International Journal of Research in Advent Technology, Vol.7, No.5S, May 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

The Double Authentication Security In OTP Accountability Data Sharing In The Cloud Storage Using Android Web

M.Selvakumar[1], B.Vinoth Kumar[2]
[1, 2] *Assistant Professor, Department of Computer Applications,*
Ayya Nadar Janaki Ammal College(Autonomous), Sivakasi, Viruthunagar District, Tamil Nadu.
mselvakumarmca@gmail.com, Mobile Number – 82 20 20 62 00

Abstract :This paper based on online cloud storage for making double authentication screen. In this paper everything based on online android web browser for double authentication privilege in AWS. This paper contains numbers of screens. They are Owners privilege, Users, CIA Privilege and CSP (Cloud Service Provider) Privilege. This paper major objective is to analysis about cloud security for double authentication OTP Screen Windows. Every privilege having authentication for more security in cloud storage. Numbers of owners, Numbers of Users and Only one CSP, CIA Privilege. If we implemented this paper no one misuse techno internal data through to these mobile apps. This paper implemented CIA Framework technology for OTP verification code and raised request code for file upload or download. In this paper have two OTP Code. One for request code one more for File Upload. This paper give more confidently secrete data from cloud to maintain lifelong more securities.

1. INTRODUCTION

It's the development of cloud storage based on CIA APPS (Cloud Information Accountability) under Owners permission for cloud login. This system user have double authentication for security in online brisk technologies servers. We have number of owner and each and every owner create their personal accounts do to login screen. Owner login for first authentication with that get more sub menus following (View Users, file upload, send request to CIA, View OTP code, reload Cost ECT.). After that raised a request to CIA and login CIA Screen and see request and granted their request.

To store more data based on cloud space under AWS (Brisk techno server domain). We are going to use online production server to maintain double authentication belongs to double login and check whether their permission granted or not, If granted their given permission to file upload or file download to Owners and Users.

2. SYSTEM DESIGN

System design concentrates on moving from problem domain to solution domain. This important phase is composed of several steps. It provides the understanding and procedural details necessary for implementing the system recommended in the feasibility study. Emphasis is on translating the performance requirements into design specification. The design of any software involves mapping of the software requirements into functional modules. The developing a real time application or any system utilities involves two processes. The first process is to design the system to implement it. The second is to construct the executable code. Software design has evolved from an intuitive art dependent on experience to a science, which provides systematic techniques for the software definition. The software design is a first step in the development phase of the software life cycle. Before system design the user requirements have been identified, information has been gathered to verify the problem and evaluate the existing system.

3. IMPLEMENTATION AND RESULTS

System implementation is the stage in this mini project where the theoretical design is turned into a working system. The implementation phase constructs, installs and operates the new system. The most crucial stage in achieving a new successful system is that it will work efficiently and effectively.

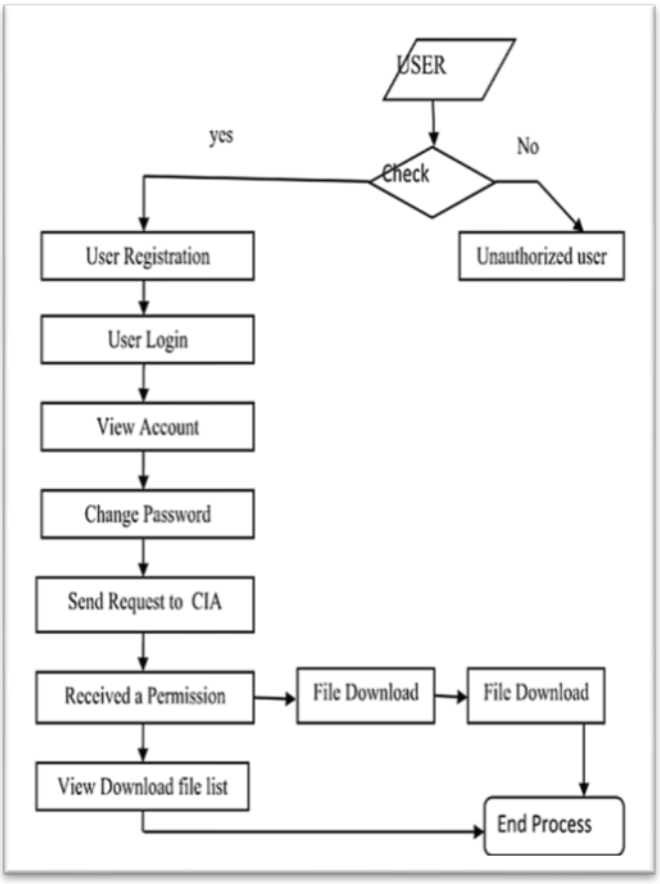

Fig 3.1 User flow control

3.1 Owner

It's the development of cloud storage based on CIA APPS (Cloud Information Accountability) under Owners permission for cloud login. This project we have double authentication for security in online brisk technologies servers. We have number of owner and each and every owner create their personal accounts do to login screen. Owner login for first authentication with that get more sub menus following (View Users, file upload, send request to CIA, View OTP code, Reload Cost ECT.). After that raised a request to CIA and Login CIA Screen and see request and granted their request.

3.1.1 Owner sub module

In this module user can develop any kind of cloud computing android apps based on these privilege authentication windows. In these apps belongs to brisk technologies purpose not for others. After login will get main menu from the android apps.

- View Users Details.
- File Upload.
- CIA Request.
- CIA Request OTP.
- File Reload.
- Logout

1. View Users Details

To view all users information for their personal cloud access data from the brisk techno cloud.

2. File Upload

To upload file from the brisk techno server into android AWS cloud location before that raised the request for privilege from the CIA Request.

3. CIA Request

This is getting grant privilege from the AWS server for make double authentication or double login windows.

4. CIA OTP

After grant privilege from the CIA screen, we will get OTP numbers from the AWS Brisk techno Server.

5. File Reload

In case any virus occur from the AWS server, Our file will be spoiled that ways , user are doing ones again upload the same file and same location.

6. Logout

After that all action from the brisk techno, the system can terminate our brisk techno server from the AWS Cloud.

3.2 User

It's the development of cloud storage based on CIA APPS (Cloud Information Accountability) under Users permission for cloud login. This project we have double authentication for security in online brisk technologies servers. We have number of Users and each and every owner create their personal accounts do to login screen. Users login for first authentication with that get more sub menus following (View Users, file download, send request to CIA, View OTP code, Download Cost ECT.). After that raised a request to CIA and login CIA Screen and see request and granted their request.

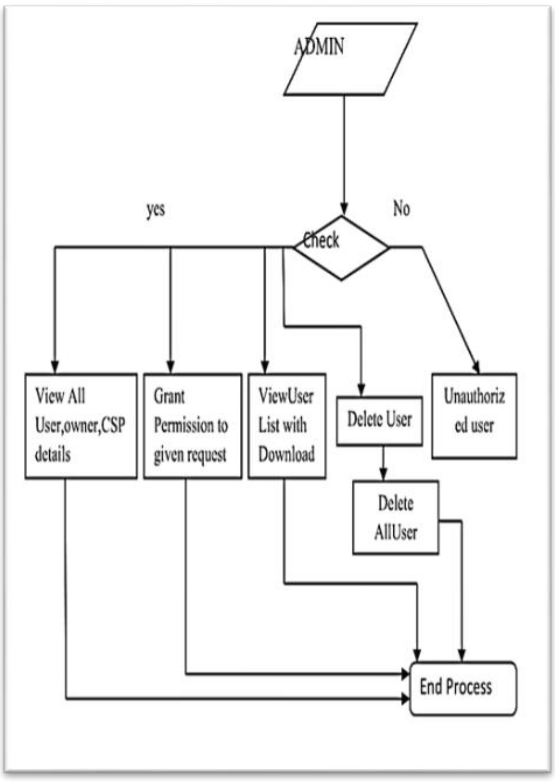

Fig 3.2 Admin flow control

3.2.1 User sub module

In this module user can develop any kind of cloud computing android apps based on these privilege authentication windows. In these apps belongs to brisk technologies purpose not for others. After login will get main menu from the android apps.

- View Owners Details.
- File Download.
- CIA Request.
- CIA Request OTP.
- File Download.
- Logout

1. View Users Details

To view all users information for their personal cloud access data from the brisk techno cloud.

2. File Upload

To download file from the brisk techno server into android AWS cloud location before that raised the request for privilege from the CIA Request.

3. CIA Request

This is getting grant privilege from the AWS server for make double authentication or double login windows.

4. CIA OTP

After grant privilege from the CIA screen, we will get OTP numbers from the AWS Brisk techno Server.

5. File download

In case any virus occurs from the AWS server, Our file will be spoiled that ways, we are doing ones again Download the same file and same location.

6. Logout

After that all action from the brisk techno, we can terminate our brisk techno server from the AWS Cloud.

3.3 Cloud Storage

To store more data based on cloud space under AWS (Brisk techno server domain). We are going to use online production server to maintain double authentication belongs to double login and check whether their permission granted or not, If granted their given permission to file upload or file download to Owners and Users

We have three major brisk technologies Cloud server mode following

1. Brisk Cloud (Implemented).
2. AWS Cloud.
3. Google Cloud.

3.4 CSP

Cloud Service Provider (CSP) based on CIA Mobile Apps; this is mediator between Owners to Users and Users to Owners based on cloud storage.

3.4.1 CSP sub module

CSP is a third party auditing for monitor all cloud storage file, whether safe or not, because of double authentication windows belongs to our brisk techno server. Following

- View Owner Details.
- View Users Details.
- View File Upload Details
- Logout.

1. View Owner Details

To record "how many owner registered with brisk techno" for set more privilege in our documents or images.

2. View Users Details

To view numbers of users registered with brisk techno server

3. View File Upload Details

To view all documents for date and time (uploading date and time)

4. Logout

Close the CIA Android Apps Screen.

4. CONCLUSION

In this paper proposed innovative approaches for automatically logging any access to the data in the cloud together with an auditing mechanism. This paper approach allows the data owner to not only audit his content but also enforce strong back-end protection if needed. Moreover, one of the main features of our work is that it enables the data owner to audit even those copies of its data that were made without his knowledge.

REFERENCES

[1] P. Ammann and S. Jajodia, "Distributed Timestamp Generation in Planar Lattice Networks," ACM Trans. Computer Systems, vol. 11, pp. 205-225, Aug. 1993.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. ACM Conf. Computer and Comm. Security, pp. 598- 609, 2007.

[3] E. Barka and A. Lakas, "Integrating Usage Control with SIP-Based Communications," J. Computer Systems, Networks, and Comm., vol. 2008, pp. 1-8, 2008.

[4] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology, pp. 213-229, 2001.

[5] A. M. H. Al-Saffar, "Identity Based Approach for Cloud Data Integrity in Multi-Cloud Environment," Ijarcce, vol. 4, no. 8, pp. 505–509, 2015.

[6] A. . Juels and B. S. . Kaliski Jr., "Pors: Proofs of retrievability for large files," Proc. ACM Conf. Comput. Commun. Secur., pp. 584–597, 2007.

[7] C. S. Pawar, P. R. Patil, and S. V. Chaudhari, "Providing security and integrity for data stored in cloud storage," 2014 Int. Conf. Inf. Commun. Embed. Syst. ICICES 2014, no. 978, 2015.

[8] Y. Gunjal, P. J. Rethna, and V. Jeny, "Data Security And Integrity Of Cloud Storage In Cloud Computing," vol. 2, no. 4, pp. 1166–1170, 2013.

[9] http://bigdata-madesimple.com/5-advantages-and-disadvantages-of-cloudstorage (last accessed on: Aug. 2015)

[10] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, "Security Issues for Cloud Computing." pp. 1–14, 2010.

[11] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Proc. 16th ACM Conf. Comput. Commun. Secur. - CCS '09, vol. 489, p. 187, 2009.
[12] A. M. H. Al-Saffar, "Identity Based Approach for Cloud Data Integrity in Multi-Cloud Environment," Ijarcce, vol. 4, no. 8, pp. 505–509, 2015.