July – August 2020
ISSN: 0193-4120 Page No. 650 - 653

Software Schema of Novel Graphical Authentication and Role Based Security

Ashish Bhardwaj Dr. Surendra Yadav
Career Point University, National Highway 12, Alaniya, Rajasthan 325003.
+91-8586927995 and bhardwajashish739@gmail.com

Article Info
Volume 83
Page Number: 650 - 653
Publication Issue:
July - August 2020

Article History
Article Received*: 06 June 2020*
Revised*: 29 June 2020*
Accepted*: 14 July 2020*
Publication*: 25 July 2020*

Abstract

In the modern IT data sharing environment, it is desired that every cloud-based organization should be perfect in its security measures. Proper authentication and validation of the data access are the primary requirement for the success of any cloud-based organization. This paper focuses over the practical implementation of the approach proposed for the secure file share in a cloud environment and the simulation of the approach is shown in Visual Studio 2010 and the database used for the simulation process is SQL Server 2008. The paper is developed to practically show the approach designed for the TPA based interaction. To start with the simulation of the data access, first valid users of the organization with simulated to be registered with the process designed for that. Then the authorized users can share data on the cloud server and an authorized user can request to get access to that data. Than The TPA come to roles and here, a checklist is maintained for the users who can access the data requested and together with that will design another way of validating the user request for access that is by the token or transaction id for that access as well as validating the OTP for the access of that file. Then chunks of the data are received by the user and decrypted with another key which is required for the decryption of the chunks and then the chucks are again combined to a single file and used by the user who had requested for its access.

Keywords: *Secure File Share, SHA, TPA Monitorin*

I. Introduction

In the previous paper of our work, titled “Novel Approach for TPA based Data Sharing using Hashing Algorithms “, They explained about the concepts of cloud based secure data sharing approach involving the TPA[1]. The algorithms is proposed in this paper explain the concept of the secure sharing involving TPA, clustering of the data shared and together with that, they involve Hash code pattern for the validation and verification purpose. In this paper only focusing on the implementation of the simulation on the basis of the algorithm proposed.

In this paper, the technology used for the simulation of the proposed work is Visual Studio 2010. It supports creating of the GUI with ease and quickly, and graphically we can represent our concept in the better way. And the simple interaction based features of the SQL Server Express Edition 2008 motivates us to use this database as the primary database in the simulation work. The working of the simulation is described in the two main sections, User Section and TPA module simulation. User Section involves user management modules and TPA[2] modules involves monitoring and facilitating the access to the authorized user.

II. Simulation Explanation

Fig. 1. Main Screen

The fig 1 shows MDI form which contains menus related to the options which are present in the simulation work. First, we are covering the User Section. It deals with all the users with tendency to access the file on the server.

July – August 2020
ISSN: 0193-4120 Page No. 650 - 653

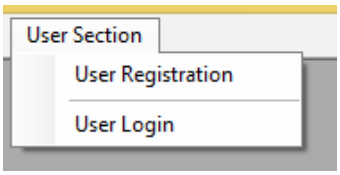

Fig. 2. User Section Menu

The fig 2 shows sub-menu options of the user section which are related to the user management, user registration and user login. [3]

Fig. 3. User Registration

User registration involves details like user name, email id and other credentials which will be later stored in the database after verification of the details in the database. The second phase is the user login, where a user enters credentials to validate himself/herself and then gets an access to the main system. User login form is shown in Fig 4.

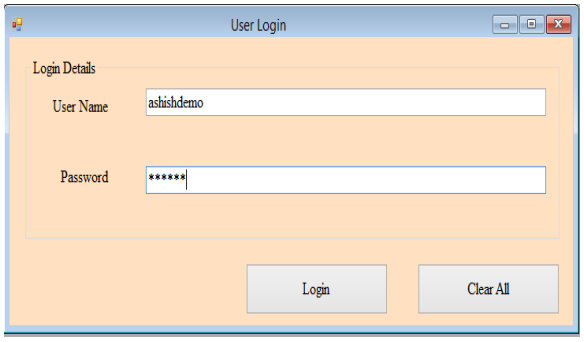

Fig. 4. User Login

Once the details are validated, main screen of the user section will get displayed as shown in the fig 5.

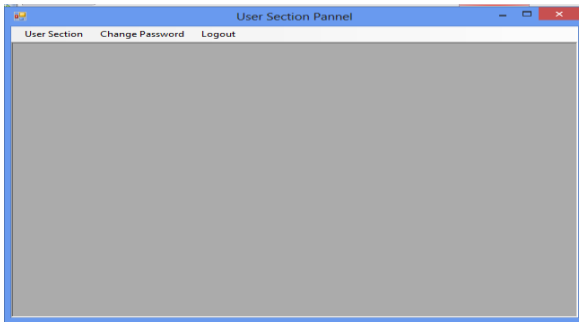

Fig. 5. User Section Panel

In the user section, options deal with file uploading and requesting for file access from the TPA.[4] In order to simulate the working of the proposed algorithm, one user first uploads the file and then another user requests access to the file. For the simulation purpose the current user, “ashishdemo” will upload the file. And the process of the upload is shown in the fig 6.

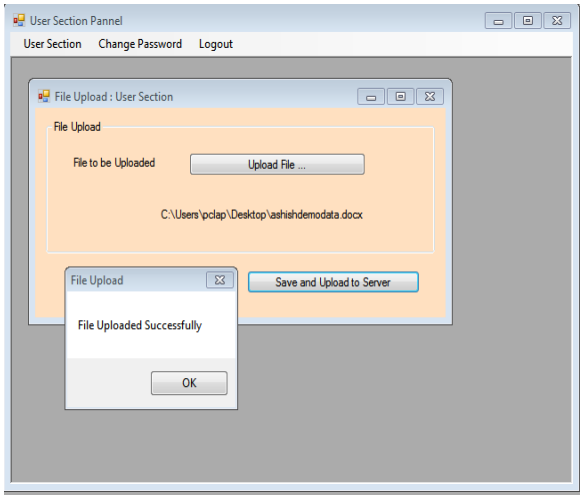

Fig. 6. File Upload Form

After the details got stored in the database, we will logout as the current user and we will login as another user “ashishdemo2”.

The user “ashishdemo2” will require an access to the file “ashishdemodata.docx” which is uploaded by the user “ashishdemo”. And the process of the request to TPA is shown in the fig 7.

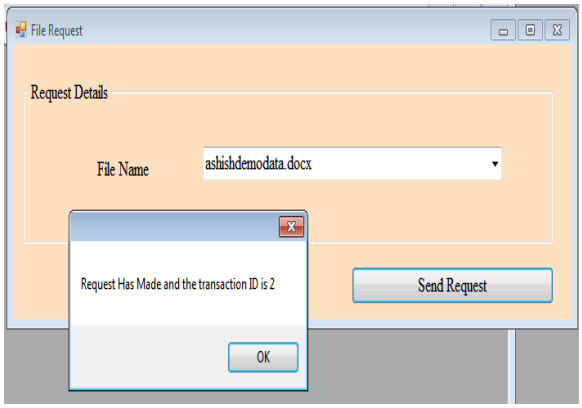

Fig. 7. File Request Form

The unique request is identified by the transaction ID which is generated on auto-increment basis.

Fig. 8. TPA Login

TEST Engineering & Management

July – August 2020
ISSN: 0193-4120 Page No. 650 - 653

Now the TPA login process is simulated and the TPA [5] gets a menu option to see the requests for access.

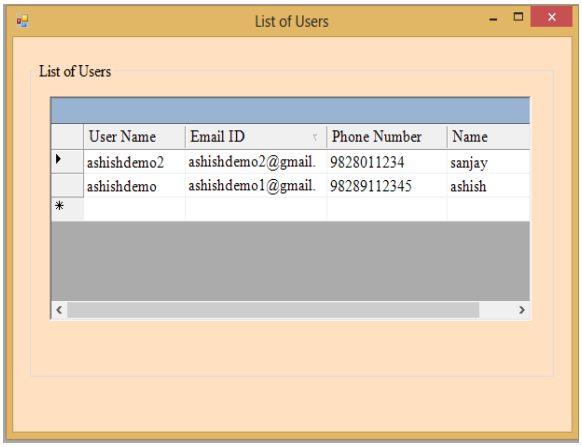

Fig. 9. List of Users Requested

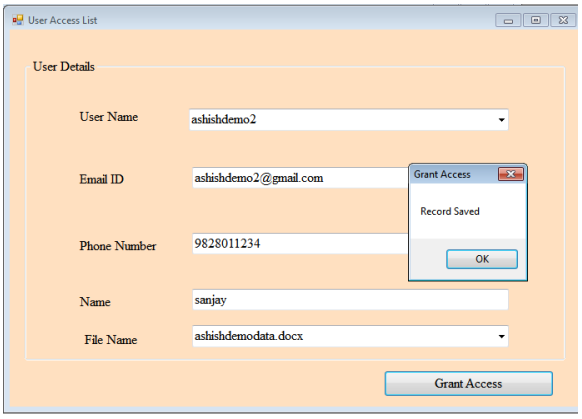

Fig. 10. Access Granting Form

Then, the grant access form of TPA will be used for granting access to the file. In the grant access form, the request ID is checked which is the transaction ID and the eligibility is checked in the database and after all validations, an OTP is sent. [6]

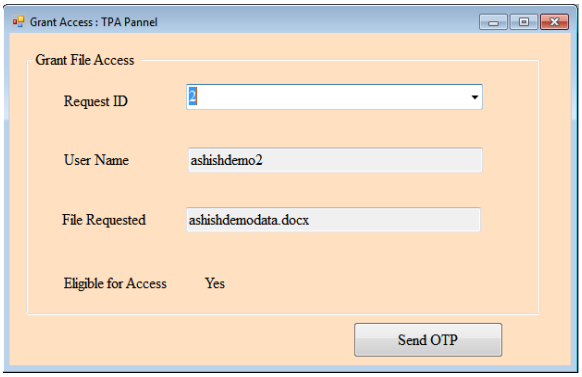

Fig. 11. User Validation Form

When the TPA clicks on the Send OTP button, an OTP is generated and the process of generation for OTP is as follows:

The generated OTP will have six random digits and 3 digits extracted from User id. Thus, the general format of the OTP will look like,

R1R2R3R4R5R6X1X2X3

Where,

R1,R2,R3,R4,R5,R6 are random numbers that can take any value in the range of 0 to 9.

X1X2X3 are the first three digits extracted from the user id of the user requesting for the cloud service. This database table will store the request id in order to correlate with the file for which splitting is done and the ekey will store the details of the encryption key used for encrypting the parts and fparts will store the details of the number of parts into which the file is split.

The fig 12 the file parts of the split file and the encrypted parts of the split file and the concept followed for sharing the encrypted parts is the same mentioned in the proposed work. The Clusters are then segmented into the groups on the basis of the size of the elements in the groups. Then a random password is generated and used as the key for encryption with the AES algorithm. Then, Hash is generated for the original file using the MD5 algorithm.

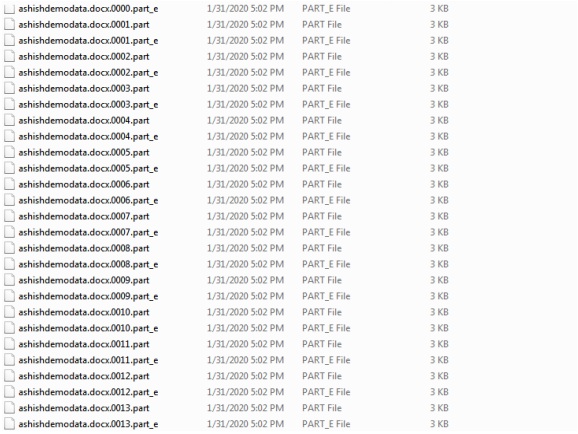

Fig. 12. File Parts Normal and Encrypted

And in order to decrypt the file, user “ashishdemo2” will login. For the decryption, the request ID and OTP are to be entered. [7]

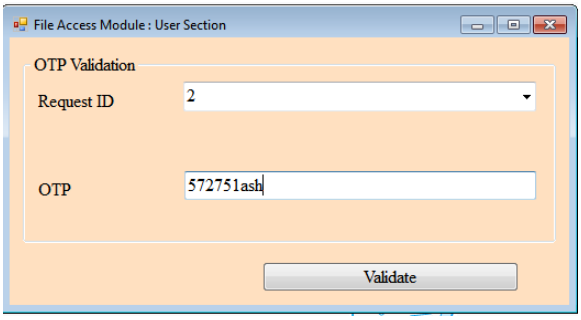

Fig. 13. OTP Validation

After the validation of the request ID and OTP, as fig 14 shows, the file decryption form in which the decryption key is provided appears. And by clicking Decrypt Files option, the file chunks are decrypted and then joined.

As this is simulated on a single machine platform, the chunks part will be simulated by splitting and joining on a single

July – August 2020
ISSN: 0193-4120 Page No. 650 - 653

machine. When implemented in the cloud environment, the real time simulation can be done. (This will be the speculated part)

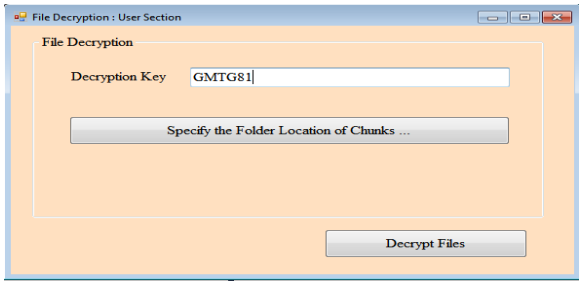

Fig. 14. File Decryption using Encryption Key

III. Conclusion

This paper is rolled around the implementation of the approach which is proposed in the previous paper "Novel Approach for TPA based Data Sharing using Hashing Algorithms" which we have published. The simulation totally describes the overall working of the algorithms and next, we will focus on the result analysis of the proposed work.

References

[1] J S. Hiremath and S. R. Kunte, "Ensuring Cloud Data Security using Public Auditing with Privacy Preserving," in *IEEE 3rd Int. Conf. Comm. Electron. Sys. (ICCES)*, Oct 2018, pp. 1100-1104.

[2] N. Paladi, C. Gehrmann and A. Michalas, "Providing User Security Guarantees in Public Infrastructure Clouds," *in IEEE Trans. Cloud Comp.*, vol. 5, pp. 405-419, 2017.

[3] Bin Feng,Xinzhu Ma,Cheng Guo,Hui Shi, Zhangjie Fu,"An Efficient Protocol With Bidirectional Verification For Storage Security In Cloud Computing", *in IEEE Acc.*, vol. 4, pp. 7899-7911, 2016.

[4] O. Heinisuo, V. Lenarduzzi and D. Taibi, "Asterism: Decentralized File Sharing Application for Mobile Devices," *IEEE Int. Conf. Mob. Cloud Comp. Serv. Eng. (MobileCloud)*, 2019, pp. 38-47.

[5] M. A. Mohammed, Z. H. Salih, N. Ţăpuş and R. A. K. Hasan, "Security and accountability for sharing the data stored in the cloud," *RoEduNet Conf. Net. Educ. Res*.,2016, pp. 1-5.

[6] S. Hiremath and S. Kunte, "A novel data auditing approach to achieve data privacy and data integrity in cloud computing," in *IEEE Int. Conf. Electrical, Electronics, Comm., Comp., Optimizat. Techniq. (ICEECCOT)*, Dec. 2017, pp. 306-310.

[7] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman and D. Woods, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," *in IEEE Trans Cloud Comp.*, vol. 5, issue. 3, pp. 523-536, 2017.

[8] Z. Xia, X. Wang, X. Sun and Q. Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," in IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340-352, 1 Feb. 2016.

[9] B. L. Adokshaja and S. J. Saritha, "Third party public auditing on cloud storage using the cryptographic algorithm," in *IEEE Int. Conf. Energy, Comm., Data Analyt. Soft Comput. (ICECDS)*, Aug. 2017, pp. 3635-3638.

[10] I. El Ghoubach, R. B. Abbou and F. Mrabti, "A secure and efficient remote data auditing scheme for cloud storage," *J. King Saud Uni. Comp. Inf. Sci.*, 2019.

[11] S. H. Abbdal, H. Jin, A. A. Yassin, Z. A. Abduljabbar, M. A. Hussain, Z. A. Hussien and D. Zou, "An Efficient Public Verifiability and Data Integrity Using Multiple TPAs in Cloud Data Storage," in *IEEE 2nd Int. Conf. Big Data Sec. Cloud (BigDataSecurity), IEEE Int. Conf. High Perf. Smart Comput. (HPSC),* and *IEEE Int. Conf. Intellig. Data Sec. (IDS),* April 2016, pp. 412-417.

[12] S. Hiremath and S. R. Kunte, "Ensuring Cloud Data Security using Public Auditing with Privacy Preserving," in *IEEE 3rd Int. Conf. Comm. Electron. Sys. (ICCES),* Oct. 2018, pp. 1100-1104.

[13] S. Patii and N. Rai, "An effectual information probity with two TPAS in cloud storage system," in *IEEE 3rd Int. Conf. Sci. Technol. Engineer. Manage. (ICONSTEM),* March 2017, pp. 432-434.

[14] A. K. Udagatti and N. R. Sunitha, "Fault tolerant public auditing system in cloud environment," in *IEEE 2nd Int. Conf. Appl. Theoret. Comput. Comm. Technol. (iCATccT),* July 2016, pp. 359-362.