Proc. of the Intl. Conf. on Recent Trends In Computing and Communication Engineering -- RTCCE 2013
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-981-07-6184-4

A Novel Method of HASBE with Improved Efficiency and Delegation Mechanism in Cloud

S.Dhivya bharathi[1] S. Sathyalakshmi [2]

SCHOOL OF COMPUTING SCIENCES, HINDUSTAN UNIVERSITY,CHENNAI

ABSTRACT

Cloud computing is one of the most influential paradigms in the IT industry in recent years. Since this technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, a hierarchical attribute-set-based encryption has been proposed (HASBE) with a hierarchical structure of users. The novel method of HASBE introduces in term of delegation mechanism and improved efficiency. It provides efficiently share confidential data on cloud servers and also involves in full delegation. The delegation defines that it involved for the transfer of authority under server permission.

INTRODUCTION

Cloud Computing is Internet-based computing, whereby shared servers provide resources, software, and data to computers and other devices on demand. However it hardly suffers from computational overhead and security problems.

Attribute Set Based Encryption has been proposed for access control of outsourced data in cloud computing. The drawback of the ASBE is inflexibility. Attribute Based Encryption,user is able to decrypt a ciphertext only if there is a match between its decryption key and the ciphertext. The drawback of ABE is expressability. Based on the attributes, the encrypted data is described and the key generation has to be made by the policies used.

Key Policy Attribute Based Encryption(KP-ABE), a ciphertext is labelled with a set of attributes and a user’s decryption key is associated with a monotonic key structure that controls which user is going to decrypt. Fine grained method defines that it involves in centralised authority i.e it provides the key to the certified users. While the coarse grained method forwards the key to the third party without the knowledge of the user.

Ciphertext Policy Attribute Based Encryption(CP-ABE), the ciphertext is encrypted with tree access policy chosen by an encryptor, while the corresponding decryption key is created with respect to a set of attributes. Hierarchical Attribute Based Encryption(HABE) combination of HIBE and CP-ABE. This scheme does not support compound attributes efficiently as well as multiple value assignments. In a hierarchical identity-based encryption scheme, user identities are arranged in an organizational hierarchy. Anyone can encrypt a message to any identity in the system using the public parameters.

For the heavy computation overhead, the problems are achieving scalability and data confidentiality are still remains. The scheme which is applicable for only if the data owners and the service providers are within the same trusted domain. If the data owner and the service provider are not in the same trusted domain, the access control scheme which employs KP-ABE in a fine grained manner but it does not provide effective flexibility and lack of scalability in the attribute management. So that CP-ABE technique is used to deal with the multiple level of attributes.

CP-ASBE is used for the multiple value assignments. Hence this is also used for combined attributes from the multiple sets. HASBE scheme defines the extension of the CP-ASBE that also provides multiple value assignments. This is not only achieves scalability but also improves flexibility and fine grained access control for the outsourced data.

The novel method of HASBE introduces in terms of delegation mechanism and improved efficiency. It provides efficiently share confidential data on cloud servers and also involves in full delegation between authority attributes(AA) which independently make decisions on the structure &semantics of their attributes.

Rakesh Bobba et al[1], As more sensitive data is to be stored and shared by the third party, there will be need to be encrypt the data on the

ISBN: 978-981-07-6184-4

preferred sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). A new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In this cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. Hence KP-ABE technique is not applicable for all terms.

A. Sahai et al proposed the CP-ABEscheme[2], defines that in a distributed system, user needs to access the data only if the user is able to define the certain attributes. The method mainly involves in the trusted server, it is used to store the data and access control. Attributes are used to define the user's credentials, the encrypted data are used to determine the policy that who is going to decrypt. Previous ABE includes based on attributes, the encrypted data and the key are to be described. The disadvantage of the existing schemes are if any server which is used for storing data.if the store data is compromised,then the confidential data will also be compromised. The advantage of the CP-ABE defines that the encrypted data is kept confidential even if the storage server is untrusted. It also works against collusion attacks.

G.Wang et al proposed the HASBE scheme[5], which includes that cloud computing is a technology for the users to store and retrieve their data into a cloud. For small and medium sized enterprises with low budgets, the advantage is cost saving and high productivity by using cloud based services. In an enterprise user, cloud service provider need to take care of confidential data if the cloud service provider is not in same trusted domain. In the existing systems, the disadvantage is privacy issues and potential security needs to be raised. The advantages of keeping sensitive data against untrusted cloud service provider, the approaches are used in cryptography technique. The main advantage of the scheme is not only achieves for fine grained access control, but also provides high performance and scalability for an outsourced data. The disadvantage is

ISBN: 978-981-07-6184-4

keeping the data in a single trusted domain leads to be computational overhead. Hence the trusted domain is divided as sub authority for authentication.

EXISTING SYSTEM

To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key).

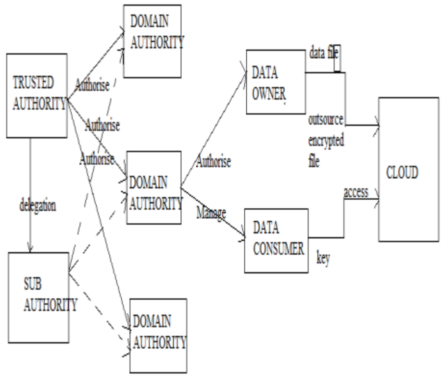
PROPOSED SYSTEM

The proposed system improves the efficiency and includes the delegation mechanism in HASBE for overcoming the computation overhead in a single trusted authority. User Revocation can update user's key by simply adding a new expiration value to the existing key. Delegation may involve in the forward of the authority to their sub authority. Delegation is done here to overcome the computation overhead in trusted authority.

The Delegation is the ability to deal with user's request under the trusted authority's permission. Here the subset of the authority acts as a server for the user. The user no need to wait for the authority until trusted authority gets freed, the request will be delegated to sub authorities when it is busy with other user'.

SYSTEM ARCHITECTURE

The process of the design implemented with the system architecture view comprises of the parts of the project work that encapsulates all modules ranging from module to module communication, setting initializations and system**.**



Architecture Diagram

The cloud computing system under consideration consists of five types of parties: a cloud service provider, data owners, data consumers, a number of domain authorities, and a trusted authority. The cloud service provider is to provide data storage service in a cloud. Data owners are mainly involves in encrypted data files and store them in the cloud for sharing. Data consumers download encrypted data files from the cloud and access the shared data files. A domain authority is managed by its trusted authority. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner. The trusted authority is the root authority and responsible for managing top-level domain authorities. Data owners/consumers may correspond to deal with an organization. In this system, neither data owners nor data consumers will be always online. They come online only when necessary, while the cloud service provider, the trusted authority, and domain authorities are always online.

Registration and Validation

A registration form can be used in several ways of information. The inserted database can be retrieved during the authentication of the user.

Creating the webpage includes the features and criteria's of the cloud. It determines the availabilities of the cloud.

User Revocation

To deal with user revocation in cloud computing, to add expiration time attribute for user's key. So that it can update user's key by adding a new expiration value to the existing key. It just needs a domain authority for the maintenance of some state information of the user keys and to avoid the generation and distribution of new keys. While updating the key, domain authority maintains some state information of user’s keys and assigns new value for expiration time to a user’s key.

Delegation

If the trusted authority is busy, the server forwards the authority to their sub authority in the hierarchical structure. Then the sub authority takes their priority to serve the files to the domain authority. Then the domain authority undergoes the validation to data owner. The data owner keeps the files in cloud in encrypted format where the data consumer decrypts the files and used.

CONCLUSION

The user needs the data to be confidential, even if the cloud service provider is untrusted. The data is to be in encrypted format while storing in the cloud. The existing techniques should not involve in the delegation of the trusted authority. The HASBE scheme provides improved performance of outsourced confidential data but lacks in its scalability and flexibility. To solve the computation overhead on the trusted authority or if it is busy with another user, the sub authority acts as a trusted authority for the specified user. The authorization has to be delegated for the sub authority to provide required information to the authorized user.

REFERENCES

1. V.Goyal, O.Pandey, A.Sahai, and B.Waters.,.“Attibute-based encryption for fine-grained access control of encrypted data,.” in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria [VA, 2006].

2. J.Bethencourt, A.Sahai, and B.Waters.“Ciphertext-policy attribute based encryption,.” in Proc. IEEE Symp. Security and Privacy, Oakland ,[CA, 2007].

3. R.Bobba, H.Khurana and M.Prabhakaran, .“Attribute-sets: A practically motivated enhancement to attribute-based encryption,.” in Proc. ESORICS, Saint Malo, France[2009].

4. Q.Liu G.Wang, and J.Wu.“Hierachical attibute-based encryption fine-grained access control in cloud storage services,.” in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago IL,[2010].

5. S.L.Lou, K.Ren, and Yu, C.Wang .“Achieving secure, scalable, and fine-grained data access control in cloud computing,.” in Proc. IEEE INFOCOM[2010],pp.534-542.