research on them. The eSTREAM project to evaluate stream ciphers, organized by the ECRYPT Network of Excellence, can be seen as an answer formulated by the part of the cryptographic community that does care about stream ciphers. It turned out to be a large part of the community.

Multiple Key Sharing and Distribution Scheme with (n, t) Threshold for NEMO Group Communication[3]. Y. Jiang, C. Lin, M. Shi, and X. Shen. 2006.In this paper, a novel secure key sharing and distribution scheme for network mobility (NEMO) group communications is proposed. The scheme offers the capability of multiple key sharing and distribution for current and future application scenarios, and a threshold mechanism that effectively improves flexibility and robustness of the key sharing and distribution process. Backward and forward secrecy both are guaranteed bythe compulsive key refreshments and automatic key refreshment mechanisms, which provide dynamic in-progress group communication joining or leaving and periodic keys renewal, respectively. Security and performance analysis are presented to demonstrate that the proposed scheme meets the special security requirements for NEMO group communications and is competent for key sharing and distribution service.

3.PROPOSED SYSTEM

In traditional approach, Most of the user thinks that their personal mobile device is secure to store the confidential information. They simply store their data without providing any security to the data. But now a day’s due to the rapidly growing mobile user population, so it challenging task to maintain privacy of our mobile data it this approach. In case if mobile device has stolen or lost it’s very simple to access confidential data without efforts. In exisiting system, we simply store our data without any security and If our mobile get lost then hacker can hack our data using powerful cryptanalysis tool. Then it is very challenging to store our confidential data in our mobile phone. That’s why our proposed system is save our confidential data with strong security. In Proposed system, Like, Upload/browse file from micro SD it perform encryption algorithm for security purpose and encrypted file automatically stored on micro SD or mobile storage. We also used cloud computing to store our data. In our Application, data are encrypted using secret key and stored in mobile micro SD. When the mobile device is lost it sends a report to a server and the server then destroys the respective key. Data on that lost mobile can never be decrypted and remains confidential from unauthorized person.

4. SYSTEM ARCHITECTURE

In our application, the user of the mobile will be able to store data in the form of image, audio, video, text files, pdf. In mobile storage and memory card, simultaneously the data will be stored on database. Our database is on cloud that is 000 webhost.com.

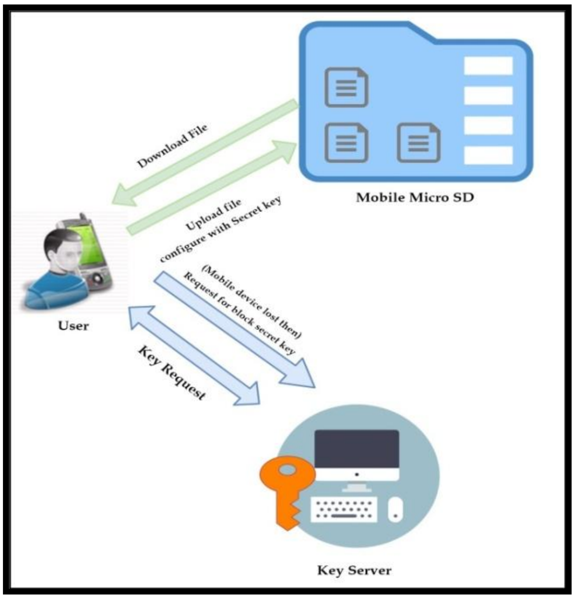

Download File
Mobile Micro SD
Upload file
configure with Secret key
User
(Mobile device lost then)
Request for block secret key
Key Request
Key Server

Fig no1: System Architecture

DOI 10.17148/IJARCCE.2018.7121

STEP 1: Firstly the user have to register on the app. After registration process, now user will be able to log in on the app with appropriate user-id and password.

STEP 2: After successfully login, user is now able to store their confidential data like images, audio, video, text files

STEP 3: The all data is stored in mobile micro SD, or Mobile storage and cloud in encrypted format. It mean unauthorized user can't access our data.

STEP 4: If in case, our mobile device is lost then we have to log in on another mobile phone and click on button "key destroyed". the key will be destroyed and data will remain in encrypted format.

STEP 5: If we want our data on another phone then log in with existing user-id and password. Press on decrypt button, it will ask one key. After providing key, the data will be retrived.

5.HARDWARE & SOFTWARE REQUIREMENTS

a. Software Requirement

1. Operating System: Windows XP/07/08
2. Programming Language: JAVA/J2EE/XML
3. IDE: Android Studio, SDK
4. Database: SQLite

b. Hardware Requirement

1. Processor - Pentium –IV
2. Speed - 1.1 Ghz
3. RAM - 256 MB (min)
4. Hard Disk - 20 GB
5. Key Board - Standard Windows Keyboard
6. Mouse - Two or Three Button Mouse
7. Monitor - SVGA.

6.SNAPSHOTS

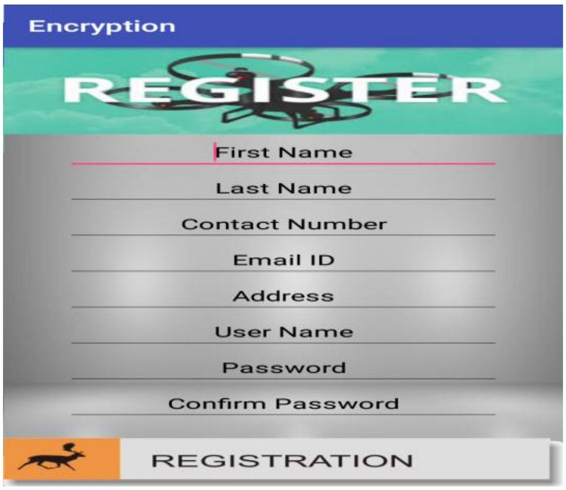


Fig no2: Registration Page

DOI 10.17148/IJARCCE.2018.7121

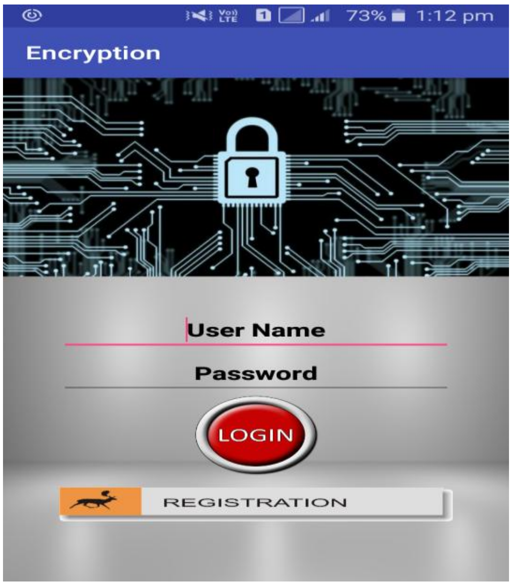
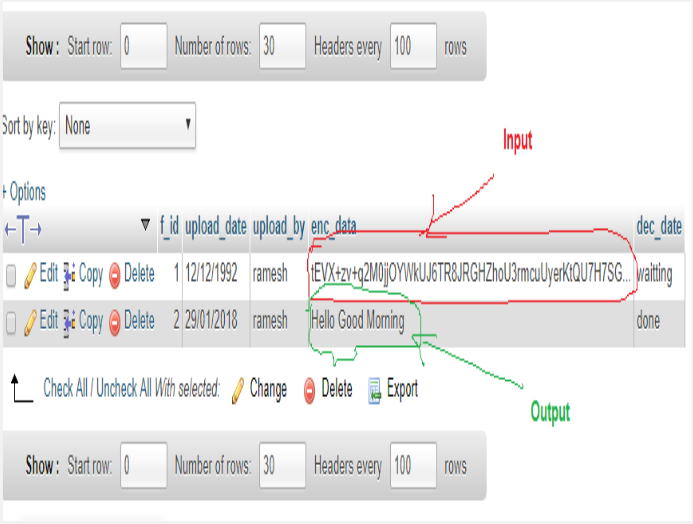


Fig no3: Login Page



Show : Start row: 0 Number of rows: 30 Headers every 100 rows

Sort by key: None

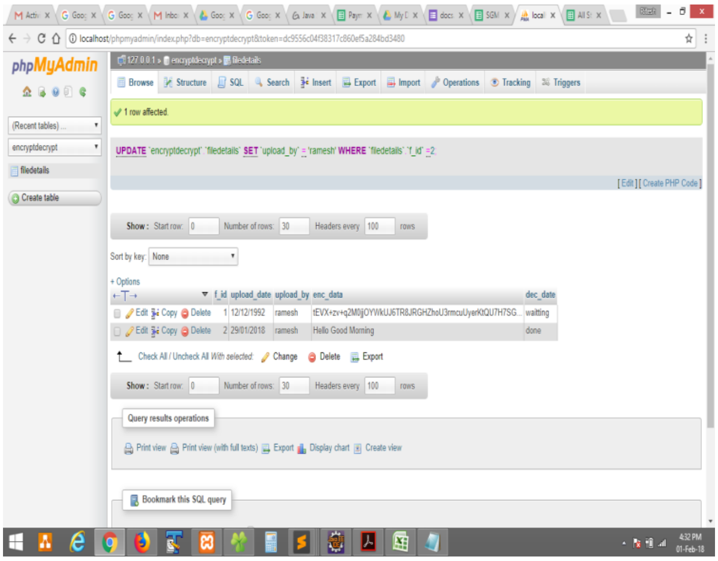
+ Options

	f_id	upload_date	upload_by	enc_data	dec_date
☐ Edit Copy Delete	1	12/12/1992	ramesh	tEVX+zv+q2M0jjOYWkUJ6TR8JRGHZhoU3rmcuUyerKtQU7H7SG...	waitting
☐ Edit Copy Delete	2	29/01/2018	ramesh	Hello Good Morning	done

Check All / Uncheck All *With selected:* Change Delete Export

Show : Start row: 0 Number of rows: 30 Headers every 100 rows

Fig no4: Database Entry



localhost/phpmyadmin/index.php?db=encryptdecrypt&token=dc9556c04f38317c860ef5a284bd3480

127.0.0.1 » encryptdecrypt » filedetails

✓ 1 row affected.

```
UPDATE `encryptdecrypt`.`filedetails` SET `upload_by` = 'ramesh' WHERE `filedetails`.`f_id` =2;
```

[Edit] [Create PHP Code]

Show : Start row: 0 Number of rows: 30 Headers every 100 rows

Sort by key: None

+ Options

	f_id	upload_date	upload_by	enc_data	dec_date
☐ Edit Copy Delete	1	12/12/1992	ramesh	tEVX+zv+q2M0jjOYWkUJ6TR8JRGHZhoU3rmcuUyerKtQU7H7SG...	waitting
☐ Edit Copy Delete	2	29/01/2018	ramesh	Hello Good Morning	done

Check All / Uncheck All *With selected:* Change Delete Export

Show : Start row: 0 Number of rows: 30 Headers every 100 rows

Query results operations

Print view Print view (with full texts) Export Display chart Create view

Bookmark this SQL query

4:32 PM
01-Feb-18

Fig no5: Registration Details

DOI 10.17148/IJARCCE.2018.7121

7.CONCLUSION

Keeping our private data is secure, it mean only the user can access the data. Encryption is used for securing files from thefts. AES algorithm is mostly used for encryption scheme. Approaches to encryption are endpoint encryption, file and folder encryption email encryption. Security is the main purpose of the project and security provided using encryption scheme.

REFERENCES

[1] Yu Chen and Wei-Shinn Ku, "Self-Encryption Scheme for Data Security in Mobile Devices". Year of publication 2009
[2] Vincent Rijmen, "Stream Ciphers and the eSTREAM Project?". Year of publication 2010.
[3] Y. Jiang, C. Lin, M. Shi, and X. Shen, "Multiple Key Sharing and Distribution Scheme with (n, t) Threshold for NEMO Group Communications". Year of publication 2006

DOI 10.17148/IJARCCE.2018.7121