*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 2, Ver. II (Mar. - Apr. 2018), PP 73-78*
*www.iosrjournals.org*

# Secure Digit Locker Application

B. Nandan[1], Devulapally Divyateja[2], Edukulla Keerthi[3],
Karipe Veera Manikanta[4]

[1]*Associate Professor, Department Of CSE, GNITC, Ibrahimpatnam, Hyderabad, Telangana.*
[2,3,4]*Department Of CSE, GNITC, Ibrahimpatnam, Hyderabad, Telangana.*
*Corresponding Author:B. Nandan*

**Abstract:** ***Secure*** *Digi locker application is an advanced application where we can store the files or documents such as certificates, PAN Card, Birth certificates, legal documents or confidential documents etc. in the internal memory. It makes it easy because holding or carrying the documents manually is difficult as there may be chances of misplacing. The application is developed where the files are uploaded and stored in the encrypted format with the key generation to avoid any kind of hacking. The registered users have permission to access the files. If the user is an intruder and wants to access the files then the message is sent to the actual user. The security is provided with the help of key generated with password entered.*

***Keywords:*** *secure, encryption, key generation.*

---

Date of Submission: 21-03-2018 Date of acceptance: 06-04-2018

---

## 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.

OBJECTIVE

Earlier Digi locker was processed with the motive of reducing physical documents and empower sharing

of e-documents over intervention. The objective of this application is that individual's documents and images can be secured and kept safely by uploading in the phone memory with an encrypted format. It will help the user to protect their documents or files from an intruder and also from losing manually. It auto decrypts by using password which acts as a key to access the files or images.

PURPOSE

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.

SCOPE

The scope of this application is that to ensure safety, privacy and secure of documents or images. The need to achieve, is to eliminate the use of physical documents and to store the files securely in phone memory. This security can be provided by using encryption technique i.e. AES (Advanced Encryption Standards) with 128 key bits.

## II. Literature Survey

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 fingerprint imageof 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 we have a tendency 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 transforms 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].

## III. Existing Method

To secure the files or documents earlier we use Digital Safe Lockers. It is an electronic safe protection system which can be operated by signals which are received from input key board and provide security to the users. Digital electronic lockers are however not much secured and reliable but they are simple to use. The existing method doesn't provide protection from hacking. The electronic safe lockers are not easily available and user cannot access the files immediately when required.

## IV. Proposed Method

The proposed system develops a system that saves the documents in an encrypted format and stores in the internal memory or external memory by using AES Encryption technique to avoid from hacking. the files are uploaded and can be accessed by auto decrypts when entered password.
User registers and logins to upload files or images to store in memory with an encrypted form. This application is for individual purposes to store their documents privately.

**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 $10^{th}$ 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 ($w_0$, $w_1$, $w_2$, $w_3$) 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 $1^{st}$ round output is taken as $2^{nd}$ round input and repeats the process until $10^{th}$ round. The output of $10^{th}$ round after **AddRoundKey** without

**MixColumns** is the desired 128 bits Cipher Text.

1. IMPLEMENTATION

There are three modules for Secure Digi locker application. They are as follows:

*USER INTERFACE*

In this module, to connects with the database user must give their username and password. If the user already exits directly can login into the database else user must register their details such as username, password and Email id, for registration. Name will be set as user id. Logging in is usually used to enter a specific page.

*UPLOAD FILES*

In these module after success registration of user. User logins to application. User can upload the files by filenames. After uploading of files and images every file is stored in application in encryption format. Every file as a key which is used to decrypt the file. When user want to access the file, they have to enter their password, then the file is decrypted using key provided for the file. If password is wrong it sends the message.

*AES ENCRYPTION*

Advanced Encryption Standard cipher with 128 bits key. This technique is useful for encrypting confidential or necessary data to be secured. AES is different from Fiestal Cipher. It is based on 'substitution-permutation network'. It has series of rounds called as transition rounds which includes Substitution bytes, ShiftRows, MixColumns, AddRoundKey. 10 rounds are performed for 128 bit key, 12 rounds for 192 bits and 14 rounds for 256 bit keys.

## V. System Architecture

In the System Architecture we have a node as a user, who registers first and logins to get authentication from database. The user profile consists of details of user such as username, password, mobile no., email id etc. The uploaded files are encrypted by using AES (Advanced Encryption Standards) technique. Once the files are uploaded and wants to access those files then password has to be given by user. If the password is matched then the files can be accessed.

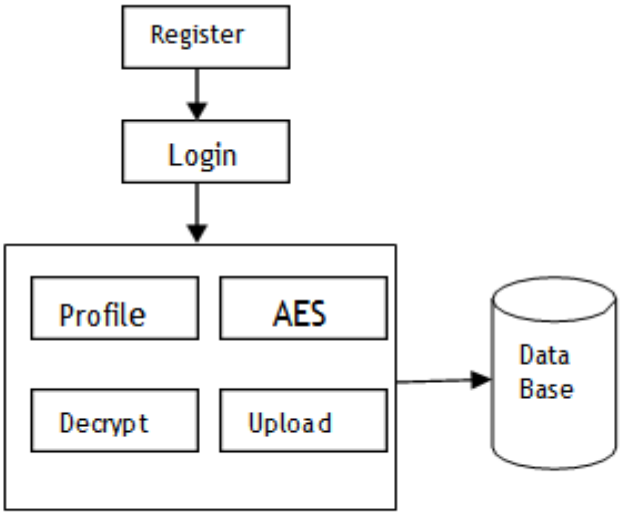


Fig.1 System Architecture

## VI. Results


**Fig.2** Registration page

The figure illustrates the registration page of Secure Digi Locker Application, where user give their credentials and sign up for login page.


**Fig.3** Login page

The figure illustrates the login page for an application, where user enters username and password to login successfully.


Fig.4 User Success Page

The figure illustrates the user success page. When the user logins successfully then they can able to upload or view documents.

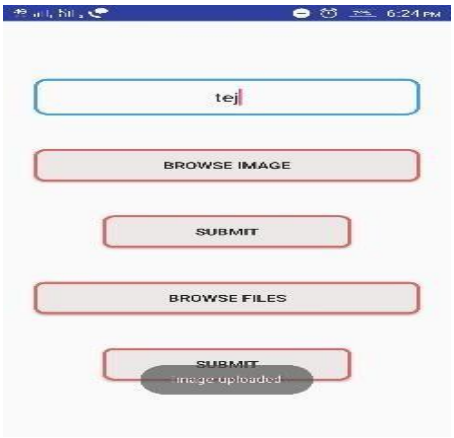


**Fig.5** Uploaded successfully

The figure illustrates that the images or files can be uploaded from phone memory. The user gives the file name and browse the images or files from memory and enters submit for uploading.


Fig.6 Accessing documents that are uploaded.

The figure illustrates that once the files or documents are uploaded they can be accessed by viewing into documents. To access those files user needs to enter the password to decrypt and the files are downloaded.

## VII. 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.

## VIII. Future Enhancement

Secure Digi Locker is an advanced application. The files are uploaded and encrypted in internal or external memory in mobile by using AES Encryption technique. 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. A user can access with a secured pin from anywhere if necessary. The AES encryption further can be used with 192 bits or 256 bits key size.

## References

[1] Visual Cryptography Authentication for Locker Systems using Biometric Input, Siddhesh Urkude, Pranjali Vaidya, Shagufta Rajguru. International Journal of Computer Applications (0975 – 8887) Volume 130 – No.1, November 2015.
[2] 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.
[3] Digital Locker. Ms.Mehek Gulati , Ms.Kanika Verma. June 2016, Volume 3, Issue 6 JETIR (ISSN-2349-5162).
[4] 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.
[5] Secure Storing and Sharing of Documents on Cloud Pavan Ughade, Nikita Kapsi, Asha Mallappagol, Apoorva Tangod IOSR Journal of Computer Engineering (IOSR- JCE) e-ISSN: 2278-0661, P-ISSN: 2278-8727 PP 67-71.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

B. Nandan " Secure Digit Locker Application." IOSR Journal of Computer Engineering (IOSR-JCE) 20.2 (2018): 73-78.