ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.3

Digilocker Cloud Storage - Overview of Privacy Protection Security Measures

Sam Muthiah Franklin[1], Anita Fernandez[2]
Ph.D Student[1], M.Phil Student[2]
Department of Computer Science
Bharath Institute Higher Learning and Education,Chennai, India

Abstract:
Digital Technologies which include Cloud Computing and Mobile Applications have emerged as catalysts for rapid economic growth and citizen empowerment across the globe. Digital technologies are being increasingly used by us in everyday lives from retail stores to government offices. They help us to connect with each other and also to share information on issues and concerns faced by us. In some cases they also enable resolution of those issues in near real time. Cloud Computing is widely used technique for data storage on-demand but involves risk such as data security, privacy protection, access-control and data confidentiality. Digital Locker is one of the ambitious aspects of Digital India Programme. Privacy issues are increasingly important in the online world. It is generally accepted that due consideration of privacy issues promotes user confidence and economic development. However, the secure release, management and control of personal information into the cloud represent a huge challenge for all stakeholders. The present study provides an overview of Digital Locker and the privacy security measures.

Keywords: Biometric, Compliance DigiLocker, Disclosure, Electronic Signature, Encryption, Gateway, Monitoring, Personal Identifiable Information, Repository, Uniform Resource Identifier.

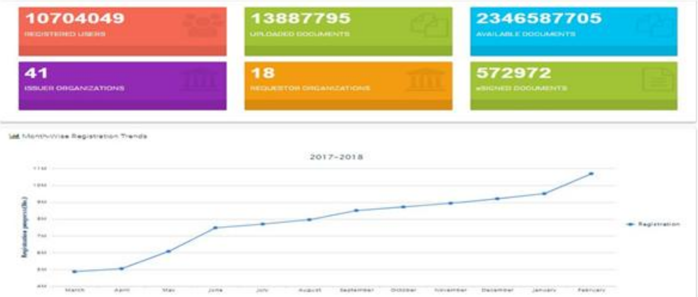
I. INTRODUCTION

Currently, in India, almost all of the government issued documents are in physical form across the country. This means every time a resident needs to share the document with an agency to avail any service, an attested photo copy either in physical form or on scanned form is shared. Use of physical copies of document creates huge overhead in terms of manual verification, paper storage, manual audits, etc. incurring high cost and inconvenience. This creates problem for various agencies to verify the authenticity of these documents, thus, creating loopholes for usage of fake documents/certificates. Due to the nature of these documents not having a strong identity attached to it, anyone with same name can indeed misuse someone else's document. Benefits include:

- ➢ Reducing administrative overheads and enabling easy access of service to individuals,
- ➢ It is an environment-friendly initiative that would reduce paper usage,
- ➢ Applying for identity cards and availing many services can have a quicker turnaround time as authentic documents will be easily accessible,
- ➢ Deterring financial fraud to a certain extent as all documents are validated and then shared with the requestor,
- ➢ All data would remain on servers located in India, and
- ➢ Two-factor authentication using mobile one-time passwords (OTPs) provides and additional layer of security.

DigiLocker is a "digital locker" service operated by the Government of India that enables Indian citizens to store certain official documents on the cloud. The service is aimed towards reducing the need to carry physical documents, and is part of the government's Digital India initiative. 1 GB of storage space is offered to users to store identification card issued by government agencies, education certificates, PAN cards, driving license, vehicle ownership documents and other documents. Personal data is not dealt with seriousness by many people and this can lead to data breaches wherein information can be copied and shared freely, without the individual's consent or knowledge. Spam and telemarketing have become an annoyance due to free sharing of personal data picked up from physical document copies. Fraudsters can also engage in identity theft, impacting individuals as well as corporations.

DIGILOCKER NATIONAL STATISTICS



10704049
REGISTERED USERS

13887795
UPLOADED DOCUMENTS

2346587705
AVAILABLE DOCUMENTS

41
ISSUER ORGANIZATIONS

18
REQUESTOR ORGANIZATIONS

572972
eSIGNED DOCUMENTS

II. PRIVACY DATA COLLECTED BY GOVERNMENT SCHEMES

The data collected under the various Government schemes include a variety of personal data including personally identifiable information that they are forced to disseminate in order to avail the benefits of the governmental welfare schemes. In all schemes, personal information of the users collected.

III. SENSITIVE PERSONAL DATA OR INFORMATION (SPDI)

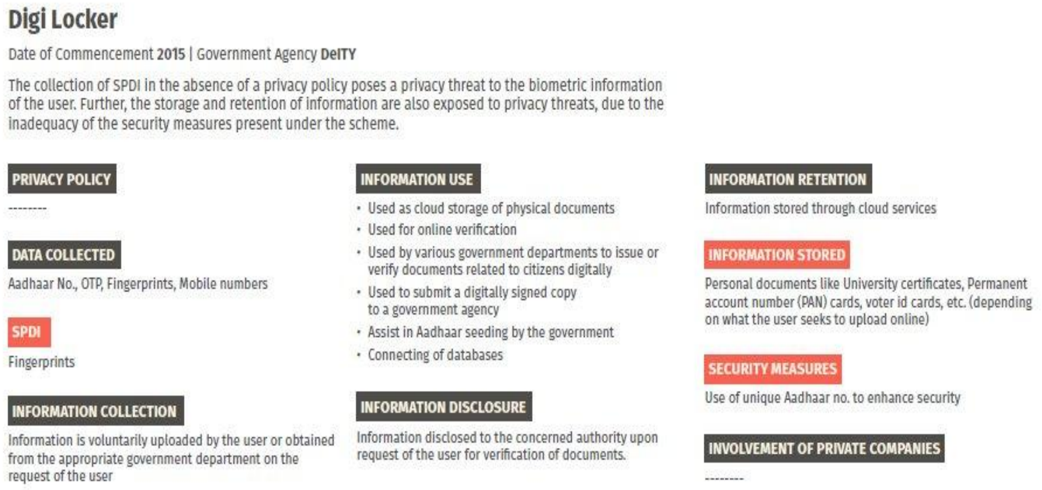
The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 is the only legislation that has defined SPDI (sensitive personal data or information). Under Section 3, the legislature has listed the data that can classify as SPDI are:

Sensitive personal data or information of a person means such personal information which consists of information relating to –

- ➢ Password;
- ➢ Financial information such as Bank account or credit card or debit card or other payment instrument details ;
- ➢ Physical, physiological and mental health condition;
- ➢ Sexual orientation;
- ➢ Medical records and history;
- ➢ Biometric information;
- ➢ Any detail relating to the above clauses as provided to body corporate for providing service; and
- ➢ Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise. The collected data stored in DigiLocker contains SPDI.

IV. "PRIVACY GAPS IN INDIA'S DIGITAL INDIA PROJECT" REPORT PUBLISHED BY "THE CENTRE FOR INTERNET & SOCIETY"

This paper seeks to assess the privacy protections under fifteen e-governance schemes: Soil Health Card, Crime and Criminal Tracking Network & Systems (CCTNS), Project Panchdeep, U-Dise, Electronic Health Records, NHRM Smart Card, MyGov, eDistricts, Mobile Seva, Digi Locker, eSign framework for Aadhaar, Passport Seva, PayGov, National Land Records Modernization Programme (NLRMP), and Aadhaar.



Digi Locker

Date of Commencement **2015** | Government Agency **DeITY**

The collection of SPDI in the absence of a privacy policy poses a privacy threat to the biometric information of the user. Further, the storage and retention of information are also exposed to privacy threats, due to the inadequacy of the security measures present under the scheme.

PRIVACY POLICY

DATA COLLECTED

Aadhaar No., OTP, Fingerprints, Mobile numbers

SPDI

Fingerprints

INFORMATION COLLECTION

Information is voluntarily uploaded by the user or obtained from the appropriate government department on the request of the user

INFORMATION USE

- Used as cloud storage of physical documents
- Used for online verification
- Used by various government departments to issue or verify documents related to citizens digitally
- Used to submit a digitally signed copy to a government agency
- Assist in Aadhaar seeding by the government
- Connecting of databases

INFORMATION DISCLOSURE

Information disclosed to the concerned authority upon request of the user for verification of documents.

INFORMATION RETENTION

Information stored through cloud services

INFORMATION STORED

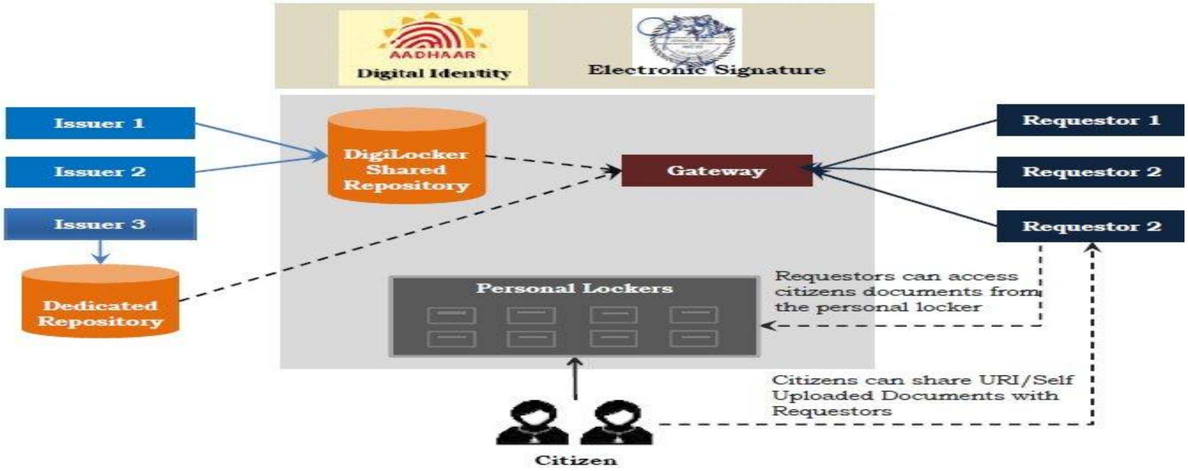
Personal documents like University certificates, Permanent account number (PAN) cards, voter id cards, etc. (depending on what the user seeks to upload online)

SECURITY MEASURES

Use of unique Aadhaar no. to enhance security

INVOLVEMENT OF PRIVATE COMPANIES

DIGILOCKER PRIVACY GAPS


AADHAAR
Digital Identity
Electronic Signature
Issuer 1
Issuer 2
Issuer 3
DigiLocker Shared Repository
Dedicated Repository
Gateway
Requestor 1
Requestor 2
Requestor 2
Personal Lockers
Requestors can access citizens documents from the personal locker
Citizens can share URI/Self Uploaded Documents with Requestors
Citizen

DIGILOCKER ECOSYSTEM

V. DIGILOCKER ECOSYSTEM ARCHITECTURE COMPONENTS

a. Electronic Document or E-Document – A digitally signed electronic document in XML format issued to one or more individuals (Aadhaar holders) in appropriate format compliant to DLTS specifications. Examples:

- ✓ Degree certificate issued to a student by a university.
- ✓ Cast certificate issued to an individual by a state government department.

✓ Marriage certificate issued to two individuals by a state government department.

b. Digital Repository – A software application complying with DLTS specifications, hosting a collection (database) of e-documents and exposing a standard API for secure real-time access. While architecture does not restrict the number of repository providers, it is recommended that few highly available and resilient repositories be setup and encourage everyone to use that instead of having lots of repositories.

c. Digital Locker- A dedicated storage space assigned to each resident, to store authenticated documents. The digital locker would be accessible via web portal or mobile application.

d. Issuer – An entity/organization/department issuing e-documents to individuals in DLTS compliant format and making them electronically available within a repository of their choice.

e. Requester – An entity/organization/department requesting secure access to a particular e-document stored within a repository. Examples:

✓ A university wanting to access 10th standard certificate for admissions

✓ A government department wanting to access BPL certificate

✓ Passport department wanting to access marriage certificate

f. Access Gateway – A software application complying with DLTS specifications providing an online mechanism for requesters to access an e-document in a uniform way from various repositories in real-time. Gateway services can be offered by repository providers themselves. While architecture does not restrict the number of repository providers, it is suggested that few resilient and highly available central gateway systems be setup and requesters can signup with any one of the gateways for accessing documents in the Digital repositories.

g. Document URI – A unique document URI mandatory for every document. This unique Digital Locker Technology Specification (DLTS) – Version 2.3 URI can be resolved to a full URL to access the actual document in appropriate repository. Document URI is a persistent, location independent, repository independent, issuer independent representation of the ID of the document. The existence of such a URI does not imply availability of the identified resource, but such URIs are required to remain globally unique and persistent, even when the resource ceases to exist or becomes unavailable. While document URI itself is not a secret, access to the actual document is secure and authenticated.

V. PRIVACY PROTECTION SAFETY MEASURES

a. 256-bit SSL encryption - DigiLocker uses a 256-bit key to encrypt and decrypt data or files. This encryption is one of the most protected methods of encryption after 128 and 192-bit encryption. Today, this encryption is most popular in encryption algorithms, protocols and technologies such as AES and SSL.

b. Automatic log out - This feature is incorporated to ensure the safety of the credentials of the user. In the event you forget to log out, logout happens automatically from the account when the browser window is closed.

c. Mobile authentication - To sign up or register with DigiLocker, the user needs to have a valid Aadhaar number. When you sign up using Aadhaar number, you'll be given authentication with an OTP (one time password) to be sent to the mobile number and email id registered with Aadhaar. Once you enter the OTP in the field, you are done. Users can log in to DigiLocker using Aadhaar number with OTP, or user Id and password. However, some people opine that the authentication should be made mandatory whenever there is login by the user to enhance security. This is so in case of logging in to email counts such as Gmail, outlook, and so on. This is because if the username and passwords are compromised, unauthorized access may occur.

d. ISO 27001 - ISO 27001 is a set of standards for information security management system (ISMS). An ISMS is a framework comprising policies and procedures including legal, physical and technical controls associated in the information risk management process of a business or an organization.

VI. CONCLUSION

International Organization for Standardization (ISO), as a new component of the ISO 27001 standard. ISO 27018 sets forth a code of practice for protection of PII in public clouds acting as PII processors. Cloud service providers (CSPs) adopting ISO/IEC 27018 must operate under five key principles:

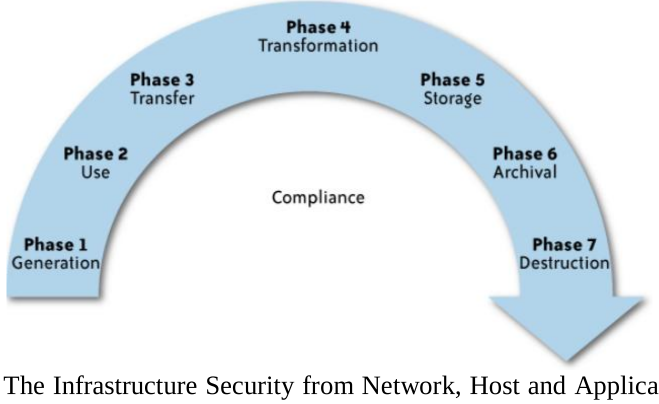
a. Consent: CSPs must not use the personal data they receive for advertising and marketing unless expressly instructed to do so by the customer. Moreover, it must be possible for a customer to use the service without submitting to such use of its personal data for advertising or marketing.

b. Control: Customers have explicit control of how their information is used.

c. Transparency: CSPs must inform customers where their data resides, disclose the use of subcontractors to process PII and make clear commitments about how that data is handled.

d. Communication: In case of a breach, CSPs should notify customers, and keep clear records about the incident and the response to it.

e. Independent and yearly audit: A successful third-party audit of a CSP's compliance documents the service's conformance with the standard, and can then be relied upon by the customer to support their own regulatory obligations. To remain compliant, the CSP must subject itself to yearly third-party reviews.



The Infrastructure Security from Network, Host and Application level has been secured effectively, however the data security and storage needs to the addressed from a data life cycle perspective. When data is in transit confidentiality and integrity is achieved using secure protocol, when the data is at rest encryption is essential as it is not associated with the application. Are the data saved on the server storage encrypted or not? If it is encrypted, Where is the encryption made? Is it made in the client side or the server side? Is if possible for the system operator to get the content of users' files? Is file metadata encrypted on the server? Is a system operator able to get file metadata? We care about this because sometimes we want to make sure not only the file content but also file metadata like file names are not accessible to others. Identity and access management (IAM) is important for diverse users. Does the server keep users' account information? Are the passwords of users saved on server? What information the system operator can get from users? System operators often claims that they will not do something, for example, to claim they will not view the files uploaded. But we would like to know whether it is trustable. Or, are the system operators have the ability to get sensitive information? Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data (or Personally Identifiable Information - PII). Real time security and compliance monitoring is essential.

VII. REFERENCES:

[1]. Mather Tim, Kumaraswamy Subra and Latif Shahed (2009) . Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliances

[2]. Singh Bharati Jyotsana and Garg Arpit, "How useful is digital locker? An empirical study in Indian context" Indian Journal of Commerce and Management Studies., Volume VII Issue 2(1), May 2016

[3]. Porey D Jayant, "Digital locker system in India" International Journal of Commere and Management Research., Volume2; Issue 12;; Page No.80-81 December 2016

[4]. [Online] : https://digitallocker.gov.in/

[5]. [Online]: http://deity.gov .in/sites/upload_ files/dit/files/Digital%20India.pdf

[6]. DigiLocker - Wikipedia, the free encyclopedia.htm

[7]. [Online]: https://blog.mygov.in/en/

[8]. [Online]: https://cis-india.org/internet-governance/f iles/digital-ind ia-report.pdf

[9]. Technical Specifications DLTS Version 2.3 document.