I. J. Computer Network and Information Security, **2018, 5, 37-44**
Published Online May 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.05.05

A Solution to Secure Personal Data When Aadhaar is linked with DigiLocker

Dr. Vinay Kumar
VIPS/IT, New Delhi, 110 080, India
E-mail: vinay5861@gmail.com

Ms. Arpana Chaturvedi and Dr. Meenu Dave
JIMS/IT, New Delhi, 110 070, India, Jagan Nath University/IT, Jaipur, India
E-mail: {ac240871, meenu.s.dave}@gmail.com

Received: 17 November 2017; Accepted: 09 February 2018; Published: 08 May 2018

Abstract—With spread of digitalization in India, the government initiated many welfare schemes for citizens as a part of e-governance. To ensure security, it is made mandatory to link Aadhaar card of beneficiaries with different schemes. The government also proposed to link UIDAI with DigiLocker to lead India towards the paperless economy. Due to this, worries related to security concern arise. Once UIDAI connected with DigiLocker, a resident can share personal data with other agencies. It generates enormous amount of Data and it may cause misuse of personal data. It is very important to keep data secure with controlled and authenticated access. It is a challenge to manage and secure this amount of data. In this paper, we propose a framework and model to secure personal data using proper authentication process. Availability of the documents should be verified by the owner and post verification, the document should be accessible for the limited time. Failing which revalidation is required.

***Index Terms*—**DigiLocker, UIDAI, URI, URL, SHA256, MD5, JSON, OTP, SSL, MAC, PAN, BPL.

I. Introduction

A citizen needs to carefully store documents like Birth Certificate, Medical Documents, Passport, PAN (Permanent Account Number) Card, Voter ID Card, Ration Card, BPL (Below Poverty Line) Card, Degree Certificate, License etc. [1]. Today an individual is required to carry the original as well as the true copy of the documents for various mandated reasons and requirements to access services. To access documents online from anywhere anytime, it is must to store them securely in electronic form on the cloud.

In November 1994, the government proposed the "DigiLocker concept. It stores all sorts of documents like government issued documents, academic certificates etc., for easy sharing on the web. It enables access to stored documents for various public and private services. As part of the Digital India initiative, the beta version of DigiLocker has been launched. It is an Aadhaar (unique identity card for Indian citizens) linked facility housed at the Department of Electronics & Information Technology (DeitY), Ministry of Communications & IT and it facilitates with online document storage [1].According to DigiLocker National Statistics, total number of registered users is 75,34,978, total number of uploaded documents is 90,59,572,total number of available documents with system is 1,75,2873,331, total number of issuer organizations associated is 30, requestor organization associated with the system is 10 and total number of eSigned documents is 4,18,366[2]. The aim of the government is to link Aadhaar card with different welfare schemes to stem pilferage and leakage of funds that do not reach to the end beneficiaries. It makes easier for citizens to access various services. According to the past experiences, Aadhaar card number and OTP (One Time Password) enabled accesses to DigiLocker facilities are not fully secure. Many cases are there where OTPs has also been illegally accessed and Aadhaar card numbers would be more easily known. It is due to the wide usage of the same data of an individual by different organizations to provide various services to right beneficiary.

According to the survey [3], India has around fifty-eight thousand (58,000) Aadhaar linked DigiLocker. It provides dedicated personal storage space of 10 MB (Mega Bytes) to every individual. This may be increased in future to 1 GB (Giga Bytes) [4]. The maximum size of e-document in the facility has been restricted to less than 1 MB and it allows pdf, jpg, jpeg, png, bmp and gif file types [5]. This online document storage facility would facilitate over 81.78 crore citizens across the nation [6]. The document issuers such as the Central Board of Secondary Education (CBSE) and the Income Tax Department could issue certificates to the citizens in electronic format via the Digital Locker. Once documents are uploaded on this site it will act as authorized documents. Individual who is the owner of the account in DigiLocker can only access the documents. It stores e-documents as well as store Uniform Resource Identifier (URI) link of e-documents issued by various issuers from Government Departments [7]. It has e-sign facility to digitally sign e-documents. Any document like government certificates or academic certificates can simply be shared by a DigiLocker link.

This paper is organized into ten sections. Section 2 deals with the problem of the traditional system, Section 3 deals with benefits of Aadhaar linked DigiLocker, Section 4 deals with the working of DigiLocker System, Section 5 deals with challenges of drawbacks of DigiLocker System, Section 6 deals with major DigiLocker security concerns. In Section 7 proposed solutions to mitigate security risks is highlighted. Security implementation model is highlighted in Section 8. Use cases for the proposed system are discussed in Section 9. The paper is finally concluded in Section 10.

II. Problem with Traditional System

Citizen of India need to show their personal documents everywhere to avail any kind of services depends upon the services they want to avail. Those required documents might not be physically present at that time. Documents required can be academic documents or personal documents. It has been experienced by many people that several times we were not able to present the required document. Broadly problems exist in traditional systems are:

- Usage and availability of physical form of academic and government issued documents of citizen's leads to huge administrative overhead [1].
- Difficulties in submission of multiple copies of physical document time to time.
- Proper verification of authenticity of the documents by Institutions/government/agencies.
- Chances of theft or lost of Original Documents.
- Chances of damage of Original Documents due to wear and tear [8].

III. Benefits of Aadhaar linked DigiLocker

Aadhaar linked DigiLocker provides many benefits (Fig. 1). DigiLocker contains two types of certificates, one educational and second life time. It alerts one month before the expiry date to some documents like passport and license to upload updated one. It has very transparent process. Once it gets logically linked with UIDAI (Unique Identification Authority of India) and then PAN (Permanent Account Number) card, can verify more accurately by matching uniqueness of first name, fathers name or husband's name. However at the same time last name can be failure [9].

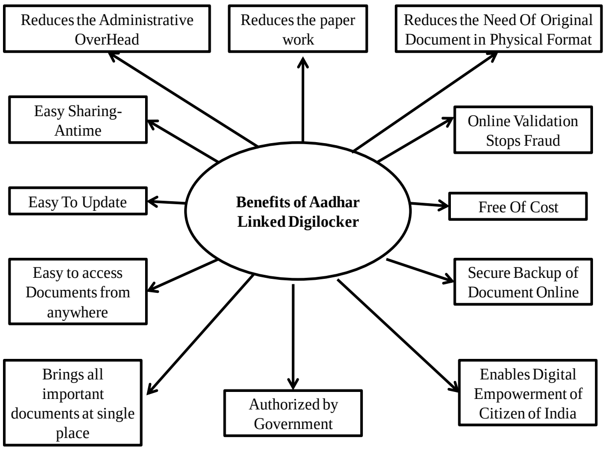
Reduces the Administrative OverHead
Reduces the paper work
Reduces the Need Of Original Document in Physical Format
Easy Sharing-Antime
Online Validation Stops Fraud
Easy To Update
Benefits of Aadhar Linked Digilocker
Free Of Cost
Easy to access Documents from anywhere
Secure Backup of Document Online
Brings all important documents at single place
Authorized by Government
Enables Digital Empowerment of Citizen of India

Fig.1. Benefits of Aadhaar Linked DigiLocker

IV. Working of DigiLocker System

To Sign-up for the DigiLocker you need to have an Aadhaar number and a mobile number registered with Aadhaar. The diagram (Fig. 2) shows the working with DigiLocker to upload documents like SSC (Secondary School Certificate) certificate, PAN card, Voter Id etc., and other options available after upload of documents.

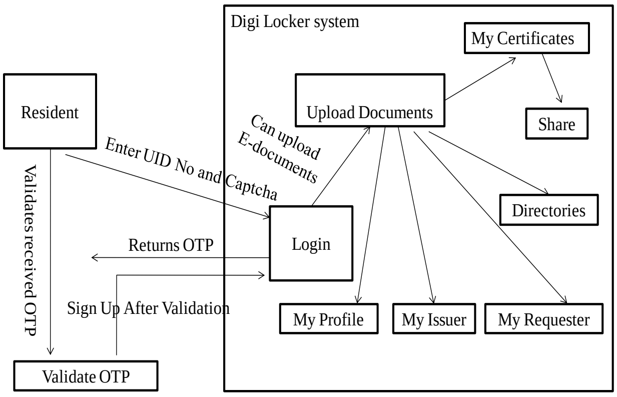

Fig.2. Working of DigiLocker System

Sub Options in DigiLocker Account of Resident have following functionalities.

a. "Share" option under "My Certificates" allows one to share documents.
b. "My Profile" option displays the complete profile of the resident (Name, Date of Birth, Gender, Residential Address, email, mobile number) as available in the UIDAI database.
c. "My Issuer" option displays the Issuer name and the number of documents issued.
d. "My Requester" option displays the Requester name and the number of documents of the resident requested by the requestor.
e. "Directories" option displays the complete list of registered Issuers and Requesters along with their URL [10].

V. Challenges or Drawbacks of DigiLocker System

The initiative taken by government to link DigiLocker System with Aadhaar has raised number of questions in the mind of common people. The main issue is that of security. People have doubt over security of their personal data. It is very difficult to trust the system. Various security challenges (Fig.3) or drawbacks of DigiLocker System are [11].

a. Aadhaar card and OTP based secure login is the only security mechanism provided for access to the digital locker. OTP while being significantly secure isn't as secure as having biometric verification at the end-user level. For this reason, the Unique Identification Authority of India (UIDAI) is in discussions with handset makers and operating system providers for embedding biometric identification technology onto mobile devices [12]. This will help people authenticate their Aadhaar biometrics on the phone itself to avail of various government schemes, subsidies and services. However, this would warrant additional security requirements in different layers of the data transfer to and from between end–user devices and server [1].
b. The DigiLocker needs an internet connection along with a smart device like a laptop/ desktop/ mobile for access making it inaccessible to a large population.
c. There is no integration between central government DigiLocker and the state government DigiLocker. For example, in an exercise carried out by R.S. Sharma, Secretary, Department of Electronics and IT, documents uploaded to the central government DigiLocker were successful in the first attempt but the same documents were not seen when logged into Maharashtra DigiLocker System [13].
d. There is no verification done on documents being accessed by other agencies like Government agencies, corporate etc.
e. Lack of online document verification facility, increases the possibility of fraudsters submitting fabricated or morphed documents. Documents of residents produced to any organization/requestor should always to be verified with reference to the original.
f. The system only supports 10 MB storage capacity per user which is low
g. Additional security layer can be used as Maharashtra DigiLocker System uses, where they also ask for a PIN number in addition to OTP [14].
h. Data can be stolen or misused from online repositories hence multiple layers of security are needed [15].

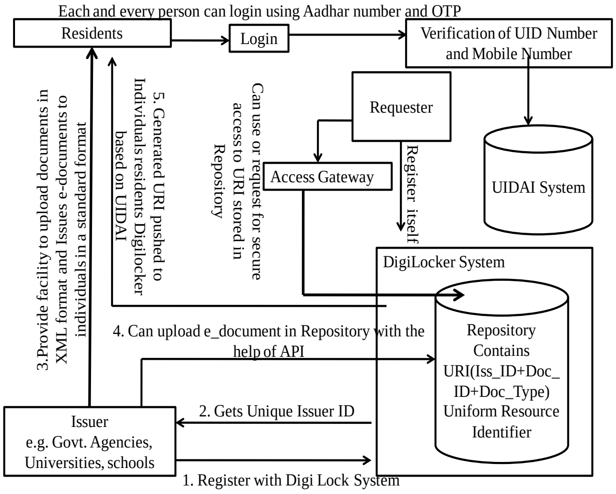
Each and every person can login using Aadhar number and OTP
Residents
Login
Verification of UID Number and Mobile Number
Requester
Access Gateway
UIDAI System
Register itself
Can use or request for secure access to URI stored in Repository
5. Generated URI pushed to Individuals residents Digilocker based on UIDAI
3.Provide facility to upload documents in XML format and Issues e-documents to individuals in a standard format
DigiLocker System
Repository Contains URI(Iss_ID+Doc_ ID+Doc_Type) Uniform Resource Identifier
4. Can upload e_document in Repository with the help of API
2. Gets Unique Issuer ID
Issuer e.g. Govt. Agencies, Universities, schools
1. Register with Digi Lock System

Fig.3. Challenges or Drawbacks of DigiLocker System

VI. DigiLocker Security Concern

The key security concerns are authentication, authorization at client-server both end and secure communication at the time of data traversal. Data transfer should be in an encrypted form with significantly high level of encryption standards. Maintenance of data integrity, verification of trust between both parties and exchange of trust certificates to complete the trust analysis enabling information exchange should also be in place.

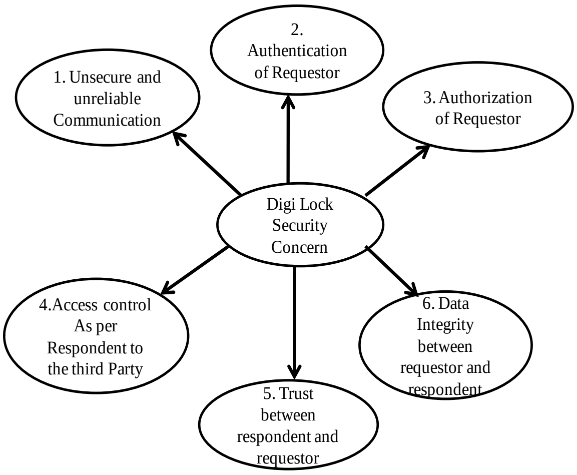
Digi Lock Security Concern
1. Unsecure and unreliable Communication
2. Authentication of Requestor
3. Authorization of Requestor
4.Access control As per Respondent to the third Party
5. Trust between respondent and requestor
6. Data Integrity between requestor and respondent

Fig.4. Digi Lock Security Concerns

VII. Proposed Solution to Mitigate Data Security Risks

It is proposed that the system should need to be defined minutely along with resource sharing services, proper data management with the services integrated with both the public and private environment. The system should be implemented with 256 Bit Secure Socket layer (SSL) Encryption for information transmitted during any activity. It should have an option of Mobile

Authentication based sign-up via OTP (One Time Password) to authenticate users. An additional security feature can be added to verify, it should ask for a PIN number in addition to OTP. For mobile applications, we should use JSON (Java Script Object Notation) as it will make faster transfer of information through mobile. The data centers should be ISO 27001 (International Organization for Standardization) certified to host the data. The data should be properly and securely backed up. System should be able to protect citizen's account from unauthorized access. Proper security audits should be done by recognized and authorized Security Audit Agency. The system should be automatically terminated sessions and it should be time bounded. Information is to be exchanged only by user consent. After mutual consent, only digitally signed documents should be granted access to the requestor.

In the case of unauthorized access to the documents, an alert message or email should be sent to the owner of the document. Requested documents should be made available to one device at a time only. Additionally, a constraint must be placed on document access wherein there is one user, one device, one document tagging. Moreover, the documents must be allowed to open in one tab only at a time instead of multiple tabs.

VIII. Proposed Security Implementation Model

In this paper, we studied various issues related to security. We have also studied in detail the working of DigiLocker System. We have proposed the model to provide better security (Fig. 5). Proposed security implementation model has two perspectives.

a. Security implementation model in requestor access scenario.
b. Security implementation model in resident permission grant scenario.

A. Security Implementation Model in user Access Scenario

Step 1: When a request is made to access a document, the request should go through the access gateway along with the requestor UID number.

Step 2: The Access gateway then verifies the aadhaar number of the requestor with the UIDAI System. If verified, it will generate a token ID which contains the requestor ID – that consists of Aadhaar number, mobile number, details of the document requested and resident ID.

Step 3: If the user permits/ grants access, an OTP would be generated (that's valid for a limited period of time typically 30 minutes or lesser) to both the requestor and user mobile numbers

Step 4: The generated token ID goes to the user for acknowledging the grant of access.

Step 5: Once OTP is verified, access to the system is granted for a limited period of time by sharing a URI from the repository.

Step 6: The URI that's shared with the requestor will be transferred in an encrypted format which will get decrypted at the requester end.

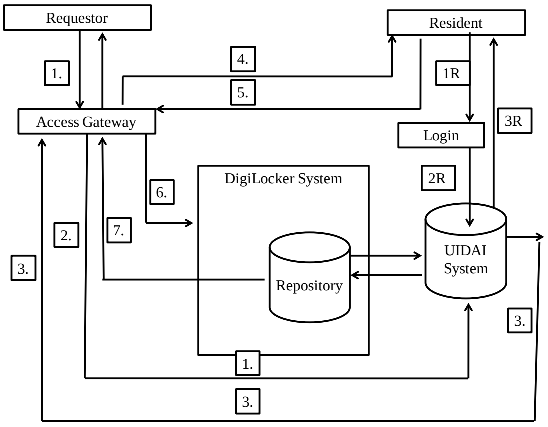

Fig.5. Security Implementation Model

B. Security Implementation Model in Resident Permission Grant Scenario

Step 1: The resident has to login to DigiLocker System with aadhaar details.

Step 2: Aadhaar details are verified by the UIDAI System,

Step 3: Once verified, a resident id is generated that serves two purposes: a) allows the user to upload documents to the repository in a standard XML format. b) Granting authenticated requestor to access the required documents.

IX. Use Cases for the Proposed System

A. Use Case I

Upload of a document by student or by citizen of India. They must be a registered user. The process is defined in Table 1.

Use Case Overview

Provide facilities to all the residents or students to upload or provide documents at one place i.e. repository. A resident should be registered user and verified with UIDAI, should have resident_id generated by the system. This online storage facility will save time, money and paper.

Pre Condition

a. The student should have valid Aadhaar number and Email account linked with UIDAI.
b. The resident should provide details to the DigiLocker authorities to grant access to upload. This could be automated via necessary PIN, OTP mechanisms and aadhaar verification of the resident.
c. The resident should have registered ID allotted by DigiLocker system after linking them Aadhaar.
d. The resident must be carrying a valid Aadhaar number linked with provided mobile number.
e. There should be individual portals for Student Portal

and must be integrated at the data end.

Post Condition

After successful upload of documents, the data must be stored in an encrypted form.

a. The resident should only allow sharing the documents with the correct requestors.
b. Verification should be done and the resident grant access to the requestor. The documents URI (Uniform Resource Identifier) in encrypted form should be shared with the verified requestor.
c. Documents should be shared for the limited period of time and enabled the requestor to open once the document on one tab only.
d. "View" option should be available to view rights and documents shared along with requestor details.
e. Access should only be role based and registered user based.

Table 1. Upload of a Document from Student

Use Case Id	Unique i.e. Uc_resid_001
Use Case Name	Upload of a document student/ citizen of India.
User Goal	To provide the platform to all students/citizen of India to upload their certificates/documents etc. in digital form.
Trigger Point	This use case will particularly trigger or will work when valid credentials of data of resident are provided. Example, when a student or citizen or registered user wants to upload documents in DigiLocker, it verifies credentials of an individual.
Actors	The student/Indian National Any official person in college or university on behalf of student.

Relationship with other Use Cases

Table 2. Relationship with other use Cases

Use Case ID	Use Case Details
Uc_issid_002	Issuer Use Case
Uc_reqid_003	Sharing of document with Requestor
Uc_vid_004	View of Rights and Document shared

B. Use Case II

Upload of a document from issuer e.g. Registrar Office, Income Tax Department, University, Municipal Council, and Election Commission of India. They all should be registered issuer. The process is defined in Table 3.

Use Case Overview

Provide facilities to all issuers to upload or provide documents at one place i.e. repository. Issuer and resident should be registered user and verified with UIDAI. This online storage facility will save time, money and paper.

Pre Condition

a. The Issuer should have valid Aadhaar number and Email account linked with UIDAI.
b. The Issuer should have registered ID allotted by DigiLocker system after linking them Aadhaar.
c. The Issuer should provide details and approach dig locker to allow them.
d. The Issuer must be carrying a valid Aadhaar number linked with provided mobile number.
e. Authorization letter from university or government agency to the person who can upload documents of individuals.
f. There should be individual portal for Issuer so that authorized person can use it.

Post Condition

a. After successful upload of the documents, it should be kept in encrypted form
b. Authorized and registered Issuer should only upload document of registered resident and resident is only allowed sharing of the documents with right users or requestor.
c. Before sharing verification should be done and after getting acknowledgment from resident documents URI (Uniform Resource Identifier) can be shared.
d. Every document issued must have this unique document URI in the format "issuerId- Digital Locker Technology Specification (DLTS) – Version 2.3 Page 10 of 16 docType-docId" printed (human readable) along with a barcode (machine readable, using "QR code"). Older documents being digitized should be defined under published list of document types so that just by using document ID, corresponding URI can be dynamically formed and document accessed from its repository [15].
e. View option should be available to view rights and documents shared with requestor details.
f. Documents should be shared for the limited period of time and enabled the requestor to open once the document on one tab only.
g. Once issuer upload documents, without acknowledgement of resident no further modification or re-upload of the document is allowed.
h. Access should only be role based and registered user based.

Table 3. Upload of a Document from Issuer

Use Case Id	Unique i.e. Uc_issid_002
Use Case Name	Upload of a document of registered resident/student/ citizen of India
User Goal	To provide the platform to all Issuer to upload the applied or legal certificates / documents etc. of registered residents in digital form.
Trigger Point	This use case will particularly trigger or will work when issuer upload e-document of registered resident in DigiLocker. It verifies credential of an individual before uploading documents.
Actors	The Issuer like Registrar Office, Income Tax Department, Election Commission of India, University, Municipal Council. Any official authorized person carrying authorization letter and linked the details with DigiLocker System.

Relationship with other Use Cases

Table 4. Relationship with other use Cases

Use Case ID	Use Case Details
Uc_resid_001	Resident Use Case
Uc_reqid_003	Sharing of document with Requestor
Uc_vid_004	View of Rights and Document shared

C. Use Case III

Share of document with requestor should be available as per the authenticated request from a registered requestor only. The process is defined in the table 5.

Use Case Overview

Provide facilities to share uploaded documents from the repository in URI format with the permitted requestor. Requestor should be registered user and verified with UIDAI. Document shared with requestor should be for the limited period, only after permission from resident and should allow him to open in one tab, once only.

Pre Condition

a. The requestor should have valid Aadhaar number and Email account linked with DigiLocker.
b. The requestor should seek permission from resident first.
c. The requestor should provide details and approach DigiLocker to allow them and then resident should acknowledge accessing the desired digitally signed document.
d. Sharing should be allowed for limited period of time and should allow accessory to use it once and open in one tab only.

Post Condition

a. Sharing is allowed for the limited time hence it checks the activated time period, once over deactivate the permission to access or view documents.
b. Should be able to view the record of the requestor and Document Details shared with.
c. View option should be available to view rights and documents shared with requestor details.
d. Should not allow the document to open in more than one tab and should allow opening once only.
e. Access should only be Role based and registered user based.

Table 5. Sharing of Document with Requestor

Use Case Id	Unique i.e. Uc_reqid_003
Use Case Name	Sharing of a document
User Goal	To provide the platform to all requestor to request for certificates / documents/ etc of registered residents.
Trigger Point	This use case will particularly trigger or will work when either requestor request to view documents of a resident or resident want to share document with requestor. It verifies credential of an individual.
Actors	1. Requestor 2. Resident

Relationship with other Use Cases

Table 6. Relationship with other use Cases

Use Case ID	Use Case Details
Uc_resid_001	Resident Use Case
Uc_issid_002	Issuer Use Case
Uc_vid_004	View of Rights and Document shared

D. Use Case IV

View of Rights and Document Shared. The process is defined in the table 7.

Use Case Overview

It keeps the audit report for future referral. Later on, if any resident wants to view or track history of his account, he/she can check. One can view that which requestor has used what all documents, share date and view time.

Pre Condition

a. The requestor should have valid Aadhaar number and Email account linked with UIDAI.
b. The requestor should seek permission from resident first.
c. The requestor should provide details and approach DigiLocker to allow them and then resident should acknowledge accessing the desired digitally signed document.
d. Sharing should be allowed for the limited period of time and should allow the one to use it once and open in one tab only.
e. Keep storing the details at the back end for future retrieval.

Post Condition

a. As per the request check the details of a resident account.
b. Which requestor is been shared resident's document.
c. What all document requestor requested for.
d. On which date requestor requested and used for how long.
e. On the basis of request, search the details and display requestor id, document type, document name, date of request and time of request.

Table 7. View of Rights and Document Shared

Use case id	Unique i.e. Uc_vid_004
Use case name	Viewing details of requestor and documents viewed
User goal	To provide platform to view the details of document used by which requestor and on which date, at what time
Trigger point	This use case will particularly trigger or will work when verified requestor used the documents of some resident. It keeps audit record requestor, document name, document type, date of view, time of view
Actors	1. Requestor 2. Resident 3.API (Application Programming Interface)

Relationship with other Use Cases:

Table 8. Relationship with other use Cases

Use Case ID	Use Case Details
Uc_resid_001	Resident Use Case
Uc_issid_002	Issuer Use Case
Uc_reqid_003	Sharing of document with Requestor

X. Conclusion

In the present DigiLocker System it uses HTTPS connection along with TLS 1.2 (Transport Layer Security). The connection is encrypted and authenticated with AES_128_GCM (Advanced Encryption Standard-128 - Galois Counter Mode) and uses ECDHE_RSA (Elliptic Curve Diffie-Hellman Key Exchange - Rivest, Shamir Adi) for key exchange mechanism.

In this paper we have proposed a security model based on use cases. We suggest in this case study, to implement the SHA (Secure Hash Algorithm) 256. It is better than already implemented techniques. After reviewing various papers we propose SHA 256 encryption technique in place of MD5 (Message Digest). SHA-256 is a cryptographic hash function with digest length of 256 bits and can be used to match keys while communication. It is a keyless hash function; that is, an MDC (Manipulation Detection Code). It is to check authenticity, digital signatures, digital time stamping, and entity authentication. SHA-256 is suggested because it provides services of data integrity and better authentication services when used in combination with digital signature algorithms and Media Access Control (MACs). It is also suggested that every requestor should be allotted with browser id and session id to open a document. Once this system is incorporated with mobile technology, JSON should be used which would help reduce time to access heavy documents.

Acknowledgment

This research was supported by various research work done by different researchers and their published papers. We thank them as their research work has provided the insight and expertise to me and their work has greatly assisted my research. We are grateful to the reviewers for their comments on an earlier version of the manuscript.

References

[1] S. Reddy, "Govt's Digital Locker System - Details & Benefits of "DigiLocker"", ReLakhs.com, 2017, https:// www. relakhs.com / digital – locker – system – DigiLocker -govt-facility/.

[2] National eGovernance Division Ministry of Electronics & Information Technology (MeitY), DigiLocker Dashboard", Digilocker.gov.in, 2017, https://digilocker.gov.in/public/dashboard.

[3] Aadhaar Card Guru, "What is Aadhaar Linked DigiLocker and how it Works? Aadhaar Card, 2017, https://aadharcard.in/aadhar-linked-digilocker.

[4] Pradeesh Chandran," DigiLocker gets good response", The Hindu, 2017, http:// www.thehindu.com /scitech/technology/internet/digilocker-gets-good-response/article7016197.ece.

[5] Dr. J.K. Bhutani, "Digital India: Digital locker, security issues and poor interface", NewsGram, 2017, https://www.newsgram.com/digital- India - digital- locker -security-issues-and-poor-interface/.

[6] Kartikeya Saigal, "All you need to know about DigiLocker", Governance Now, 2017, http:// www .governance now .com / gov-next /egov / all-you-need-to-know-about-the-DigiLocker.

[7] A Digital India Initiative National e-Governance Division, Department of Electronics and Information Technology,2017,https://digilocker.gov.in/assets/img/DigiLocker-Pull-API-Specification-v1%200-1.pdf.

[8] Negd.gov.in, 2017,http: // negd.gov.in/ writereaddata/ files/Digital%20Repository/Digital%20Locker%20System%20%28DigiLocker %29%20-%20A%20 Government%20 of %20 India %20 Initiative.pptx.

[9] Nitin Bhatia, 2017, http://www.nitinbhatia.in /views/advantages-of-DigiLocker-service/.

[10] National Portal of India, 2017, https: // India .gov .in / spotlight/DigiLocker-online-document-storage-facility.

[11] Susheel Tiwari, 2017, https: // www. quota. com/ Is -the-governments-DIGILocker-safe-What-are-the-security-features-that-assures-me-my-documents-cant-be-stolen.

[12] A. Sharma and N. Alawadhi, "UIDAI wants to make mobile phones Aadhaar-enabled, holds discussion with Smartphone makers", The Economic Times, 2017, http : // economictimes.indiatimes.com / tech / hardware / uidai-wants-to-make-mobile-phones - Aadhaar-enabled-holds-discussion- with – Smartphone - makers / article show / 53441186.cms.

[13] Ambika Choudhary,"Aadhaar Linked Digital Locker Goes Live. Here Is How To Securely Store Documents Online!" Trak.in - Indian Business of Tech, Mobile & Startups,2017,http://trak.in/tags/business/2015/02/12/aadhaar-digital-locker-store-documents-online/.

[14] K V Chowdary, Central Vigilance Commissioner, PTI,"CVC calls for foolproof system to verify bank customers data", India today. in today. in, 2017, http : // indiatoday.intoday.in / story/ cvc-calls-for-foolproof - system - to-verify- bank-customers-data /1/ 710323.html.

[15] "Digital Locker" Technology Specification (DLTS) Version 2.3, March 2015, https:// digilocker.gov.in/ assets/img/technical-specifications-dlts-ver-2.3.pdf.

Authors' Profiles

Dr. Vinay Kumar is Dean IT & Professor in Vivekananda Institute of Professional Studies, Delhi. Earlier he worked as Scientist in National Informatics Centre, MoCIT, GOI. He completed his Ph. D. in Computer Science from University of Delhi and MCA from JNU, Delhi. He has authored a book on Discrete Mathematics and contributed many research papers to refereed journals and conferences. His areas of interest are graph algorithm, steganography, data security, data mining and e-governance. He is member of CSI and ACM. Details available at http://knowdrvinaykumar.blogspot.in / Ph: 011- 2734 3402. E-Mail: vinay5861@gmail.com

Arpana Chaturvedi is working as an Assistant Professor in Jagannath International Management School, Delhi. She is M.Sc. (Math), MCA and M. Phil. (Comp. Sc). She is pursuing PhD from Jagannath University. PH-01149219191. E-mail: ac240871@gmail.com

Dr. Meenu Dave, M.Tech., Ph.D.(Computer Science) has taught Computer Science in different capacities at a number of Engineering Colleges and Institutes. At present, she is deputed as Professor and Dean, Faculty of Engineering & Technology, Jagan Nath University, Jaipur. She has extensive experience in teaching Cloud Computing, Artificial Intelligence, Knowledge Management and Data Mining at the post graduate level. She has also authored several research papers in the specified areas which have been published in leading journals. E-mail: meenu.s.dave@gmail.com

How to cite this paper: Vinay Kumar, Arpana Chaturvedi, Meenu Dave,"A Solution to Secure Personal Data When Aadhaar is linked with DigiLocker", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.5, pp.37-44, 2018.DOI: 10.5815/ijcnis.2018.05.05