ISSN: 2278-4632
Vol-10 Issue-5 No. 1 May 2020

ANDROID SECURE DIGI LOCKER

T. Anil Karuna Kumar

Associate Professor, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur, AP, India.

M. Sushma

PG Scholar, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur, AP, India.

Abstract – *Secured Digi Locker* is an advanced application in which the file storing makes it very efficient and reliable as we don't have to carry each and every document with us every time. Legal document such as Passport, Birth Certificate etc. are very important and it can be misused. Uploading it to any server is a risk-taking action as it can be hacked and keep it in our phone is also dangerous. Therefore, we have developed a system that saves the uploaded document in an encrypted form and stores it in the Internal Memory, to avoid any kind of hacking internal or external. The main advantage of this system is that it asks for Secure Pin to access the file which we enter while registering ourselves. Secure pin ensures that if our phone is in someone's hand, they won't be able to access the files. The files are secured in many ways which no intruder can access them in any case. We make uses of SQLite as it's backend to support the application.

Keywords – AES Encryption, File Security, Memory Management.

I. INTRODUCTION

Every person has some legal documents like Passport, PAN Card, Matric Certificates, Birth Certificates, Proof of identity, or any confidential documents. These files are difficult to carry every time with us. There may be chances of misplacing. To overcome this problem, Secure Digi Locker application is developed where the files can be stored in the internal memory and can be easily accessed through an application. It makes it efficient and reliable as there is no need to carry the files manually. To avoid any kind of hacking, security is provided as when we upload these files they are stored in the encrypted format and key is used by the authenticated users to decrypt the files to access. The advantage of this application is that when the registered user wants to access the files, it needs the user (secret) key i.e. password to decrypt the files. If the password entered is wrong, then the message is sent to the user. In this way the files are secured from the intruders.

The purpose is to increase the reliability and efficiently as to protect the documents from any kind of hacking. The vision of Digi Locker is to increase the growth in areas of public services which helps to protect their documents and also in ensuring security as it uses AES encryption, and documents can be automatically decrypts by giving password. The need of Secure Digi Locker is that hiding from the third person or from an opponent to secure, by storing in the internal or external memory in an encrypted format.

In the current system, there so many apps available in play store to make secure file storage. Some of the apps are related to store the legal documents only like driving license and etc. Some apps provide inaccurate results.

ISSN: 2278-4632
Vol-10 Issue-5 No. 1 May 2020

In this paper, we propose an android app called secure digi locker. In which the user can securely store the images, and files. This project provides security by using AES encryption technique. Using this app the user can securely store the file and it cannot be lost. The advantages of this application are as follows:

- Files cannot be lost.
- After entering valid secured pin the user can download the file.
- System auto decrypts the files.
- Encrypted it will stored in Phone memory

II. BACKGROUND WORK

Visual Cryptography is an encryption technique that hides information in the images such that it can be decrypted by the human vision if the correct key image is used. This technique divides a secret image into various parts called shares depending on the variation of pixels. Biometrics deals with the automated methods of verifying the identity of a person based on physiological or behavioral characteristics. This project aims to implement visual cryptography and biometric authentication to build a secure locker system. The finger print image of a user is considered as a secret image to generate shares that will be distributed among admin database and user. Authentication will take place by comparing the real time fingerprint image of the user and the image generated from the combination of the shares [1]. The primary objective of Digital Locker system is projected by, in which all documents of a personal are going to be keep in electronic format. During this projected work wet end to describe Digital Locker to a scanned picture of a persons' documents by employing a methodology of desegregation along visual cryptography and steganography through image process, the methodology to perform steganography and Visual Cryptography at identical time exploitation pictures as cowl objects for steganography and as keys for cryptography [2]. Digital locker scheme under the digital India campaign to provide a secure dedicated personal electronic space for storing the documents of resident Indian citizens. This new development seeks to create an electronic space for storing the documents which is further linked to the Aadhar number of the user and thus can be utilized for securing personal documents such as PAN card etc. of the citizens of India [3]. The storage space (maximum 10 MB) is linked to the Aadhar number of the user. The space can be utilized for storing personal documents like University certificates, PAN cards, voter id cards, etc., and the URI's of the e-documents issued by various issuer departments [4]. This software system trans forms the paper document/identities to the digital form for the better and easy access with verification and security of documents using AES (Advanced Encryption Standard) algorithm. Hence nobody can upload fake documents into this system. This software system helps the people to maintain their documents/identities for long time and citizens will always feel that they have their documents/identities in their hands. This paper explains the methodology of the securely storing and sharing the documents [5].

ISSN: 2278-4632
Vol-10 Issue-5 No. 1 May 2020

III. PROPOSED WORK

System Model

The system can be shown in the Figure 1 in which mainly has only on entity such as User.

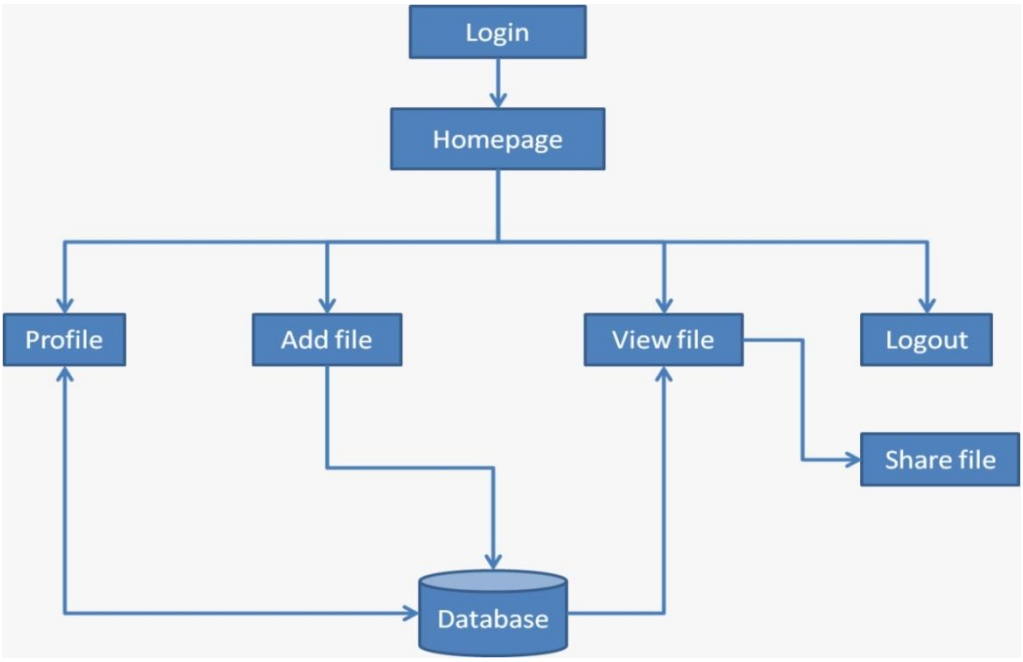

Figure. 1: System Overview

User Module

- In this module user able to upload the private file after login in the app. When upload the sensitive files he encrypt the file and store the encrypted file in the storage space and he can able to view the encrypted files.

Encryption Module

- This module helps user to encrypt sensitive file before upload to storage and this module provides the protection to file by converting file in plain text to cipher text.

Decryption Module

- In this module, the user able to view the file information by decrypting the file. For that this module performs decryption process by converting cipher text to plain text.

Share Module

- In this module, user can share the encrypted file with other. Encrypted can be decrypted using decryption algorithm.

ISSN: 2278-4632
Vol-10 Issue-5 No. 1 May 2020

To process the Secure the SMS we use AES algorithm as follows

Algorithm used: AES (Advanced Encryption Standard)

Input: 128 bits block data, plain text.

Output: 128 cipher text Procedure: AES takes 10 rounds for 128 bits block size. This algorithm has four transition rounds they are: Substitute bytes, ShiftRows, MixColumns and AddRoundKey. For 128 bits it will take 16 bytes and performs transition rounds from 0-9 and last 10th round doesn't have

MixColumns. The 16 bytes are arranged as two-dimensional array in hexa-decimal format which is called as state array. Each state array has 4 words as (w0, w1, w2, w3) which are used for rounds from 0-9. i.e. 44 words are used for 10 rounds. The next step is Substitute bytes where it uses an S-box to perform a byte-to-byte substitution of the block. Further it uses ShiftRows as a simple permutation. The output of ShiftRows is multiplied with actual plain input box this round is called MixColumns method. In AddRoundKey a simple bitwise XOR of the current block with a portion of the expanded key. The 1st round output is taken as 2nd round input and repeats the process until 10th round. The output of 10th round after AddRoundKey without MixColumns is the desired 128 bits Cipher Text.

IV. RESULTS AND DISCUSSION

In this system we developed mobile based Secure Digi Locker to improve the user experience and Security. The following screens show that our system is more users friendly and efficient.

This is the interface which appears when open the application, after successfully install it into the mobile shown as Loading page in below Fig-2.

Figure. 2: Loading Page

ISSN: 2278-4632
Vol-10 Issue-5 No. 1 May 2020

Fig-3: The application having the user login page as figured in the below screen.

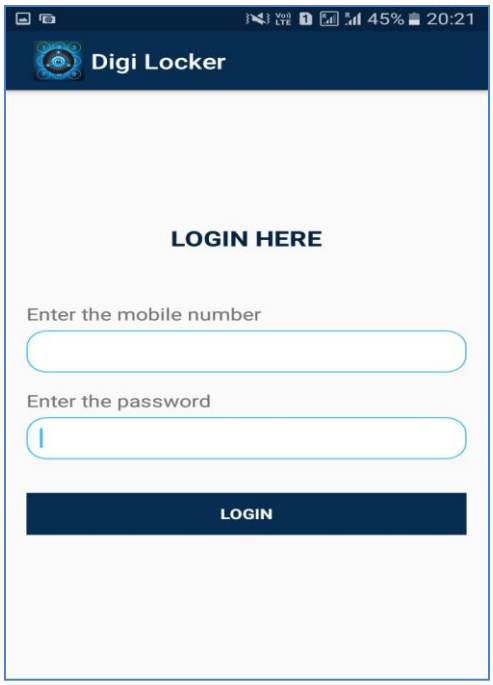

Figure. 3: Login Page

Fig-4Showing the menu page of this application having some options.

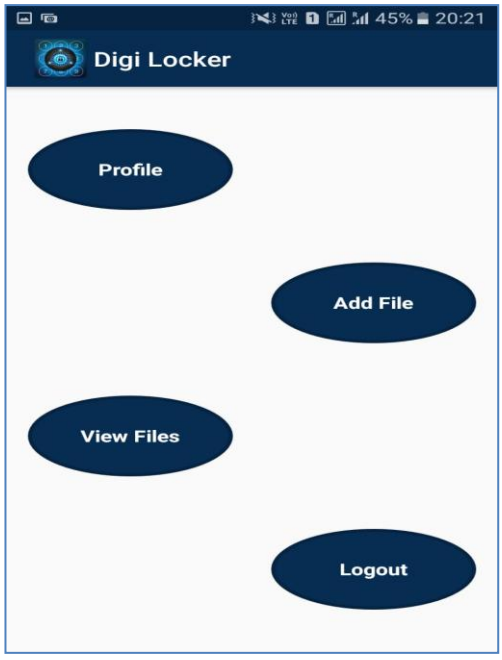

Figure. 4: Menu Page

Fig-5Showing the uploaded files.These files are uploaded in an encrypted form into the application.

ISSN: 2278-4632
Vol-10 Issue-5 No. 1 May 2020

Figure. 5: Uploaded Files

Set a secure pin to each file when uploading them and use the secure pin to decrypt and download the files as in Fig-6.

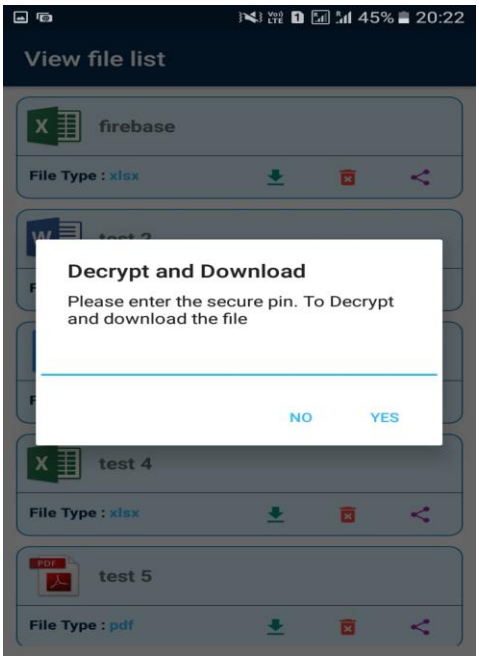

Figure. 6: Decrypt and Download

Fig-7: Share or delete the uploaded files which are in an encryption form.

ISSN: 2278-4632
Vol-10 Issue-5 No. 1 May 2020

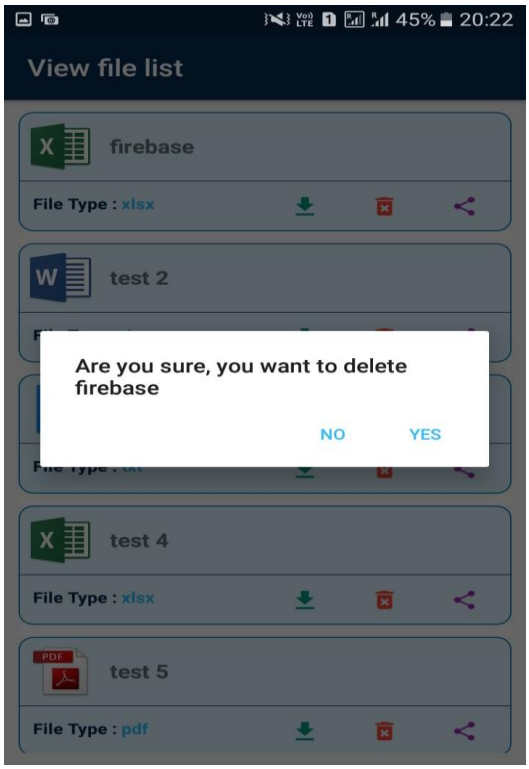

Figure. 7: Delete File

V. CONCLUSION

We proposed an application Secure Digi locker. A user has many documents or files which are difficult to carry manually. So, to overcome this problem, an application is proposed where a user uploads some necessary files. These files are secured as they are encrypted by using AES Encryption technique and stores in internal memory or external memory. If the files are to be accessed then password is given as a secured pin to decrypt those files and thus can be viewed. As we use AES encryption technique it is difficult to get hacked and if the password entered wrong then message is sent to user for verification. AES encryption uses 128 bits key which is secured. There may be chance of losing if files are corrupted in mobile. To overcome this, the future scope may be that, the files can be stored in cloud like iCloud, Google, Gmail, etc. so that we can able to access files from anywhere and are secured. The files are uploaded in cloud with encryption and large number of files can be stored.

REFERENCES

1. https://www.tutorialspoint.com/randroid/an-droid_resources.htm
2. https://developer.android.com/guide/inde-x.html
3. https://www.engineersgarage.com/articles-/what-is-android-introduction
4. http://www.beginandroid.com/intro.shtml
5. http://www.gcflearnfree.org/androidbasics/intro-to-android-devices/1/

ISSN: 2278-4632
Vol-10 Issue-5 No. 1 May 2020

6. https://en.wikipedia.org/wiki/Android
7. A Digital Locker for Scanned Documents by using Steganography and Visual Cryptography, Ms. Vaishnavi J. Deshmukh , Dr. M .A.Pund, International Journal of Scientific & Engineering Research, Volume 7, Issue 2, February-2016 ISSN 2229-5518.
8. Digital Locker. Ms.Mehek Gulati , Ms.Kanika Verma. June 2016, Volume 3, Issue 6 JETIR (ISSN-2349-5162).
9. Rajasekar, P. and Mangalam, D. (2016) Efficient FPGA implementation of AES 128 bit for IEEE 802.16e mobile WiMax standards. *Circuits and Systems*, **7**, 371-380. doi: 10.4236/cs.2016.74032.
10. Digilocker (Digital Locker - Ambitious Aspect of Digital India Programme)., Purushottam Petare,, Pratapsinh Mohite, Mugdha Joshi,GE-International Journal of Management Research, Volume - 3, Issue- 6 (June 2015) if-4.316 ISSN:(2321-1709) Page no-299-308.

Author's Profile:

T. Anil Karuna Kumar has received his PG degree in *Master of Computer Applications* from R.V.R & J.C College of Engineering, affiliated to *Acharya Nagarjuna University, Guntur.* At present he is working as an *Associate Professor* in Narayana Engineering College, Gudur, Andhra Pradesh, India.

M. Sushma has received her B.Sc degree in *Computer Science* from Pragathi Degree College, Kota affiliated to *Vikrama Simhapuri University, Nellore* in 2017 and pursuing PG degree in *Master of Computer Applications* (MCA) from Narayana Engineering College, Gudur affiliated to *JNTU, Ananthapur,* AndhraPradesh, India.