AN ASPECT OF JOIN INGRESS AUTHORITY FOR CIVIC DIRECTORY

Premamala T[1]*, Menaka R[2]*, Poorani S.T[3] , Saranya k[4]

Professor[1&2] &Final Year Students[3&4],
Department of Information Technology Velalar
College of Engineering and Technology, Thindal,
Erode, Tamilnadu, India, Pin Code: 638012.
Corresponding Author Email: pooranist99@@gmail.com

Abstract: *In public cloud storage services, information is provided to externally trusted cloud servers that trust the data owner's domain. To prevent trusted service providers from accessing owner personal information, the exported information is hidden. In this situation, how to manage access to that data can be a difficult problem. Attribute Based Encryption (ABE) has been a critical privacy tool for implementing accessibility standards, which can provide better access, flexibility and security to external data. However, the current ABE access management system does not support users gaining access through collaboration. Here, this system explore specific features based on access management capabilities, in which many users with different sets of attributes can work together to gain access if the data owner allows the collaboration to not be specified in the access policy. However, cooperation that is not included in the access policy should be considered a collusion and the application for entry should be rejected. This paper propose that the access control system is accessible through custom control configurations. The data analysis showed that it is the guarantee of the security of the secret, and the many other people who are able to, proposed from the difference between the security of the features of plans. The analysis shows that it has a wide range of performance in terms of storage system design and storage head.*

Keywords*: Public cloud storage, Access Control, CP-ABE (Ciphertext Policy-Attribute Based Encryption), Collaboration.*

INTRODUCTION

The Cloud computing provides many advantages, such as speed and efficiency, via dynamic scaling This cloud security threat includes data breaches, human error, malicious interior people, account theft and DDoS attacks. With increasing in cyber threats across the internet for cloud computing. Need to provide more advanced security to safeguard data. Cloud computing is the development of other services such as web hosting and online storage, so it faces many challenges and cybercrime. Hackers who can convert to a large number of private or private buildings can steal, use or sell important information to many users. Credit card type information, financial records, software and reports are at risk of being stolen by many customers. CSP'S (Cloud service Providers), therefore are obligated to stay Vigilant to keep this information safe continually consequently, user data safety defends on a CSP'S safety level and culture. Encrypting data ensures that even if that data falls into the wrong hands, it is useless as long as its key remain secure. This is especially beneficial when data is being stored in the cloud, as it protects data contents if a provider, account or system is compromised. Attribute Based Encryption is a type of public key encryption in which the secret key of a user and the cipher text are dependent upon the attributes. In such case decryption of a cipher text is possible only if the set of attributes of the user key matches the attribute of cipher text.

.

1. OBJECTIVES

The main objectives are:

- Speed and efficiency via dynamic scaling .
- Cloud service provider obligated to stay vigilant to keep sensitive information safe continually.

- Encrypting data ensures that even if the data falls into wrong hands, it is useless as long as its key remain secure.
- Each collaboration is only useful to decrypt one ciphertext.

2. RELATED WORKS

A new advancement in the encryption method based on Attribute Based Encryption (ABE) is implemented. Using proposed algorithm, able to provide a collaborative access control scheme for public cloud storage. For an enterprise, the data stored is enormous, and it is very precious. All tasks are performed through network. Hence, it becomes imperative to have the secured use of data. In cloud Computing, the most essential concerns of Security are data security and privacy.
Let us consider the various approaches used in the existing system.

A.Ciphertext Policy Attribute Based Encryption

ABE is regarded as a promising technique to provide fine-grained, flexible, and secure access control of outsourced data in public cloud storage. The first CP-ABE scheme was designed by Bethencourt and subsequently some literatures were proposed to improve its security. To improve its expressiveness, the work has been proposed, and then the work of further improves the scalability. Considering that users may hold attributes from multiple authorities, some multi- authority schemes, the authors pointed out that ABE schemes cannot express access control rules like role hierarchy and object hierarchy. Consequently, propose a secure role-based access control scheme to address the problem.

B.Secret Sharing Scheme

A feasible solution to support collaboration among users and it has been adopted in collaborative access control. It specifies that a secret can only right. Weighted threshold secret sharing schemes are natural generalizations of threshold secret sharing schemes, where each participant is assigned a weight depending on his/her importance in the group of all participants. For example, in a bank, the tellers and directors have different weights as to the rights to reconstruct the key of bank vault. The secret can be reconstructed if and only if the sum of the weights assigned to a set of participants is greater than or equal to a fixed threshold. A variant of weighted secret sharing is multi- level secret sharing schemes, where participants are partitioned into levels. Generally speaking, those schemes distinguish a user by only one factor (e.g. importance, role, or level).

Literature Survey

A.Security Of Cryptographic Keys

G.R.BLAKLEY (1979) In this system, certain cryptographic keys, such as a number which makes it possible to compute the secret decoding exponent in an RSA public key cryptosystem or the system master key and certain other keys in a DES cryptosystem, are so important that they present a dilemma, If too few are listed, they will all be damaged.

B.Decentralizing Attribute Based Encryption

In this system, the party can be the authority and there is no requirement for global coordination in addition to establishing the initial reference parameters. A party may only have ABE authority by creating a public key and issuing a private key for the other user's service which may indicate its settings. Users can encrypt data in any format Boolean formula for attributes coming from the selected authority set.

3. EXISTING AND PROPOSED SYSTEM

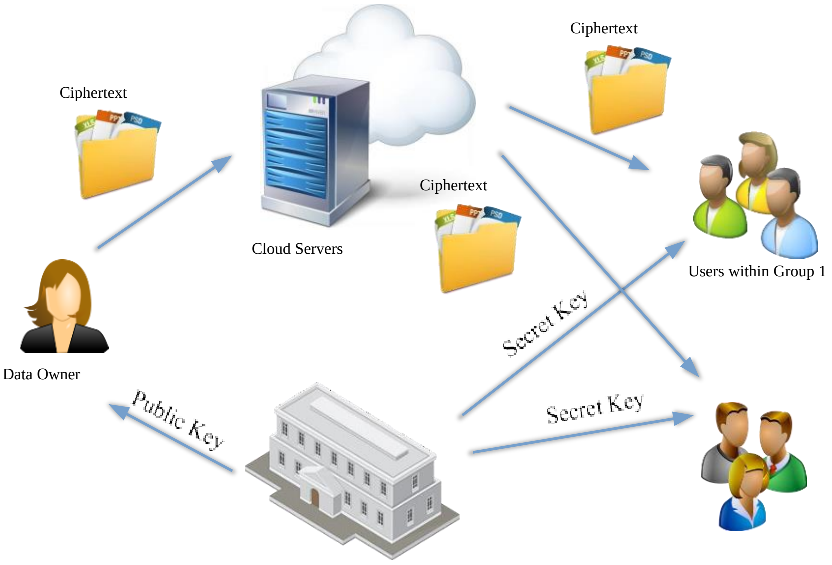
A.Exsiting System

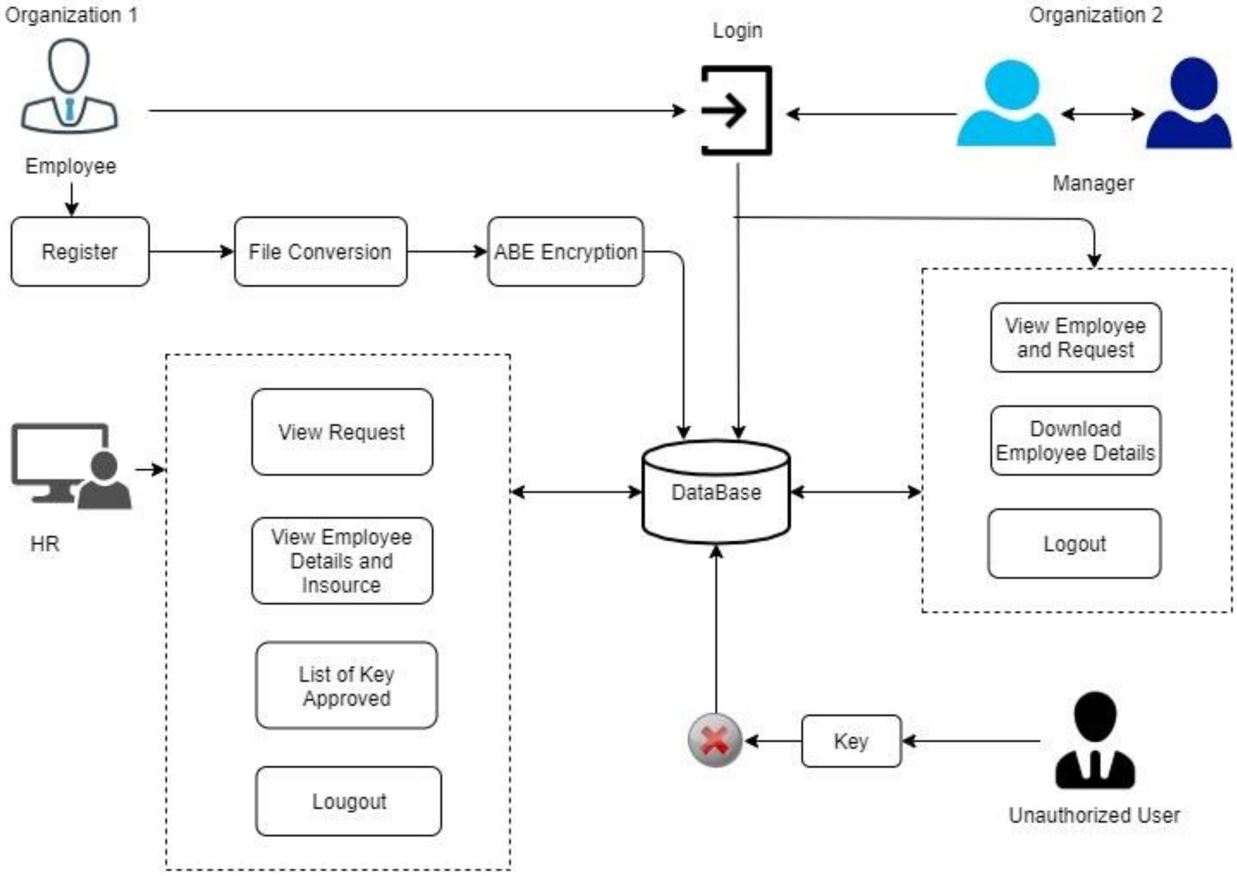
Storing a massive number of data in the cloud may pose serve challenges of information theft and data manipulation since all data is always online, and this leads to a significant problem as its data could be altered for the harmful causes. In the present system the attribute based encryption technique, the cloud will not allow collaborative access control for the data users, which can make it less efficient. Attribute policies are related to data, and properties are associated with data, and attributes are associated with key, and only key where attributes are related to basic data can decrypt. The existing application is just concentrated on security in the cloud. It focuses on providing access to the high threshold users in the system. And does not provides full hiding of data with other users. In the existing system, the algorithm only concentrates on the accessibility and security methods, which even less protects sensitive data from unauthorized access.

B.Proposed System

In this proposed system, unlike the standard attribute based encryption, users within the same group. Policy, and at the same time, also resist the collusion attack when curious users try to combine their attribute sets in other ways. Technically, embed translation keys in the secret keys of CP-ABE schemes and modify the secret keys to associate groups to users. The data owner can designate collaboration by setting translation nodes in the policy tree. This system is promising to provide fine grained access control in collaborative setting where data need to be accessed by multiple users.

SYSTEM MODEL





SYSTEM ARCHITECTURE

Advantages:

The proposed system has the following advantages

- The controlled collaboration within the same group can be implemented.
- Key privacy will be more secure than the typical attribute based encryption.
- Data is more secure and accessible.
- User collusion resistance is available in this system.

4.MODULE DESCRIPTION

A.Upload Information

The employee will register the information like that address, educational details, experience details, account details and etc.... All information and records are set in database. Personal information is all kept under each employee records for easy references. High regulated access levels and security settings make it easier for authorized users to protect workers data.

B.File Conversion

Collects the information of the employees registered details and it convert into a document the stored in the database. The converted document is stored in a secured ways which means file is only access by the set of attribute key. Without using a key, it can’t be able to read a file or download a file.

C.Attribute Based Encryption

For securing the employee details within an organization used by attribute based encryption method. Attribute encryption is a type of public key encryption text in which the user's secret key and encrypted text depend on the property. In such a system, the decryption of the encrypted text is only possible if the set of attributes of the user key corresponds to the characteristic of the encrypted text. ABE identified one step further, not as nuclear but as a set of attributes.

D.Collaborative

Collaboration is the process in which two or more people work together to complete a task or achieve a single common goal. Collaboration is same as cooperation. Most collaborations require leadership, although the form of leadership can be social within a dispersed and equitable group. Collaborative teams often gain more resources, recognition, and rewards when faced with limited resource competition.

E.*Retrive Information*

The operations on the data retrieving are performed only by the basis of attribute key, this is delegated to loyal authority. A key is only accessible by an administrator for the authorized users. The key generation to access the data by an entity within a organization is to be maintained by the administrator level. If the hacker try to access the data by using the same key, it will not allow to download information. The data only access by authorized users.

5.CONCLUSION

In this paper an attribute based controlled collobarative access control scheme, in which data owners can designate selected users to collaborate for data access. More importantly, the data owner can devise the way for chosen users to combine their attribute sets to satisfy the access policy, and at the same time also resist the technically, embed translation keys in the secret keys of CP-ABE schemes and modify the secret keys to associate groups to users. The data owner can designate collaboration by setting translation nodes in the policy tree. Our security analysis shows that proposed scheme effectively supports data confidentiality, user collusion resistance**,** controlled collaboration within the same group, secret key privacy, secure revocation of the collaboration and non reusability of intermediate results.

Future Scope

The algorithm proposed using ABE is a framework for a real-time system. The proposed algorithm has to verify and validate using a simulator. The proposed algorithm is provided security from malicious insiders and threats during the processing of the data. And finally, proposed new ABE based encryption algorithm with collaborative access control, for public cloud storage. The proposed algorithm will be suitable for the application or the information that needs high level security and accessed time is being reduced which indeed cost is reduced comparatively.

REFERENCES

1. *W.Li, K.Xue, Y.Xue, and J.Hong, "TMACS: A robust and verifiable threshold multi authority access control system in public cloud storage," IEEE Transactions on Parallel and Distributed Systems, volume: 27, no. 5, pp:1484–1496, 2016.*
2. *K.Xue, W.Chen, W.Li, J.Hong, and P.Hong, "Combing data owner-side and cloud-side access control for encrypted cloud storage," IEEE Transactions on Information*

Forensics and Security, vol:13, no:8, pp:2062– 2074, 2018.

3. A.Shamir, "How to share a secret," Communications of the ACM, vol:22, no:11, pp: 612–613, 1979.
4. T.Tassa, "Hierarchical threshold secret sharing," Journal of Cryptology, vol:20, no:2, pp:237–264, 2007.
5. M.Li, X.Huang, J.K.Liu, and L.Xu, "GO-ABE: group- oriented attribute-based encryption," in Proceedings of the 8th International Conference on Network and System Security (NSS). Springer, 2014, pp:260–270.
6. J.Bethencourt, A.Sahai, and B.Waters, "Ciphertext- policy attribute-based encryption," in Proceedings of the 28th IEEE Symposium on Security and Privacy (Oak- land). IEEE, 2007, pp:321–334.
7. M.Kallahalla, E. Riedel, R.Swaminathan, Q.Wang, and K.Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proceedings of the 2nd USENIX Conference on File and Storage Technologies (FAST), 2003.