IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 67-71
www.iosrjournals.org

Secure Storing and Sharing of Documents on Cloud

Pavan Ughade[1] Nikita Kapsi[2] Asha Mallappagol[3] and Apoorva Tangod[4]

[1]Computer Science and Engineering, Assistant Professor, Jain College of Engineering, VisvesvarayaTechnological University, Belgaum, India
[2, 3,4]Computer Science and Engineering, Students, Jain College of Engineering, Visvesvaraya Technological University, Belgaum, India
nikitakapsi@gmail.com, ashamallappagol@gmail.com, sunita.tangod@gmail.com

Abstract: *Nowadays most of the citizens of India have their identity and personal documents starting from date of birth certificate, educational certificate, Voter ID, Ration Card, Driving License, vehicles registration number, PAN Card, Passport, Electricity bills, bank account numbers, insurance etc. While searching for jobs, it's mandatory to carry important documents, but this involves risk. There are chances that these documents may be lost, stolen or even sometimes people may forget to carry necessary documents. 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.*

Keywords: *Digitization, Encryption, cloud storage, Rijndael encryption*

I. Introduction

Cloud computing is an emerging technology based on a pay per-use model that is able to provide high availability and accessibility to remote IT resources to customers who cannot afford to maintain their own infrastructure [1]. The outsourcing of IT functions to cloud providers has become the solution for organizations to cut costs in the acquisition and maintenance of IT infrastructure, to boost their productivity and to accelerate building online collaborative workspaces [2][3].

Nevertheless, security and privacy violations could arise when outsourcing data to a third party. This storage model puts organizations at risks of unauthorized users read, modify or analyze documents stored in the cloud storage infrastructure without they can either avoid or notice such privacy and security violations. Moreover, there is a potential lack of control and transparency when a third party holds private documents; as a result, there exist scenarios in which an organization cannot trust sensitive information to a cloud service provider.

Simple encryption techniques have becoming a solution to avoid privacy and security issues but it imposes a set of constraints on file sharing workflows. In file sharing procedures, the cloud storage performs decryption tasks for delivering the files to the users included in the sharing workflows, which may not be allowable by organizations when the users are sharing sensitive files[2]. Similar tasks are invoked when members of collaborative workspaces search for information inside files. There exists a need for enabling secure documents exchange through cloud services promoting collaboration workflows. In addition, such schemes would have to preserve data integrity[8].

II. Literature Review

Earlier government issued official document in the form of hard copy. This lead to wastage of paper which in turn causes deforestation. One had to carry all the documents physically wherever he/she goes. There is always a risk of losing documents.

Later Google came up with google drive concept which allowed to store and share any type of documents online but it had following limitations:

1. Hackers hack or remove your important data

One of the disadvantages that I think might happen will be the hackers who hack or remove your important data, or they install virus into your server and your files are gone. You may have some confidential file such as financial statement or cash flow which you need to share between you and your partner, these files might be dangerous if 3rd party can hack and view it too.

2. Impossible to add a password to files

With Google Drive**,** because there’s no way to put a password on individual files or folders, when you share something, that person can access that file or folder whenever they want. Moreover, it is a fact that Google has access to our data. In many cases, personal information of the users are analyzed then sold to advertisers.

3. No Encryption mechanism

Documents stored on drive are not in encrypted format hence cannot trust and are not safe.

Recently government of India has launched Digital Locker which provides the citizens of India to store personal as well as educational documents online and share by e-signature[6].

The drawbacks of this system are:

- The problem is: the trust that the data will not be breached by government or anyone else. Earlier we have seen that government had breached data.
- E-signing is not reliable for authenticity.

III. Inference From Literature Review

From the above literature survey considering the drawbacks of cloud storage on the factors of trust, reliability, and security we have opted a solution where in user will be having the control over generation of decryption keys and upon sharing them the documents can be decrypted. The RijnDael (pronounced Reign Dahl) algorithm was adopted in October 2000 as the Advanced Encryption System (AES) by the American National Institute of Standards and Technology (NIST)[8]. This algorithm is a successor to what is currently used - the Data Encryption Standard (DES) which has proved to be crack-able, given enough computing resources.

IV. Methodology

A. Rijndael Algorithm

Although the number of rounds of Rijndael is fixed in the specification, it can be modified as a parameter in case of security problems. Rijndael is expected, for all key and block lengths defined, to behave as good as can be expected from a block cipher with the given block and key lengths.

The Rijndael algorithm is a new generation symmetric block cipher that supports key sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks - however, in excess of AES design criteria, the block sizes can mirror those of the keys. Rijndael uses a variable number of rounds, depending on key/block sizes, as shown in table.

Rounds	Key size(bits)
9	128
11	192
13	256

Table (i): Iterations based on Key size

Overall, the structure of Rijndael displays a high degree of modular design, which should make modification to counter any attack developed in the future much simpler than with past algorithm designs.

B. Working Of Private Key Sharing

Private access keys are generated through PAK-M for each *user* (U) whom the *owner user* (OU) wants to share information. A PAK (*abePrivK*) is created based on a set of well-defined *attributes* of the owner user (OU); a PAK sets a relation of kind *OU->U* in which, user U could not be able to decrypt documents from OU if U doesn’t have PAK from OU. In order to create a PAK, OU uses the certain attribute list (*AU*) and his public keys performing

PrivKU=*KeyGenMethod*(*AttrOU, PubKOU*).

Finally, the owner uploads the session based PAK to the cloud storage in order that U may retrieve it, and use it to decrypt ensured documents by OU[4]. The aforementioned process is performed through the workflow shown in Figure.

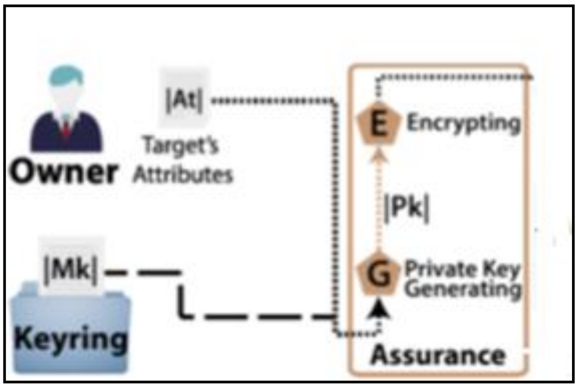


Fig (i): Key Generating mechanism[4]

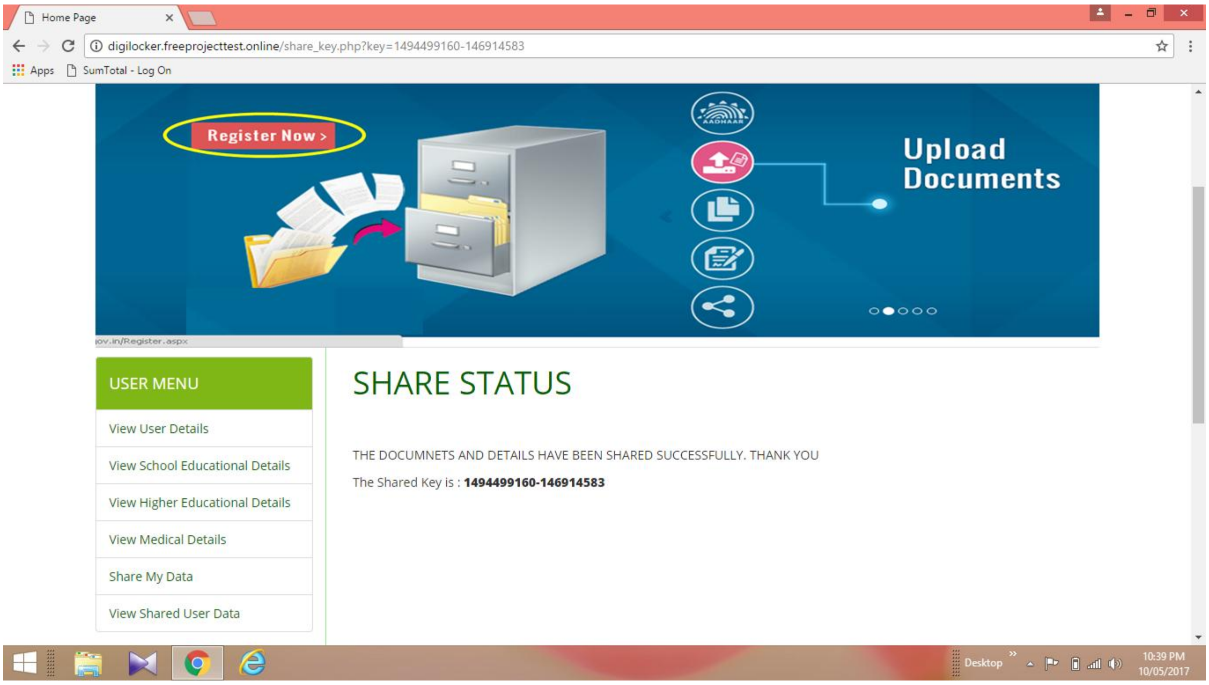
C. Key Sharing And Data Access

The session based key generated by the owner is shared with the requestor through email. The key can be used to view the documents only once by the requestor. If he tries to view the document again using the same key an error is prompted. The owner needs to send a new key.

Advantages

- **Anytime Anywhere Access:** You can access your documents anytime anywhere. No need to carry your documents. Therefore, DigiLocker brings convenience factor[6].
- **Reliability**
- **Securely share and view documents**

V. Results

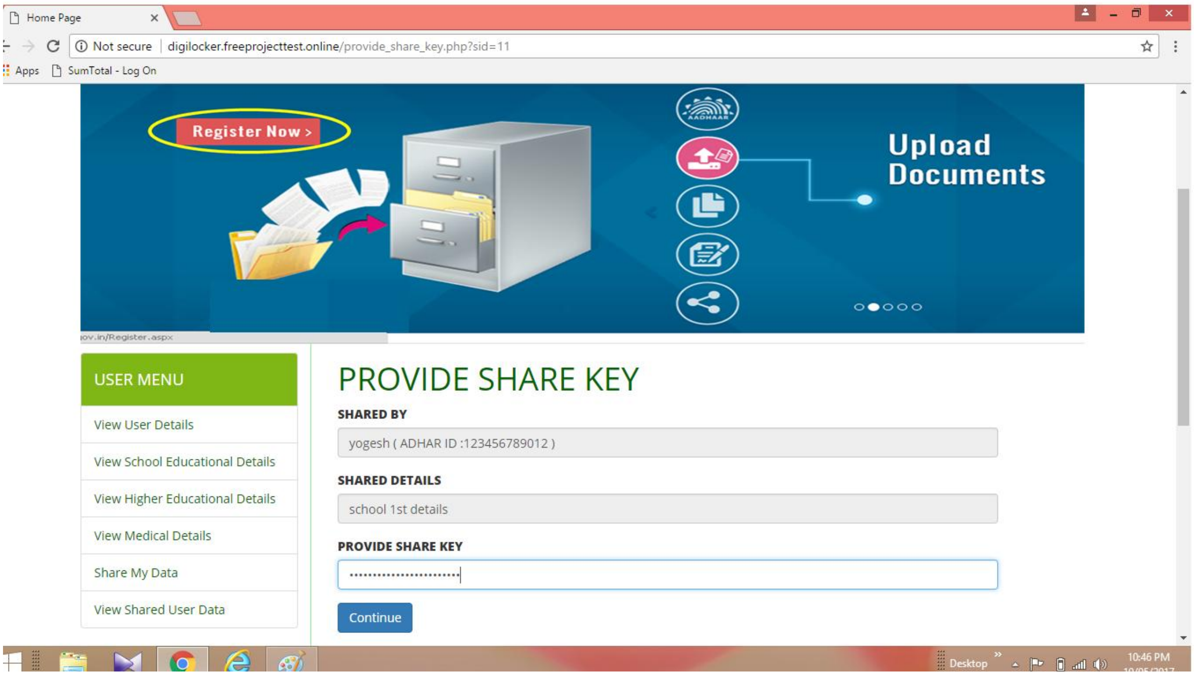


SHARE STATUS

THE DOCUMNETS AND DETAILS HAVE BEEN SHARED SUCCESSFULLY. THANK YOU

The Shared Key is : **1494499160-146914583**

Screenshot (i): Key Generation While Sharing Documents



PROVIDE SHARE KEY

SHARED BY

yogesh (ADHAR ID :123456789012)

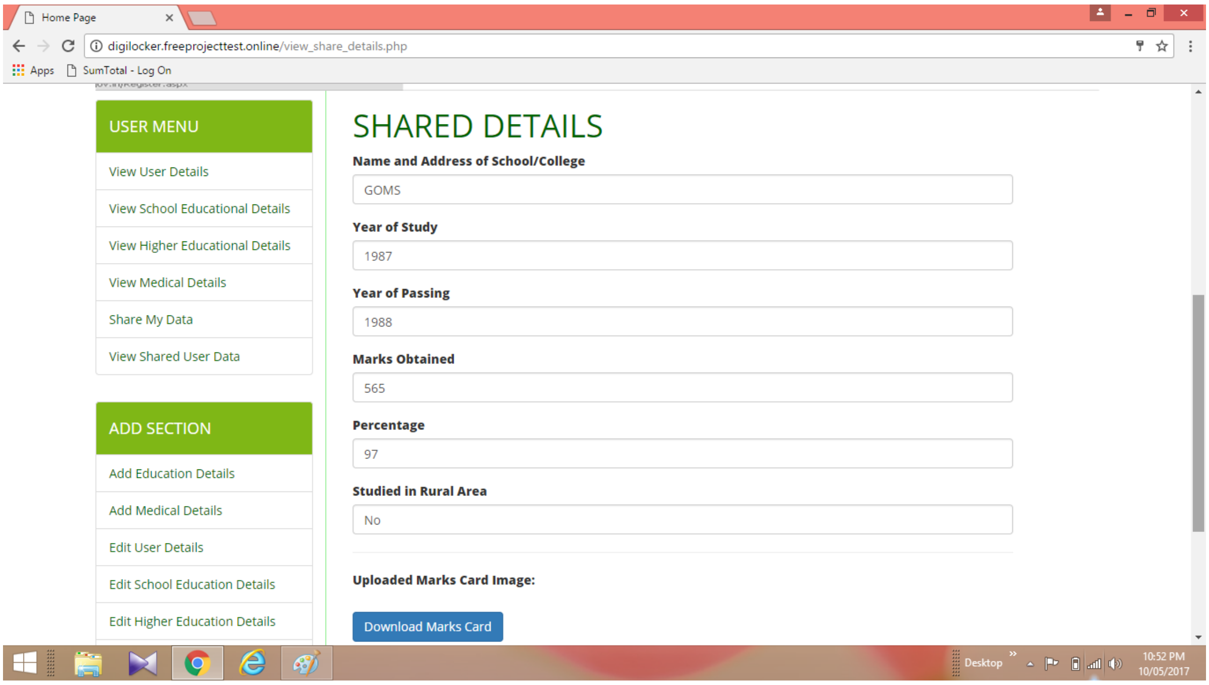
SHARED DETAILS

school 1st details

PROVIDE SHARE KEY

•••••••••••••••••••••••••

Screenshot (ii): Requester must enter the session based key shared for viewing



SHARED DETAILS

Name and Address of School/College

GOMS

Year of Study

1987

Year of Passing

1988

Marks Obtained

565

Percentage

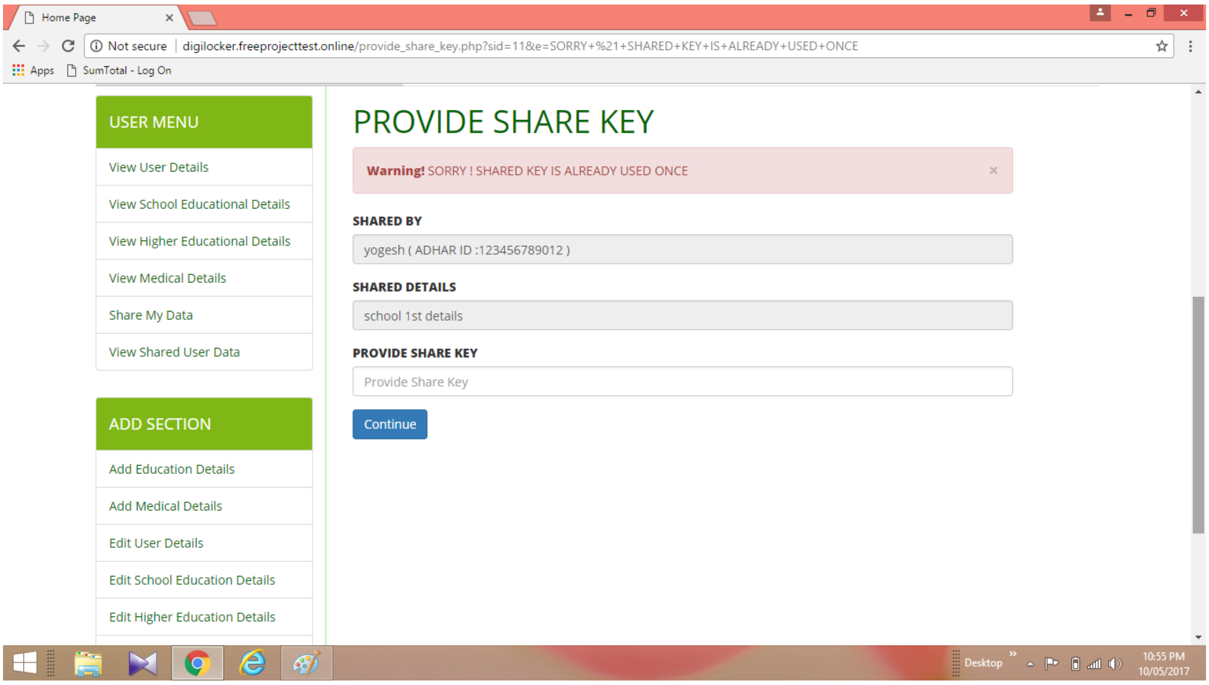
97

Studied in Rural Area

No

Uploaded Marks Card Image:

Screenshot (iii): Displaying Details after entering session key



Not secure | digilocker.freeprojecttest.online/provide_share_key.php?sid=11&e=SORRY+%21+SHARED+KEY+IS+ALREADY+USED+ONCE

PROVIDE SHARE KEY

Warning! SORRY ! SHARED KEY IS ALREADY USED ONCE

SHARED BY: yogesh (ADHAR ID :123456789012)

SHARED DETAILS: school 1st details

PROVIDE SHARE KEY: Provide Share Key

Screenshot (iv): Displaying error message if key is reused

VI. Conclusion

It plays an important role in making all the information digitally and provides a fruitful environment to use the services very efficiently to the citizens of India. Citizen/users are relief from carrying or keeping risky information. Finally this project used in N number of situation where it plays a vital role. Where citizen goes his/her information will be with him/her.

References

[1]. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, Jan. 2014.

[2]. P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” 2011.

[3]. Amazon, “Amazon AWS.” [Online]. Available: http://aws.amazon.com/. [Accessed: 01-Jan-2015]

[4]. A Digital Envelope Scheme for Document Sharing in a Private Cloud Storage, Jedidiah Yanez-Sierra, Arturo Diaz-Perez, Victor Sosa-Sosa, J. L. Gonzalez CINVESTAV Tamaulipas – Mexico. {jyanez,adiaz,vjsosa,jgonzalez}@tamps.cinvestav.mx

[5]. DigiLocker. (2016). Digilocker.gov.in. Retrieved 4 April 2016, from https://digilocker.gov.in/www.mygov.co.in

[6]. DigiLocker for Commuters Assistant Prof. Ms. Mythili Dept of Computer Science and Engineering, V.S.B. Engineering College, Karur

[7]. Data Security and Privacy Protection Issues in Cloud Computing, 2012 International Conference on Computer Science and Electronics Engineering

[8]. Komal D Patel, Sonal Belani, Image Encryption Using Different Technique: A Review