Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 6, Issue 4, April-2019

Document Storage And Retrieval System Using Aadhaar Number

Abhishek Sarje
Information Technology (IT),
Pimpri Chinchwad College of Engg.
Pune, India.
abhisheksarje007@gmail.com

Abhijit Pawar
Information Technology (IT),
Pimpri Chinchwad College of Engg.
Pune, India.
abhijitdpawar2@gmail.com

Prof. Sachin. R. Jadhav
Information Technology (IT),
Pimpri Chinchwad College of Engg.
Pune, India.
srjadhav02@gmail.com

Shashikant Pattewar
Information Technology (IT),
Pimpri Chinchwad College of Engg.
Pune, India.
pshashikant1998@gmail.com

Sourabh Nimse
Information Technology (IT),
Pimpri Chinchwad College of Engg.
Pune, India.
nimsesourabh5599@gmail.com

***Abstract*—: Aadhaar Number issued by UIDAI (Unique Identification Authority of India) has many advantages. They are used to create an authorized identity of individual by which individuals can be identified. This identity can be useful in applications of documents in banking, college, RTO's, etc. Our system is focused on storage of personal confidential documents of individuals by which they can access it from anywhere and at any time. To uniquely identify each individual, we use Aadhaar number as a unique user ID for everyone. User can be identified by their Aadhaar number as it is a unique number for each individual. Document security is provided using AES (Advanced Encryption Standard) algorithm. Documents will be encrypted using the AES Image Encryption Algorithm and stored. During document Retrieval the encrypted documents are decrypted using the Decryption Algorithm and then user can access them. User Validation is done by sending OTP (One Time Password) to the user or by providing a Biometric Scan of the user. Individuals documents can be accessed by either providing the OTP received by the user or by biometric scan of the user. At time of document retrieval, users permission is needed for his/her document access. This permission is given either by OTP or Biometric Scan. The application of this system in real world environment will reduce the paperwork related to documents in Government sectors. The use of documents in a digital way will reduce the maintainability and the effort of carrying the documents everywhere.**

Keywords: Aadhaar Number, AES (Advanced Encryption Standard), OTP (One Time Password), Biometric Scan, Storage, Retrieval, Validation.

I. INTRODUCTION

The need for document storage and retrieval has come about because electronic documents are gaining importance in various organizations like companies, government sectors, etc. As the world is getting digitalized, there is a requirement of storage space to store these electronic documents. These documents can be in many formats such as scanned images, MS Word files and audio and video files. Instead of storing them on remote machines, they can be saved in such a way that the digitalized documents possess the property of mobility. But by saving the personal data on a global network, there is a chance of security breach; hence to protect the privacy of confidentiality of data, there is a requirement of implementation of some security measures.

There is a system called "Digilocker.it provides same functionalities that we mentioned in our system. We have tried to improve these services by giving more security through encryption, decryption, validation and verification and more importantly we have worked on customer satisfaction. Our system is focused primarily on the storage and retrieval of personal documents and providing certainty to these stored documents. In other word, the storage should be done in a secured environment.

The UID Aadhaar is one of the prestigious projects in India where Biometric card [10][11] with Unique Identification Number will be issued to every citizen, as it requires registering all the 10 Fingerprints of the person. Fingerprint is the most essential part of the project, which makes the citizen distinctive. So, we have considered Aadhaar Number for user validation and verification.

This system is divided into two processes, Storage and Retrieval [1] with provision of Security. Storing process of these personal documents often includes registering the user by validating user using their Biometric information (i.e. data related to fingerprint), Aadhaar number [5] provided by UIDAI and Demographic data (i.e. data related to Name, Address, Gender, Date of Birth, Relationship, Mobile number and Email). After user validation, the user then needs to scan the documents and then upload them on our system. These uploaded documents are stored on our secured system environment by using image security algorithm such as AES (Advanced Encryption Standard) [3][8]. These documents can be accessed on user demand by verifying himself/herself on our system, by providing OTP (one-time password) [9] received by him/her at that instance or by giving fingerprint.

II. Problem Statement

To overcome the problem of showing any Identity Card to particular government officer or to any organizations where Identity proof is essential, we are going to develop a system which will save time and hassle of the authorized person of checking the document of the particular user whose information is stored in the database. We access the data using the UID Aadhaar card number, that we stored securely preventing from unauthorized access.

III. Literature Survey

A. Literature Survey Related to Document Security.

Paper - 1

"Arijit Karati, Member, IEEE, SK Hafizul Islam, MarimuthuKaruppiah, member, IEEE" [2].suggested that the Certificate less Signature scheme is a cryptographic primitive that provides data authenticity in IIoT systems. Refer Table III(a) for comparison of research done on document security.

Paper - 2

Sneha Ghoradkar, Aparna Shinde, Assistant Professor" [3] proposed that An Image Encryption and Decryption Using AES (Advance Encryption Standard) Algorithm drthat divides the image into blocks of 3x3 and changes the image quality of each block (Encryption) and stores the image and reverses the above procedure for retrieval of image (Decryption). Refer Table III(a) for the comparison of research done on document security.

Features	Paper - 1	Paper - 2
Document Security.	Low (provides the same key for the document and the user which can be easily accessed by any third party.)	High (encrypts the documents and stores it securely.)
Algorithm Used.	Uses a CLS scheme for data authenticity.	Uses Advanced Encryption Algorithm.

Table III(a) - Comparison of paper research done on document security.

B. Literature Survey Related to Storage.

Paper - 1

"Antonio M. A. Ferreira, André C. Drummond, Aletéia Patrícia F. de Araújo" [4] they suggested that the Cloud computing platforms provide easy and transparent access to a company's storage infrastructure through services. Which is commonly known as Storage as a Service, which allows users to store their data at remote disks and access them anytime. Refer Table III(b) for comparison of research done on storage.

Paper - 2

"Pramod K. Meher and Jagdish C. Patra" [1] in this paper authors has presented a novel technique for secure distributed storage and dissemination of digital documents using Chinese Remainder Theorem.The proposed technique not only involves significantly low computational complexity but it also imposes various stages of difficulties to an intruder who intends to extract the original image from the encrypted sub-blocks. Refer Table III(b) for comparison of research done on storage.

Features	Paper - 1	Paper - 2
Efficiency of performing user level operations.	High.	Low.
Computational Complexity.	Moderate.	Low.
Algorithm Used.	EDM (Electronic Document Management) Algorithm.	Chinese Remainder Theorem for secure distributed storage.

Table III(b) - Comparison of paper research done on cloud storage.

C. Literature Survey Related to Login Module.

Paper - 1

"Chopra, Ghadge, Padwal, Punjabi, and Gurjar, 2014" [5] in this paper author has explained that There can be improvements made when the image is captured using a camera, as it decreases the resolution factor of the images and thus, degrade their quality. The project can be extended for recognition of handwritten characters as well as its application in various fields of

recognition of diverse cards. Thus, the system has achieved the clarification for automatic reading of Aadhaar Card with a good accuracy. Refer Table III(c) for comparison of research done on login module.

Paper –2

"Deepu and Dr. Vijay Singh, 2012 Knowlton and Whittemore, 2008" [5]in this paper the authors has suggested that the government will use the information to issue identity cards the word which is generally known as AADHAR CARD, (Tiwari, 2013)described that the user logins to the account using his Aadhaar card number and the password which is provided to him at the time of registration and giving vote. Refer Table III(c) for comparison of research done on login module.

Paper –3

"Goel & Singh, 2014,and Shah & Shah, 2014" in this paper authors has described that India's most recent Aadhaar card includes QR code implementation [6]. Based on all the information the government consider only one card for the identity card of the person as Aadhaar card which is also helpful to provide the different government activities like to take subsidy and also take advantages of the different governments scheme. Refer Table III(c) for a comparison of research done on login module.

Features	Paper - 1	Paper - 2	Paper - 3
Security.	Less. (User's confidentiality is less.)	High. (The confidentiality of user is checked by providing an OTP to the registered mobile number.)	Moderate. (Provides a QR code to the user.)
Confidentiality of a User.	Weak.	High.	Weak.

Table III(c) - Comparison of paper research done on Login Module.

IV. Objectives of Implementation

- To create a Digital Document system and ensuring correct access management without loss of any document.
- To assess the problem to issue & collect the Government services with minimal arousal of issues.
- To eliminate the need for the residents to maintain hard copy of government issued documents which can be accessed at anytime, anywhere.
- To reduce the paperwork of documents and contribute towards healthy and green environment.
- To be more time/cost efficient.

V. Existing System

The existing system is "Digilocker ".This system is similar to our proposed system, there is only difference is in our system we have using AES algorithm for encryption of the document. In our proposed system the documents will be stored in encrypted format.

VI. Proposed System

This system can be used for document storage on a trusted environment and its retrieve for any application where document submission is necessary. This method can be useful for proper maintenance and management of documents. There will not be any need to carry the paper documents everywhere in handy. The document can be stored on a secured storage system and can be made easily accessible to user at anytime and anywhere.

Users can access the documents simply by entering the Aadhaar number as his/her username. An OTP will be sent to the registered number for users' authentication. In case of OTP failure another method provided for authentication is Biometric scan here, fingerprint. After the verification of Aadhaar number and OTP/fingerprint, user can gain access to his/her account and can store or retrieve the documents as necessary. Refer Figure VI(a) for architecture diagram.

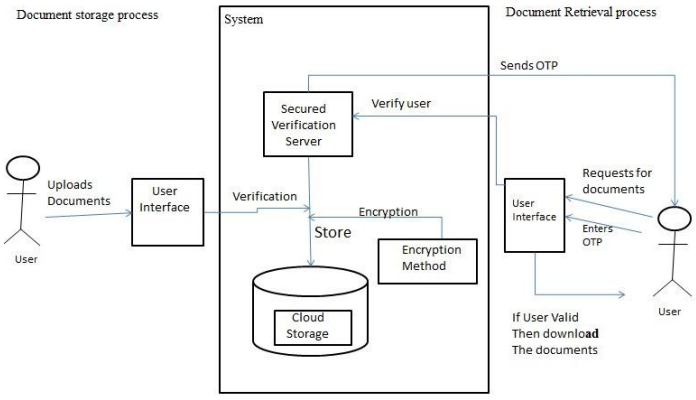

Figure – VI (a) architecture diagram.

VII. Implemented System

Our system is implemented in two parts.

A. Document Storage Process

This process includes registration of user. It is done by collecting Biometric Information and Demographic Data. The user then needs to convert the paper documents into digital format by means of scanning. Then the scanned image is uploaded and stored on cloud. Before storage is done the digital documents are Encrypted using AES Image Encryption Algorithm. Refer Figure VII (a) for block diagram of document storage process.

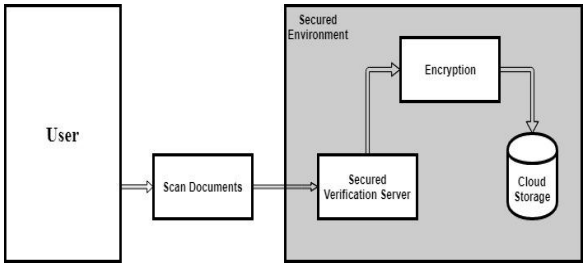

Figure VII (a) – Document Storage Process.

B. Document Retrieval Process.

This process is done to get back the digitally stored documents. This Retrieval process is done by verifying and validating the user for to overcome security breach. This is achieved by Fingerprint and OTP (One Time Password). After confirmation of the user the documents are Decrypted and are ready for download.Refer Figure VII(a) for block diagram of document retrieval process.

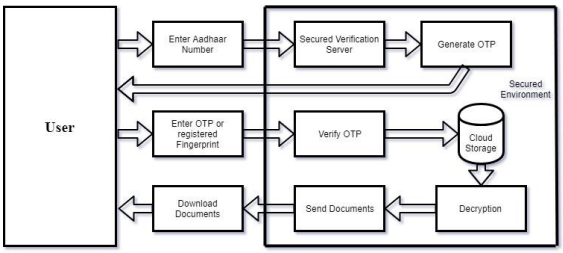

Figure VII(b) – Document Retrieval Process.

VIII. Modules of our System

Modules of our system are mentioned below.

1) Registration and Login module: - Registration module consists of list of fields where the user will input data and submit. Users have to register to the system in order to store the documents. For the system to identify each user, Aadhaar number is taken as the unique identification number from the users.

2) Document uploading module: - To upload the documents we have implemented this module. Document will be uploaded only if the document size does not exceed then specifies limit. Registered users can then upload their documents. The Administrator of the system does the work of uploading the documents.

3) Storage and Encryption: - Documents are stored on secured storage. Storage is done only after encryption of uploaded documents. The documents are encrypted using the AES Image encryption algorithm. The algorithm is applied to encrypt the documents, so that they cannot be accessible to anyone other than the user.

4) User Validation: - At the time of retrieval of documents, the authentication of user is must. In this module, user authentication is done by sending OTP to the registered mobile number or taking his/her biometric scan. This module is necessary to check whether the user has authorized access to the system

5) Decryption and Retrieval module: - Once user is authenticated, the documents to be retrieved can be selected and downloaded. The Decryption process also uses the AES image decryption algorithm. For retrieval of particular documents, the user needs to provide the OTP received or fingerprint. After this process the document is converted into decrypted format and is ready to be used.

IX. Algorithm Used

In our system we use the following algorithm for implementing a secured system.

A. Image Encryption AES Algorithm.

The process of encryption consists of encoding the data in such a way that the data can be accessed by only authorized user. The image which is to be uploaded is divided in the form of Matrix (3×3 Matrix). This divides the image in 9 blocks. We change the RGB values of each of the 9 blocks. RGB (red, green, and blue) refers to a system for representing the colors to be used on a computer display. Simultaneously system Note down the original values. These original RGB value are stored in such a way that they are secured and cannot be accessed by anyone other than the system itself. Encrypted image is stored [7][8]. Refer Figure – IX (a) for AES Encryption method.

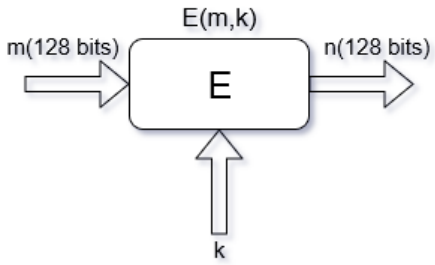

Figure – IX(a) AES Encryption method.

Where,

E- Encryption function for a symmetric block cipher.

m- Plain text message of size 128-bits.

k- Key of size 128-bits.

n- Cipher text.

Refer Figure – IX(b) for stepwise AES Encryption process and Refer Section IX for explanation of figure – IX(b)

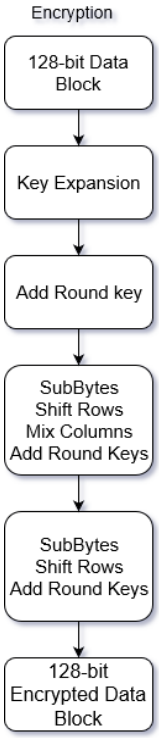

Figure – IX(b) Stepwise AES Encryption process.

Section IX:-

1. Perform Byte Substitution:-

   Byte substitution takes place in this step.

2. Perform Shift rows:-

   Each row of the matrix is shifted to the left. Any entries that ‘ fall off’ are re-inserted on the right side of row. Shift is carried out in following step −

3. Do not shift first row.
4. Shift the second row one position to the left.
5. Shift the third row two positions to the left.
6. Shift the ourth row to three positions to the left.
7. In result a new matrix is generated consisting of 16 bytes which are same but shifted with respect to each other .
8. Perform Mix Columns:-

   In this step each column transformed using mathematical equation,

9. To Add the Round Key:-

   In this step 16 byte matrix having size 128 bit are XORed with 128 bit round key.

B. Image Decryption AES Algorithm.

Decryption of encrypted data takes place using this algorithm. The authorized user can only decrypt the data because decryption requires a secret key or password. The original RGB values of each block in 3 x3 Matrix are access by the system. In this process encrypted value is replaced by the Original value from the database. The image is decrypted using this original RGB value [7][8].Refer Figure - IX(a) for AES Decryption method.

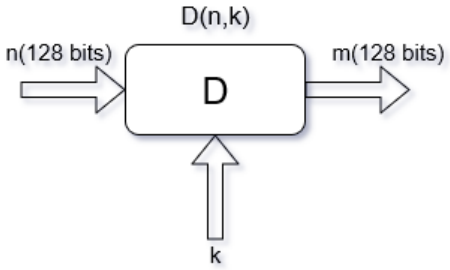

Figure – IX(c) AES Decryption method.

Where,

D- Decryption process for a symmetric block cipher.

m- Plain text(128-bits).

k- Key(128-bits).

n- Cipher text.

Refer Figure – IX(d) for stepwise AES Decryption process and Refer Section IX for explanation of figure – IX(b)

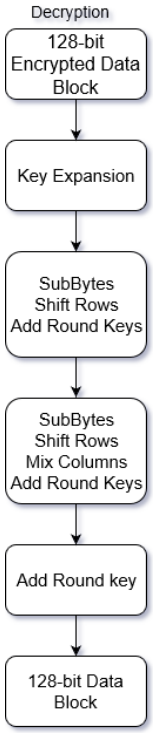

Figure – IX(d) Stepwise AES Decryption process.

C. Image Uploading method.

Basically, Uploading is the transmission of a file from one computer system to another, usually larger computer system. From a network user's point-of-view, to upload a file is to send it to another computer that is set up to receive it. In this project image uploading is must for creating the secret image for hiding the information for security purpose. Firstly, you have to add packages for accessing the methods and functions. Then you have to add the drives for connecting the database. Then you create the connection link for database. Then you put the proper SQL query for storing the image into database.

D. OTP Generation.

Here OTP is a typical two-factor authentication process, which is used for authentication of user. when a user enters Aadhar number and click on button "send OTP", a one-time password is generated which is sent to registered mobile number or email and then the user types that OTP, The server then also runs OTP to verify the entered one-time password [9].
Here we are using "SMSZONE" for sending the OTP.

E. Biometric Authentication.

The authentication is done by the third-party website (000webhost). 000webhost is one of the very few web hosts which give you the ability to host your website while paying nothing. 000webhost provides free users with 1.5 GB of free disk space which is quite a lot especially if you consider that you are practically paying nothing for it. 000webhost provides you with 100 GB bandwidth which is made possible by the unmetered connections their servers utilize. Our fingerprint sensor scans the user's finger and sends the scanned data to the third-party website which in turn provides a unique id for the data. This id is later used during Retrieval process for comparing the data received during Registration process. For this sending and receiving data a Wi-Fi module is required which is attached to our fingerprint sensor.

X. Conclusion

The proposed method is a great contribution towards moving towards healthy and green environment. As our focus was on creating paperless India, we have achieved it to some extent. Digitally storing documents makes reduction in demand of paper and in turn reduces the damages done to the environment by cutting down trees. The system also saves time and also the efforts required for carrying documents in handy. This system can be used by anyone having Aadhaar card, at any time, at anywhere with ease.

XI. Acknowledgment

We wish to express our profound thanks to all those who helped us directly or indirectly in implementation of our system. We wish to thank to all our friends and well-wishers who supported us in completing this project successfully. We are especially grateful to our guide Mr. Sachin Jadhav for time to time, very much needed and valuable guidance. Without the full support and cheerful encouragement of our guide, this implemented system would not have been completed on time. We take this opportunity to express our thanks to all who rendered their valuable help, along with all those unseen people across the internet for maintaining those valuable resources for the successful completion of our project. We owe my success to all of them.

XII. References

[1] Pramod K. Meher and Jagdish C. Patra, "A New Approach to Secure Distributed Storage, Sharing and Dissemination of Digital Image," ISCAS 2006, 0-7803-9390-2/06/$20.00 ©2006 IEEE.

[2] Arijit Karati, SK Hafizul Islam, *and* Marimuthu Karuppiah, "Provably Secure and Lightweight Certificateless Signature Scheme for IIoT Environments," 1551-3203 (c) 2017 IEEE, in press.

[3] Sneha Ghoradkar, and Aparna Shinde, " Review on Image Encryption and Decryption using AES Algorithm," International Journal of Computer Applications (0975 – 8887) National Conference on Emerging Trends in Advanced Communication Technologies (NCETACT-2015).

[4] Antonio M. A. Ferreira, André C. Drummond, and Aletéia PatríciaF. de Araújo, "Performance Evaluation of a Private Cloud Storage Infrastructure Service for Document Preservation,".

[5] Pramod K. Meher and Jagdish C. Patra, "A New Approach to Secure Distributed Storage, Sharing and Dissemination of Digital Image," ISCAS 2006, 0-7803-9390-2/06/$20.00 ©2006 IEEE.

[6] Nimesh P. Bhojak, "Access the awarenes level of people on aadhar card as public welbeing," International Journal of

Interdisciplinary and Multidisciplinary Studies (IJIMS), 2015, Vol 2, No.5, 88-95, ISSN: 2348 – 0343 .

[7] Sharu Goel, and Ajay Kumar Singh, "Cost Minimization by QR Code Compression," Cost Minimization by QR Code Compression ISSN: 2231-5381.

[8] Ako Muhamad Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data,".

[9] Priya Deshmukh, "An image encryption and decryption using AES algorithm," International Journal of Scientific & Engineering Research, Volume 7, Issue 2, February-2016 ISSN 2229-5518.

[10] Swapnoneel Roy, Matt Rutherford, and Charlene H. Crawshaw, "TowardsDesigningandImplementingaSecureOneTimePassword(OTP) AuthenticationSystem," 978-1-5090-5252-3/16/$31.00 ©2016 IEEE.

[11] Cătălin LUPU, Vasile-Gheorghiță GĂITAN, and Valeriu LUPU, "Fingerprints used for security enhancement of online banking authentication process," ECAI 2015 - International Conference – 7th Edition Electronics, Computers and Artificial Intelligence 25 June - 27 June, 2015, Bucharest, ROMÂNIA, 978-1-4673-6647-2/15/$31.00 ©2015 IEEE.

[12] Ravi Subban, and Dattatreya P. Mankame, "A Study of Biometric Approach Using Fingerprint Recognition," Lecture Notes on Software Engineering, Vol. 1, No. 2, May 2013, DOI: 10.7763/LNSE.2013.V1.47.