ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Secure data sharing using attribute based encryption in cloud computing

G.K.Sandhia[1], G. K.Bhaskar[2*]
[1]SRM University, Chennai, India
[2]B.S. Abdur Rahman University, Chennai, India.
***Corresponding author: E-Mail: kbhaskar91@gmail.com**

ABSTRACT

To protect the outsourced data in cloud storage during transmission and at rest, becomes critical. Attribute based encryption provides the security and access control mechanisms for integrity. Cipher text attribute based encryption plays a major role in providing security and integrity with the help of access tree structure. The existing encryption algorithms are not feasible to protect the data. In cipher text attribute based encryption the keys are encrypted using symmetric encryption and the attributes in the access tree are used for access control mechanisms. Whenever the size of the attribute increases the size of the cipher text also increases. The main objective is to provide the security using asymmetric encryption and access control structure for authentication and data integrity. The size of the cipher text will be constant even though the number of attributes are increased. The constant size cipher text can be achieved through integrated access structures. The proposed work provides confidentiality, authentication and data integrity. The personal health records are encrypted using ABE scheme.

KEY WORDS: cloud computing, access control, attribute based encryption.

1. INTRODUCTION

Social networks such as Orkut, Facebook, Friendster enables the users to find or connect with other users based on mutual interests. To use these applications, users must mention about the personal information (e.g. name, age, address, personal interest, etc.) into the public domain. Groups of people sharing similar interest are automatically connected to other people around the world. Be that as it may, such frameworks give just powerless protection ensures system participation permits access to the abundance of client data. Appropriately, client information can promptly be mined and manhandled by undesirable gatherings. ABE-based frameworks are appropriate to give client controlled-security, as clients in these groups are as of now portrayed by their characteristics. In Friendster, for instance, a client with the quality Anon U. Former student is consequently selected in a gathering of the same name. As needs be, the making of white-records for correspondence instantly gets to be conceivable without requiring specification of all client personalities. Developing an informal community utilizing ABE likewise gives adaptability. Current interpersonal organizations require a trusted focal server to store all profile data and authorize arrangement. Since ABE-based frameworks do not require a trusted stockpiling framework, profile data could be put away on untrusted servers altogether diminishing the activity and capacity necessities caused by a framework. To keep information private to information servers the information proprietor encodes information before transfer. Client access is allowed by having the information unscrambling keys. When this sort of cryptographic-based access control plan gives security assurance on information, there are likewise a few noteworthy difficulties related to the plan outline. To pick up protection of information from cloud administration supplier and other non-related hubs encryption, systems are the key source that gives significant security. Security consists of number of methods to achieve cryptographic security. One of the most popular method is Attribute-based encryption (ABE). It is shown in Fig 1.

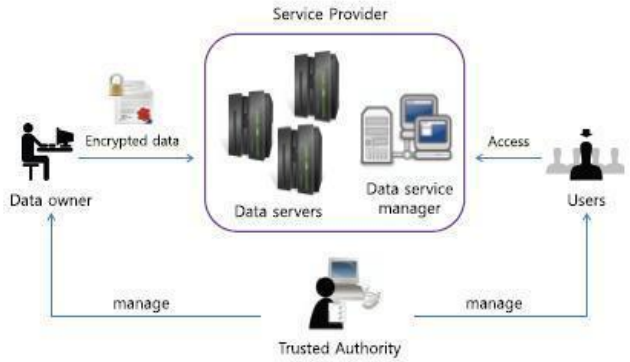

Figure.1. Architecture of Data sharing System.

The data sharing system consists of the following components:

A. Data Owner: When the client wants to send the information and desires to add it into the external data storage center for data sharing or for cost saving. A knowledge proprietor is liable for outlining (attribute founded) access coverage and implementing it on its possessing data by means of encrypting the data beneath the coverage before distributing it. Data owner should get key from key generator and encrypt the file. Encryption is the process of converting the data into cipher text that can't be simply understood with the aid of unauthorized individuals.

B. Data Storing Centre: This component provides the information to the service provider. It is accountable for controlling the accesses from external customers to the storing knowledge and supplying corresponding contents offerings. The data storing center is a different key authority that generates personalized consumer key with the Key Generation Center and revokes attribute staff keys to legitimate customers per every attribute which might be used to enforce a high-quality-grained consumer entry control. Knowledge storage facilities presents offsite file and tape storage.

C. User: This is an entity who wishes to access the information. If a consumer possesses a suite of attributes enjoyable the access coverage of the encrypted information outlined by way of the data proprietor and it is not revoked in any of the attribute businesses, then user has to decrypt the cipher text to obtain the information. It is shown in Fig 2.

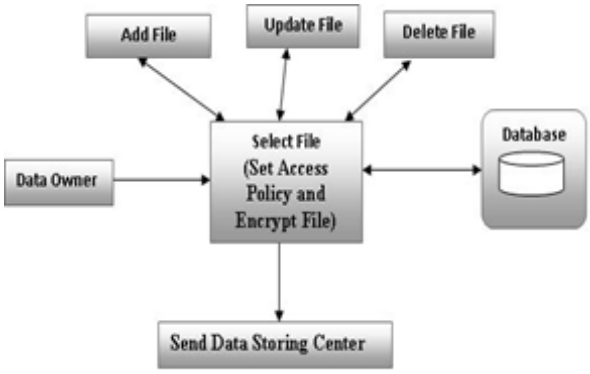

Figure. 2. Data Owner (Access Policy, Encrypted File)

D. Key Generation Centre: The key authority center generates public and secret parameters for CP-ABE. This will be used for revoking and updating the user key attributes. It provides various access rights to individual customers with respect the attributes. Key iteration is the system of generating keys for cryptography. It is shown in Fig 3.

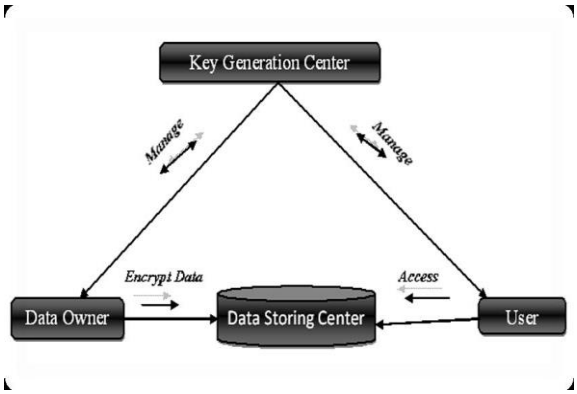

Figure.3. Structure of Attribute Based Sharing

The structure of the Attribute based data sharing is shown in Figure.3. The entities involved are administrator and customers which stand as UI for the approach. Key generation Centre (KGC) is a key authority that generates public and secret parameters for CP-ABE. Data storage center is the component that presents a knowledge sharing carrier. The information storing center is one more key authority that generates customized consumer key with the KGC and revoked attribute staff keys to legitimate customers per each attribute that are used to provide a fine-grained user access control. The client who owns information and desires to add it into the external data storage center for data sharing or for cost saving. A knowledge proprietor is responsible for defining entry policy and also it possesses data by encrypting the information below the policy earlier than distributing it. Consumer is an entity who wishes to access the information.

2. LITERATURE REVIEW

Cloud service providers determine the access control mechanisms for data on the cloud. Access control is a procedure that restricts, denies or allows access to system. In the cloud, data security is crucial to protect against inside attack, denial of service attack and collision attack. Traditionally different expressive access control policies are used to protect data stored locally and data stored remotely. The approaches include Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC). In DAC, users are given complete control over resources on the basis of user identity. The use of DAC is not feasible when the size of the network and the number of users increase or when data is distributed across

different servers. In RBAC, access is based on particular roles and varies depending on the user. A role is assigned to different tasks, for example members of staff have different roles.

RBAC is not feasible because all entities have the right to access and large groups would have same type of access. ABAC considers attributes based on user requests including names and value pairs and are associated with actions, users, subjects, objects, contexts and policies. ABAC is more flexible, secure, and scalable and works in a hierarchical fashion. ABAC solved the RBAC problem of assigning privileges to a user. However, such access control schemes or the use of a server as a reference monitor cannot be applied in cloud environments because clouds have plenty of resources, lot of dynamic users and flexible construction because every autonomous system has its own security policy. As networks grow and the number of users increases, a more complex structure must be created to improve the performance and reliability of stored data. The data are replicated across several locations and stored in distributive fashion across many servers. This creates a lack of confidentiality and security. The only method for protecting sensitive data across multiple sites is to encrypt the data before uploading to the server. Data stored on the cloud must be protected through different mechanisms. One of the vital techniques is public key encryption. In the traditional public key infrastructure, the data owner encrypts the data with the data user public key, before uploading it to the cloud. When a data user sends a request to access data on the cloud, the cloud decrypts the cipher text with the private key. There are two major disadvantages with this technique. First, for encryption, the data owner must obtain the data user public key before uploading. Second, because the same plaintext is used with different public keys, the storage overhead becomes excessive.

Attribute based encryption: The Sahai-Waters (ABE) cryptosystem as implemented in this paper is specifically detailed. Attribute-centered Encryption can be considered as a generalization of identity-headquartered Encryption (IBE). In IBE a person identification is a string which is similar to "bobsmith@yahoo.com". A celebration in the method can encrypt a message to this designated person with handiest the competencies of the recipient identity and the procedure public parameters. In exact the encryption algorithm ought no longer to have entry to a separate public key certificate of the recipient. In Attribute-established Encryption, user identification consists of a collection, S, of strings which serve as descriptive attributes of the user. For illustration, a person identity could include attributes describing their university, department and job function. A get together in the system can then specify an extra set of attributes for the receiver to decrypt a message if his identity S has at the least single set of attributes with the set S0.

The user needs to get related with each the parties before getting the set of keys. The role of KGC is to authenticate customers along with the distribution of the set of attribute keys in order that user is ready to generate secret key via combining the important thing accessories received from the each authorities.

Security based on ABE for data sharing: In proposed a mediated Cipher text-policy Attribute-head quartered Encryption (CP-ABE) which extends CP-ABE with instantaneous attribute revocation. Additionally, they reveal how user can observe the proposed CP-ABE scheme to soundly manage private wellbeing records (PHRs).

In offered the inspiration of Fuzzy identification founded Encryption, which enables the error-tolerance between the identification of secret key and the general public key used for encrypting a cipher text. Two realistic functions of Fuzzy IBE of encryption using biometrics and attribute-based encryption and also provided the development of a Fuzzy IBE scheme that makes use of set overlap as the gap metric between identities. Ultimately the proved scheme is the Selective identity mannequin with the aid of decreasing an assumption that can be viewed as a modified variant of the Bilinear Decisional Diffie Hellman assumption. Confidential information is shared and stored on websites on the web, on these websites will need to encrypt data stored. Encrypt knowledge to a problem is that it selectively best a rough-grained level will also be shared (i.e., supply your private key to yet another occasion). The attribute Key-satisfactory-grained policy-founded encryption (KP-Abe) is to share encrypted data to advance a new cryptosystem. Elements of our cryptosystem texts are represented and secret keys which might be capable to decrypt cipher strength texts customers are associated with access control constructions.

In provided procedure for Cipher textual content-policy Attribute situated Encryption. The approach enables for a new sort of encrypted access control the place person exclusive keys are distinct by using a suite of attributes and a party encrypting information can specify a policy over these attributes specifying which users are competent to decrypt.

In presented a dispensed KP-ABE scheme that solves the key escrow quandary in a multi authority system. In this process, all (disjoint) attribute authorities are participating in the important thing new release protocol in a distributed way such that they cannot pool their data and link multiple attribute units belonging to the identical consumer. One drawback of this kind of entirely distributed process is the performance degradation. Due to the fact that there is no centralized authority with master secret understanding, all attribute authorities will have to communicate with the other authorities in the procedure for the reason that the grasp key is a centralized authority with understanding, procedure presenting all officers to generate secret key a person to be in contact with different officers. M to generate a user's secret key.

In the motive instances of corruption of KGC and corrupted data stored and also furnished with a proof of 2pc protocol however the difficulty of this procedure was once reliability and cargo balancing underneath actual time environment.

3. CONCLUSION AND FUTURE SCOPE

ABE is an extensively used encryption technique for access control in cloud computing. The main advantage of ABE is that it gives users access to stronger encryption and allows key strength distribution. This paper has analyzed several different ABE techniques and categories and reviewed the functionality and limitations. The extended survey to weighted attribute based encryption techniques perform better by offering fine-grained access control.

REFERENCES

Armbrust M, Fox A, Grith R, Joseph A.D, Katz R, Konwinski A, Lee G, Patterson, Rabkin D A, Stoic I, Zaharia M, A view of cloud computing, Communications of the ACM, 53 (4), 2003, 50-58.

Bethencourt J, Sahai A, and Waters B, Cipher text policy attribute based encryption, Proc. IEEE Symp. Security and Privacy, 2007, 321-334.

Boneh D, Franklin MK, Identity-based encryption from the weil pairing, In Proceedings of the 21st Annual International Cryptology, 2001, 1-31.

Cocks C, An identity based encryption scheme based on quadratic residues, In IMA Int. Conf., 2001, 360-363.

Dikaiakos M.D, Katsaros D, Mehra P, Pallis G, and Athena Vakali, Cloud computing: Distributed internet computing for it and scientific research, IEEE Internet Computing, 13, 2009, 10-13.

Garg S, Gentry C, and Halevi S, Candidate multilinear maps from ideal lattices, in Eurocrypt, 2013.

Garg S, Gentry C, Halevi S, Sahai A, and Waters B, Attribute-based encryption for circuits from multilinear maps, Lecture Notes in Computer Science, 8043, 2013, 479–499.

Ghafoor A, Sher M, Imran M, and Saleem K, Light weight key freshness scheme for wireless sensor networks, 12th International Conference on Information Technology - New Generations, 2015.

Khader D, Attribute Based Authentication Schemes, Ph.D Dissertation, University of Bath, 2009.

Kirubakaramoorthi R, Arivazhagan D, and Helen D, Survey on Encryption Techniques used to secure Cloud storage system, 8 (36), 2015.

Lee C, Chung P, and Hwang MS, A survey on attribute-based encryption schemes of access control in cloud environments, International Journal of Network Security, 15 (4), 2013, 231–240.

Li K, Hu TX, and Fen LJ, Tight chosen cipher text attack (CCA)-secure hybrid encryption scheme with full public verifiability, Science China Information Sciences, 57 (11), 2014, 1–14.

Rupesh Vaishnav, Attribute Based Signature Scheme for Attribute based Encrypted data in cloud, International Journal of Engineering Research & Technology (IJERT), 1 (10), 2012.

Sahai A, and Waters B, Fuzzy identity based encryption, Eurocrypt, 2005.

Saikeerthana R, Umamakeswari A, Secure data storage and data retrieval in cloud storage using cipher policy attribute based encryption, 8 (S9), 2015, 318-325.

Sakthi Saravanan B, Dheenadayalu R, Improving Efficiency and Security Based Data Sharing in Large Scale Network, International Journal of Engineering Science and Innovative Technology (IJESIT), 2 (1), 2013, 120-128.

Shamir A, Identity based cryptosystems and signature schemes, In Proceedings of CRYPTO 84 on Advances in Cryptology, Springer Verlag New York, Inc., 1985, 47-53.