Attribute Based Revocable Data Access Control for Multi Authority Cloud Storage

Syeda Rabiya Basri, Rashmi K H

Abstract— **Cloud Computing is emerging tremendously due to its advantages and the flexible storage services provided by it. Due to this the number of users has reached at the top. Obviously the users will be sharing the sensitive data through the cloud. And the user can't believe the untrusted cloud server. Hence the data access control has become very challenging in cloud storage system. In existing work revocable data access control scheme is proposed for multi-authority cloud storage systems which supports the access control based on the authority control. The authorized users who have eligible attributes given by multiple authorities can access the data. But it could not control the attacks which can occur by the authorized user who are not having eligible attributes. In this work we propose a new algorithm Improved Security Data Access Control which overcomes the problem exists in the existing work. And also include the efficient attribute revocation method for multi authority cloud storage.**

Index Terms— **Attribute revocation, Flexible storage service, Multi-authority, Sensitive data**

I. INTRODUCTION

Cloud Computing provides so many services in that the most important service which is provided by it is cloud storage service. The data owners can store the huge amount of data into the cloud server and the data will be accessible flexibly from everywhere. This property of cloud not only provides the benefit but also creates major challenge to data access control. As the cloud server cannot be fully trusted by the data owners. Hence to do access control one of the most accepted schemes is Ciphertext-Policy Attribute Based Encryption (CP-ABE) [1]. In CP-ABE scheme, there is an authority [2], [3] that is responsible for attribute management and key distribution. The data owner defines access policies and provides attributes to the users.

There exists another type of CP-ABE scheme that is multi authority CP-ABE [4], [5] with single authority CP-ABE scheme, where attributes are maintained and managed by different trusted authorities. The authorities are responsible for providing attributes to multiple users. In multi authority cloud storage systems user attributes can be changing from time to time. Hence the system must support the attribute revocation [6], [7].

Different authorities will provide different attributes to the end users. Hence here in multi authority system the data will also be of multiple type but all the users will not be having all the attributes. Hence the security issue arises. In this paper we propose a new algorithm called Improved Security Data Access Control. This algorithm is proposed to improve the security issue exists in the existing system. The data owner when stores the data into the cloud server he first encrypts the data then it will be stored in the cloud server. The key will be generated by the authorities to different users. And it will be given to the data owners. So when the end user accesses any data he should not only have eligible attributes but also provide the keys to access the data.

The new algorithm also helps to maintain the integrity of the data stored. If the data have got modified by any attacker the data owner will come to know about it when he verifies it. And when any of the users tries to access the data which he cannot access then this kind of attack will also be notified by the authority and will be informed to the data owner. Our system does not require the server to be fully trusted. And even if the server is semi trusted then also our system provides security.

The remaining paper is structured as follows. Section II describes about the related work. Section III describes the proposed System. System Model is described in section IV. Security Analysis is described in section V and the Conclusion are given in section VI.

II. RELATED WORK

Data access control scheme is more important hence more works have conducted in this field the important and related works have been discussed here.

Ciphertext-Policy Attribute Based encryption (CP-ABE) [1]: Ciphertext-Policy Attribute Based encryption scheme represented a system for realizing complex access control on encrypted data. Using this technique encrypted data is kept confidential even if the storage server is untrusted. The proposed system allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over their attributes specifying which users can decrypt it. It was proved secure only under some general group heuristic, and not in other situations.

Single Authority Ciphertext-Policy Attribute Based encryption [2] [3]: Here there exist only one authority which provides attributes to multiple users. And all the attributes are

Manuscript received May, 2015.

Miss Syeda Rabiya Basri, *Department of Computer Science and Engineering, Visvesvaraya Technological University, Belgaum / Godutai Engineering College for Women, Raichur, India, 9916161308*

Prof. Rashmi K H, *Department of Computer Science and Engineering, Visvesvaraya Technological University, Belgaum / Godutai Engineering College for Women, Gulbarga, India, 8095409630*

managed by this authority only. This produced a security problem and overhead to the authority as all the users need to be maintained and managed by this authority only. It was not efficient too.

Multi-Authority Ciphertext-Policy Attribute Based encryption [4] [5]: Here multiple authorities exist in the system all the authorities are included in the distribution of the attributes to the users. This scheme is more appropriate for data access control of cloud storage systems, as users may hold attributes issued by multiple authorities and data owner can share the data using access policies defined on the attributes by different authorities. This reduced the overhead of maintaining different users. Multi- authority CP-ABE scheme represented attribute revocation problem.

Attribute Revocation [6] [7]: As multiple authorities exist there will be multiple attributes to the user and the attributes can be changed dynamically. That is a user can be given some new attributes by the authority or revoked some existing attributes. This kind of attribute revocation should be considered accordingly. The new scheme overcomes the problem of revocation [8] but still there exist security problems in the existing system.

III. PROPOSED SYSTEM

The proposed system overcomes the problem exist in the existing system. We proposed a new algorithm named as Improved Security data Access Control. This algorithm improves the security of the system. The data owner when stores the data into the cloud server he encrypts it and then stores it. The keys will be provided to the authorized users by respected authorities. So when the user tries to access the data to which he is not having the eligible attribute the request gets rejected and the user gets blocked by the authority. And authority will also generate a message about the attack to the data owner. So that data owner can take further action.

If the user has done it by mistake the authorized user can contact the data owner to unblock him. If the user has not done it then also the user can contact the data owner and can ensure more security by asking the data owner to change the login details.

This new algorithm also provides data integrity. It informs about the attack by the un-authorized user to data owner when data owner verifies about it. That is, when the data owner needs to check the files stored on the cloud frequently. If any modifications are found in the file on the server by any unauthorized access then this algorithm informs the data owner that the file is not safe, it is modified.

Our system is proposed to do the following:

- Our system not only provides forward and backward security but it also provides improved security by providing access control on authorized users.
- The algorithm proposed by us improves the security by informing about the attack to the data owner.
- We also provided the data integrity. As the data owner comes to know about the verification in the data stored when he verifies it.

IV. SYSTEM MODEL

The figure shows the system architecture and it consists of the modules: Data owner, Cloud Server, Data Encryption and Decryption, Authority, Data Consumer and Improved Security

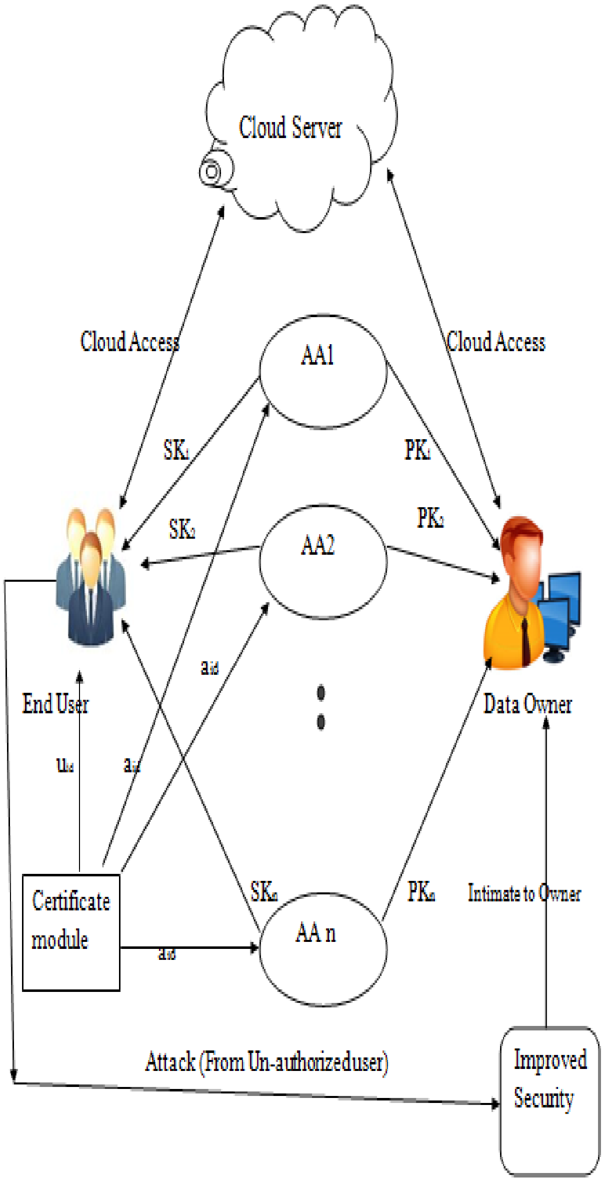

Fig 1: System Architecture

- **Data Owner**: In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then stores it in the cloud. The data owner can change the policy over data files by updating the expiration time. The Data owner is capable of manipulating the encrypted data file.

  Data owner is also responsible for blocking and unblocking the malicious user when he gets the message of the attack by the authorized user. Data owner also checks for the integrity by verifying the uploaded files time to time.

- **Cloud Server**: The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

- **Data Encryption and Decryption**: All the legal users in the system can freely query any interested encrypted and decrypted data. Upon receiving the data from the server, the user runs the decryption algorithm Decrypt to decrypt the cipher text by using its secret keys from different Attribute Authorities (AAs). Only the attributes the user possesses satisfy the access structure defined in the cipher text CT, the user can get the content key. Here AES Algorithm is being used to encrypt and decrypt all the data.

- **Authority**: Authorities from different domain provide the attributes to the end users. One end user can have the attributes given from different authorities and even the authorities can give the attributes to different end users. Only the end users who have the authorized attributes can access the particular files.

- **Data Consumer**: Here the user can only access the data file with the encrypted key if the user has the privilege to access the file that is if the user have enough attribute to access that file. For the user level, all the privileges are given by the Domain authority as attributes and the data users are controlled by the Domain Authority only. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. And these kind of malicious users are caught by the improved security algorithm.

- **Improved Security**: This newly designed algorithm is responsible for providing improved security to the data stored. It generates the email message to the data owner that some attack has been occurred by the malicious user. Then the data owner can take the further action by blocking that user. If any attacker modifies some file then it informs to the data owner about the modifications when the data owner verifies that file.

V. SECURITY ANALYSIS

Our Data access control scheme is secure where we achieve forward security, backward security, improved security, and data integrity.

1. **Forward Security**: Forward Security is achieved when any new user is joined. If the new user has sufficient attributes new keys will be generated and provided to the new users. Hence the new user can access previously published data also. And the already existed authorized users will also be provided the newly generated keys. Hence the problem is resolved even for them.

2. **Backward Security**: Each time when the secret key update algorithm runs it provides new secret key to all the authorized users. When any attribute is revoked then user will be automatically removed from the list of that authority and hence he will not get the new key. When the user does not have the attribute and the newly generated key he cannot access the data. Like this the backward security is achieved.

3. **Improved Security**: When the authorized user tries to access the data for which he is not having the attribute at that time this will come into picture. The authorized user will obviously not get that requested data and also he will get blocked. A message informing about this will also be sent immediately after the attack. This reduces security risk of the unauthorized users who have compromised authorized users also.

4. **Data Integrity**: Data integrity is maintained by data owner. Data owner keeps checking the files stored into clod data base. When any of the attackers attacks and modifies the data stored then data owner will come to know about the attack and the verification of that file. Like this the data integrity is maintained.

VI. CONCLUSION

As the number of users in cloud computing increasing security issues are also increasing accordingly. The main security issue can be how to control the unauthorized data access in cloud. In this paper we proposed an efficient data access control scheme with improved security. Our scheme not only restricts the unauthorized access but also ensures secure access by the authorized users. Along with that data integrity is also provided. This scheme is proposed for multi-authority cloud storage system. This scheme can be applied in social networks which are online and also in the remote storage systems.

ACKNOWLEDGMENT

I would like to express my sense of proud gratitude and indebtedness to my guide, for her valuable guidance, suggestions, timely supervision for successful completion of my paper. Above all I would like to thank my parents and all my family members and friends for their constructive criticism and construct support in making this grand success.

REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in *Proc, IEEE Symp, Security and privacy (S&P'07), 2007,* pp. 321-334.

[2] B. Waters, ''Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,'' in *Proc.4th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC'11),* 2011, pp. 53-70.

[3] V. Goyal, A. Jain,O. Pandey, andA. Sahai, ''Bounded Ciphertext Policy Attribute Based Encryption,'' in *Proc. 35th Int'l Colloquium on Automata, Languages, and Programming (ICALP'08),* 2008, pp. 579-591.

[4] M. Chase and S.S.M. Chow, ''Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,'' in *Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09)*, 2009, pp. 121-130.

[5] A.B. Lewko and B. Waters, ''Decentralizing Attribute-Based Encryption,'' in *Proc. Advances in Cryptology-EUROCRYPT'11*, 2011, pp. 568-588.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, ''Attribute Based Data Sharing with Attribute Revocation,'' in *Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS'10),* 2010, pp. 261-270.

[7] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, ''Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,'' *IEEE Trans. Parallel Distributed Systems*, vol. 24, no. 1, pp. 131-143, Jan. 2013.

[8] K. Yang, X. Jia, "Expressive Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage", in *IEEE Transactions on Parallel and Distributed Systems,* vol.25, no.7, pp 1735-1744, July 2014.

Syeda Rabiya Basri received the B.E degree in Information Science and Engineering from Visvesvaraya Technological University, Karnataka, India in 2012, now doing M.Tech (4th sem) degree in computer science from Visvesvaraya Technological University, Godutai Engineering College for Women Gulbarga, Karnataka, India in 2015(Pursuing).

Prof Rashmi K H received the B.E degree in Information Science and Engineering from Visvesvaraya University, Belgaum, Karnataka, India in 2009, M.Tech in computer science and engineering from Visvesvaraya University, Appa Institute of Engineering Technology Gulbarga, Karnataka, India in 2013, working as Asst. Prof in Godutai Engineering College for Women.