ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

ROLE CHECK SECURED USER DATA ACCESS WITH GLOBAL KEY& SECRET KEY USER REVOCATION SYSTEM

[1]C. Deepa, [2]S. Chulochana
[1]Assistant Professor, Faulty of Computing, Sathyabama University, Chennai-600119, Tamil Nadu, India.
[2]PG Student, Department of MCA, Sathyabama University, Chennai-600119, Tamil Nadu, India.
Email:depmca@gmail.com

Received on 14-02-2016 *Accepted on 25-03-2016*

Abstract

ABE (Attribute-based encryption) explains a method for complex progression control over protected data. In existing method the data can store only in cloud through cloud the data can access by user. In this paper Remote Cloud is proposed to store the data. The data owner can able to share key and data to Permitted Users. The data will be share based on three types 1. User Based 2. Role (Position / Role) Based 3. Attribute (Experience). In proposed system based on Global Key, Group Key, Secret Key and Public Key data owner upload the data in cloud. The Public Key being generated randomly. Group Key & Secret Key being generated based on Attribute/ Role like Designation and User Name. Global Key is being randomly generated. Using AES (Advanced Encryption Standard) algorithm the file will encrypt before uploading in to the cloud. The User Revocation also extended in this ingredient. The key will alter when user moved or removed out of group and the new key will mail to Present Members. For further Authentication token is being generated while E Mail apart from all keys will verify during data download.

Key Words: Attribute, Group key, Secret key, Encryption

1. Introduction

Cloud computing is extremely interesting model in which storage and computation shifted away from cloud terminal devices. This popular and new model brings significant revolutions and creates valiant improvements for manner which individuals manage, share, and enterprise and distribute content. The cloud service provider outsources the information technology ability through this cloud service accomplish important cost savings. The cloud computing widely concerns on the data security of cloud user. In university, the colleges upload the development projects in to university cloud before that encrypt the data. Cryptographic technique is necessary in close storage system. For example ABE (Attribute-Based Encryption) is a powerful encryption technique to encrypted information [1]. The

Waters and Sahai introduced ABE. Two different type of ABE system are there KP-ABE (Key-Policy Attribute-Based Encryption) and CP-ABE (Cipher text-Policy Attribute-Based Encryption). Each cipher text associated by access policy and each private key associated by attributes in CP-ABE. Decryption process requires attributes should matches with access policy [2]. For data access control in cloud the ABE is most important and natural technologies. In existing ABE method, efficiency is not sufficient the cipher text efficiency disadvantage in that and computational cost of decryption is high with access policy complexity. Due to complexity this becomes significant barriers in resource limited devices while applications running [3]. For example, using pairing based ABE method encrypt the development of project after encryption process the encrypted file will upload in the create Attribute Based Encryption cipher text to university cloud. The university administrative authorized officer who has business ship drawn to stare up the college development projects through his/her limited resource then he have to download the data and have to encrypt using cipher text ABE [4]. Since cipher text could have large size also pairing procedure in decryption procedure generally luxurious for resource limited. The user has to wait for long time even aborts decryption procedure.

2. Related Work

The default attribute control the trivial policy in construction and using AND gate connect user's policy and trivial policy. Goyal et al. first deal identity based Fuzzy encryption [5]. Two complementary and various ABE concepts explained in CP-ABE and KP-ABE. The KP-ABE creation given in same paper [6], Bethencourt et al presented [7] generic group representation based on tree structure while CP-ABE construction. The ABE concerning delegatable revocation proposed in [8] to fine-grained and gain scalable access control. For load reduction at local always requires to distribute expensive computational tasks. Atallah et al. explained [9] a method to scientific computations secure outsourcing like quadrature and matrix multiplication. Through this solution disguise technique to outpour private data. Li and Atallah [10] investigated the computing issue. Efficient protocol is proposed to secure outsource sequence compare by two servers. The recommended protocol needed homomorphic encryption pricey operations. Frikken and Atallah [11] studied the issue and presented enhanced protocols to secure data. Wang et al. proposed [12] efficient methods to linear programming computation secure outsource. Several methods introduced expensive computations of secure outsource, they not appropriate for recollect ABE computational exponentiation at the user side. To accomplish this goal, server-aided techniques of traditional approach applied [13]. Using mistrustful server existing work conformed to speed up exponentiation. ABE is not efficient to utilize the technique. Another method

may leverage general outsourcing method or homomorphic encryption based delegating computation or interactive proof system. Gentry [14] revealed less security restrictions on bootstrapping process of homomorphic encryption. Therefore using general technique, computational overburden is impractical and large. Recently concrete construction [15] proposed ABE to achieve security and also achieve verifiability with no random oracles. To correctness check use the ciphertext redundancy.

3. Overall Architecture

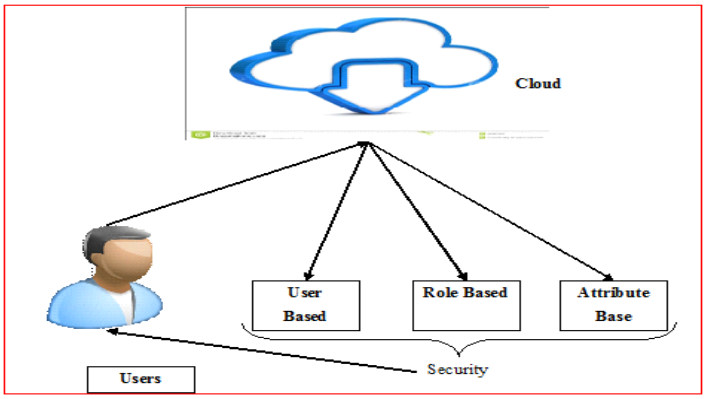

Figure-1: Cloud System.

4. Proposed Work

4.1 Cloud Server and Fifo Process

Cloud Service Provider contain huge amount of information in Data Storage and also it contain User information to validate user when they login their account. The user details will store in Cloud Service Provider database. User requested Job will redirect to Assigning Module for process by Data Server. Resource Assigning Module processes all requested user. Data Server establishes the connection to communicate with Client and other network module for this purpose we create User Interface Frame. Based on FIFO (First in First out) manner Cloud Service Provider sends Job request of user to Resource Assign Module.

4.2 Three Layer User Access Control System

The information stored in remote cloud in three layer user access control system. The data owner may share the key and data to permitted users. The data sharing accomplished as three types 1.User Based, 2.Role Based (Position/Role), 3.Attribute (Experience)

4.3 User Based

The different types of user can upload and access the data into the cloud. The user only gives the permit to cloud which type of user can view or access their data. So the user uploaded data have some restriction to view only the authorized user can able to access and view the data in cloud.

4.4 Role Based

For better security and access the information on cloud role based access is used. Role-based access control gives access permissions to user to access the data on cloud through roles which they assigned or hierarchical roles. Based on role the cloud gives the access to the use because of that the access differs. Due to controlling access of user through roles simplifies management benefits the organization.

4.5 Authentication Process

Authentication process is used share data across multiparty third authentication. Using this process permitted and new users can send request to cloud service provider to access the data then cloud will authenticates the user request if permitted user mean then it forwarded the data to requested user in case of non sensitiveness.

4.6 Algorithm

```
Void Cipher (byte[] in, byte[] out, byte[] w) {
        byte[][] state = new byte[4][Mb];
        state = in;
       AddRoundKey(state, w, 0, Mb - 1);
       for (int round = 1; round < Mr; round++) {
       SubBytes(state);
       ShiftRows(state);
       MixColumns(state);
       AddRoundKey(state, w,  round*Mb, (round+1)*Mb - 1); }
       SubBytes(state);
       ShiftRows(state);
       AddRoundKey(state, w, Mr*Mb, (Mr+1)*Mb - 1);
       out = state; }
```

5. Result and Discussion

Our proposed Approach is experimented in this paper by configuring the following requirements like Windows 7 or XP Operating System with I3 processor and also it's require 2GB RAM and 500GB hard disk drive to implement this paper in asp.net.

5.1 User Registration

The figure 2 shows user registration. In user registration the user have to fill user name, password, Email id etc. These user details verify by the cloud before login.

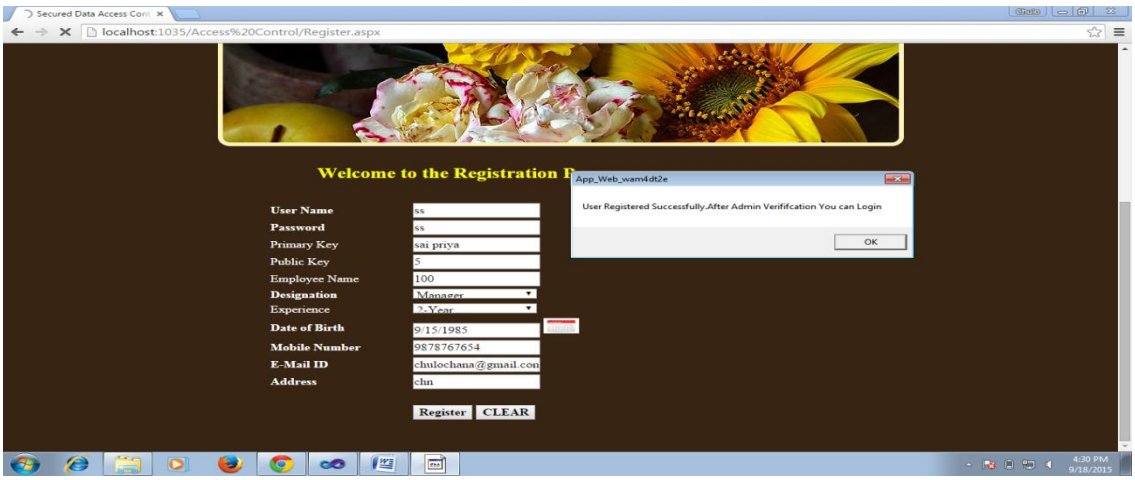

Figure 2 User Registration

5.2 File Uploading Page

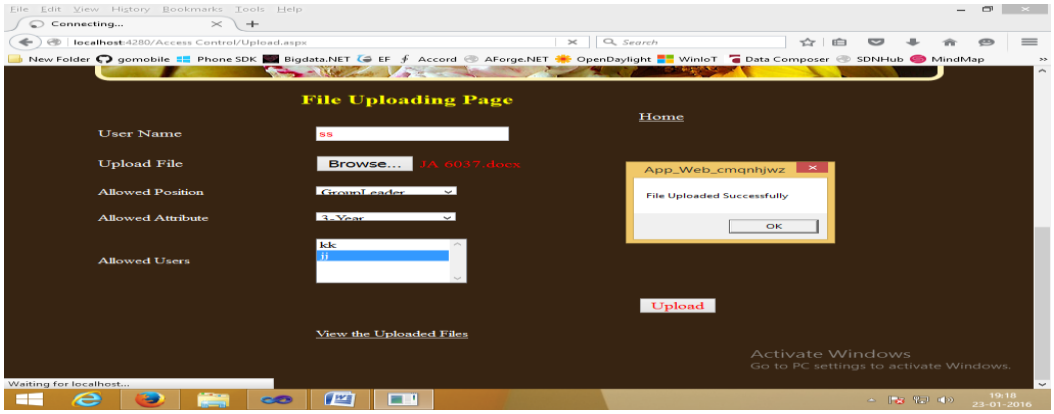

Figure 3 File Uploading Page

The figure 3 shows file uploading page. In this page the user select file to upload into cloud before uploading the user give his/her position and attribute.

5.3 User Updation Page

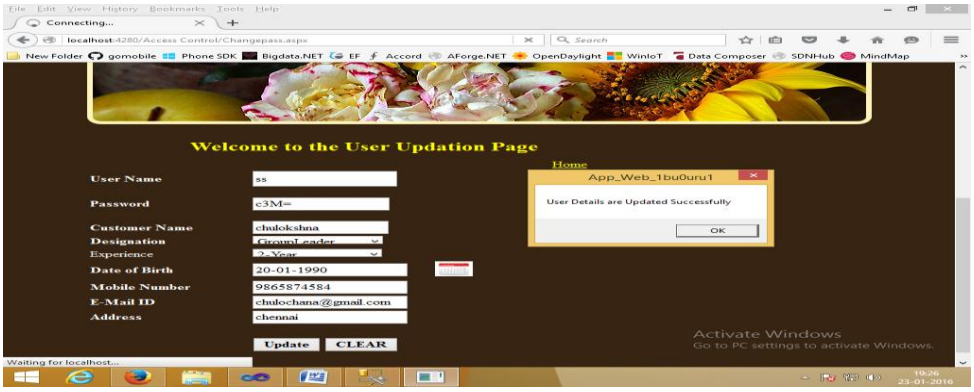

Figure4 User Updation Page

The figure 4 shows user updation page. In this page the user has to give his/her designation, experience, date of birth, mobile number and Email id.

5.4 File Downloading Page

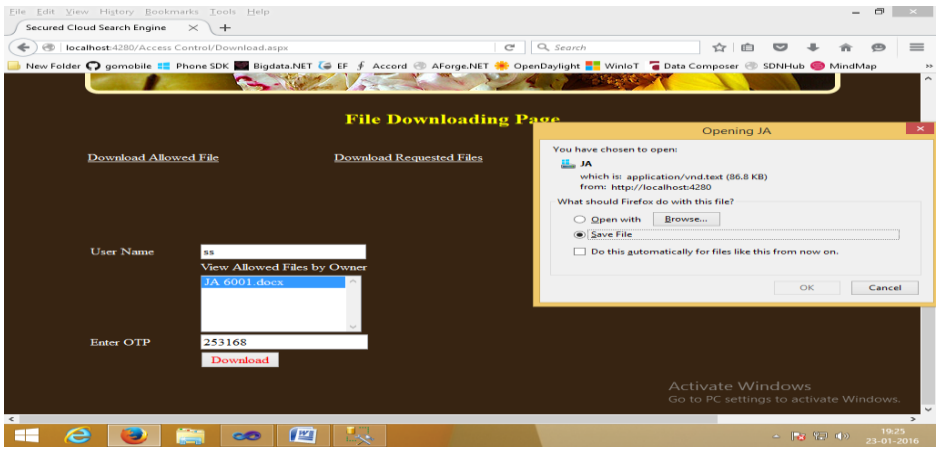

Figure-5: File Downloading Page

The figure 5 shows file downloading page. By giving the one time password the user can download the file from the cloud.

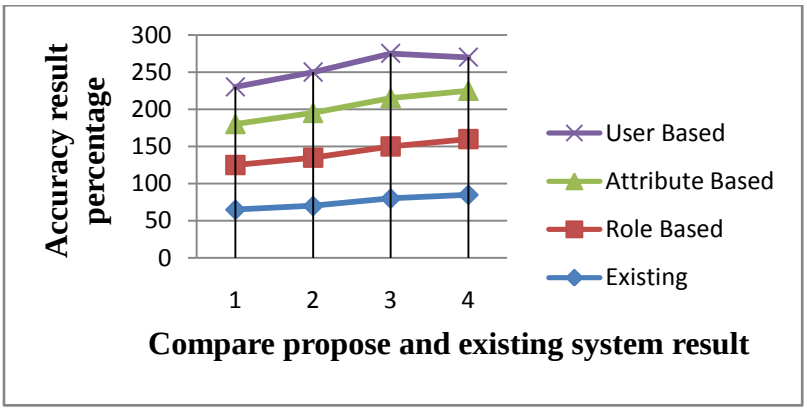

Figure-6: Display Proposed and Existing System Technique Accuracy Result.

The Figure 6 shows the accuracy result between proposed and existing technique, this result show better proposed technique. All process is show accuracy percentage in proposed system.

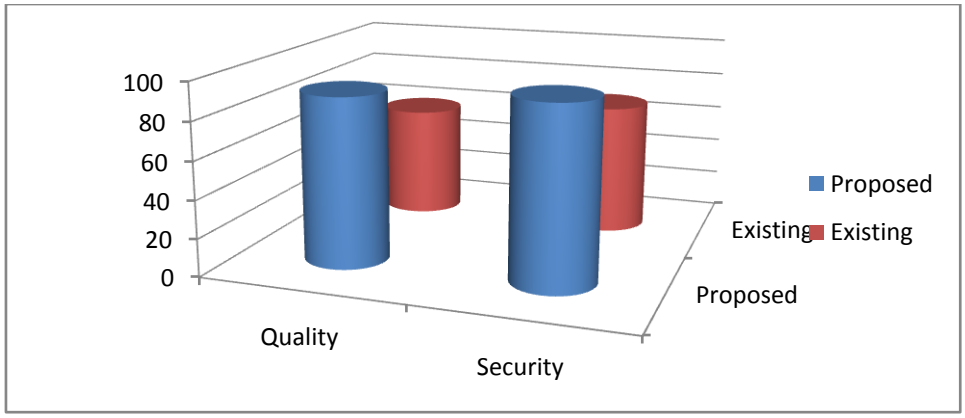

Figure-7: Display Proposed and Existing Efficiency and Quality Result.

This figure 7 shown more security better than existing system compare propose technique and that result is high quality in proposed system.

6. Conclusion

This paper proposed AES algorithm to upload the data in cloud before that it encrypt. The previous system ABE has complex progression control over protected. To overcome this complexity we proposed remote cloud to store the data in cloud. In this paper three processes have used they are, User Based, Role Based and Attribute Based. User Based process helped to know which user handle the data. Role based process gives permit to the user to access files in cloud based on position. Attribute based process contain the user experience. Through this process we secure the data in cloud.

7. Reference

1. A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, ―Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption,‖ in Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques, ser. EUROCRYPT'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 62– 91.
2. J. Lai, R. Deng, C. Guan, and J. Weng, ―Attribute-based encryption with verifiable outsourced decryption,‖ IEEE Transactions on Information Forensics and Security, vol. 8, no. 8, pp. 1343–1354, Aug 2013.
3. J. Hur and D. K. Noh, ―Attribute-based access control with efficient revocation in data outsourcing systems,‖ Parallel and Distributed Systems, IEEE Transactions on, vol. 22, no. 7, pp. 1214–1221, 2011.
4. S. Yu, C. Wang, K. Ren, and W. Lou, ―Attribute based data sharing with attribute revocation,‖ in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS '10. New York, NY, USA: ACM, 2010, pp. 261–270.
5. A. Sahai and B. Waters, „„Fuzzy Identity-Based Encryption,"" in Proc. Adv. Cryptol.-EUROCRYPT, LNCS 3494, R. Cramer, Ed.,Berlin, Germany, 2005, pp. 457-473, Springer-Verlag.
6. V. Goyal, O. Pandey, A. Sahai, and B. Waters, „„Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,"" in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89-98.
7. J. Bethencourt, A. Sahai, and B. Waters, „„Ciphertext-Policy Attribute-Based Encryption,"" in Proc. IEEE Symp. Security Privacy, May 2007, pp. 321-334.

8. S.Yu,C. Wang,K.Ren, and W. Lou, „„Achieving Secure, Scalable, Fine Grained Data Access Control in Cloud Computing,"" in Proc. IEEE 29th INFOCOM, 2010, pp.534-542.

9. M.J. Atallah, K. Pantazopoulos, J.R.Ricea,E.E. Spafford, „„Secure Outsourcing of ScientificComputations,"" in Trends in Software Engineering, vol.54, M.V.Zelkowitz,Ed.Amsterdam, The Netherlands: Elsevier, 2002, pp. 215-272.

10. M.J.Atallah and J.Li,„„Secure Outsourcing of Sequence Comparisons,""Int"l J.Inf.Security,vol. 4, no. 4, pp.277-287, Oct. 2005.

11. M.J. Atallah and K.B. Frikken, „„Securely Outsourcing Linear Algebra Computations,"" in Proc. 5th ACM Symp. ASIACCS, 2010, pp. 48-59.

12. C. Wang, K. Ren, and J. Wang, „„Secure and Practical Outsourcing of Linear Programming in Cloud Computing,"" in Proc. IEEE INFOCOM, 2011, pp. 820- 828.

13. S. Hohenberger and A. Lysyanskaya, „„How to Securely Outsource Cryptographic Computations,"" in Proc. Theory Cryptogr., LNCS 3378, J. Kilian, Ed., Berlin, Germany, pp. 264-282, Springer- Verlag.

14. C. Gentry, Fully Homomorphic Encryption Using Ideal Lattices,"" in Proc. 41st Annu. ACM

15. D.Boneh and M. Franklin. "Identity-Based Encryption from the Weil Pairing." Proc. of CRYPTO"01, Santa Barbara, California, USA, 2001.

Corresponding Author:

S. Chulochana*,

Email: *chulochana@gmail.com,*