International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 4, July-Aug-2021, ISSN (Online): 2395-566X

GASBE: A Graded Attribute-Based Solution for Access Control in Cloud Computing

Piyush Kumar Jain, Prof. Rupali Bhartiya
Department of CSE
SVITS,Indore,India

***Abstract-* Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against un-trusted 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. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to un-trusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re- encryption, and lazy re-encryption.**

***Keywords*- Grade, Access control, cloud computing, data security.**

I. INTRODUCTION

Cloud computing is a delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility over a network. Cloud computing provides computation, software applications, data access, data management and storage resources without requiring cloud users to know the location and other details of the computing infrastructure. End users access cloud based applications through a web browser or a light weight desktop or mobile application while the business software and data are stored on servers at a remote location. Cloud application providers strive to give the same or better service and performance than if the software programs were installed locally on end-user computers.

Although cloud computing provides many exciting features for IT companies, academic researchers, and potential cloud users, security and data confidentiality should be considered. Due to Internet- based data storage and management, security has become a great concern. In cloud computing, users have to give up their data to the cloud service provider for storage and business operations, while the cloud service provider is usually a commercial enterprise which cannot be totally trusted [1]. Data is an important asset in any system and disclosure of data to business competitors and users leads to serious consequences. In addition to security, flexibility and fine-grained access control is strongly desired in the service-oriented cloud computing model. All these problems are defined and solution is provided in the proposed model.
In this paper we propose modified ASBE algorithm to with a hierarchical structure to improve scalability and flexibility in cloud system. The proposed model is GASBE (Graded Attribute-Based Solution) for flexible and scalable access control in cloud computing.

GASBE belong to SaaS systems. With these cloud computing sys-employs multiple value assignments for access expiration time. Also, enterprise users no longer need to invest in deal with user revocation more efficiently than existing schemes hardware/software systems or hire IT professionals to maintain. We formally prove the security of GASBE based on security of the ciphertext-policy attribute-based encryption (CP-ABE) scheme by this IT system, thus they save cost on IT infrastructure system.

II. RELATED WORK

This section deals with brief overview of ASBE (Attribute Based Encryption) scheme. Sahai and Waters describe a scheme (from here on referred to as SW) in which a sender can encrypt a message specifying an attribute set and a number d so that only a recipient who has at least d of the given attributes can decrypt the message. There is, however, one major limitation to the SW scheme. In their scheme, the user must go to a trusted party and prove his identity in order to obtain a secret key which will allow him to decrypt messages. In this case, each user must go to the trusted server, prove that he has a certain set of attributes, and then receive secret keys corresponding to each of those attributes. However, this means we must have one trusted server who monitors all attribute. In reality, we have 3 different entities responsible for maintaining this information.

ABE schemes are classified [2] into key-policy attribute-based encryption (KP-ABE) and cipher text-policy attribute-based encryption (CP-ABE).In KP-ABE model[3], when a user requests a private key, the authority determines what combinations of attributes must be present in order for this user to decrypt and gives the user the corresponding private key. CP-ABE is much more flexible than plain identity-based encryption, in that it allows complex rules specifying which private keys can decrypt which cipher texts. Specifically, the private keys are associated with sets of attributes or labels, and when we encrypt, we encrypt to an access policy which specifies which keys will be able to decrypt.

III. SYSTEM MODEL AND ASSUMPTIONS

1. System Model:

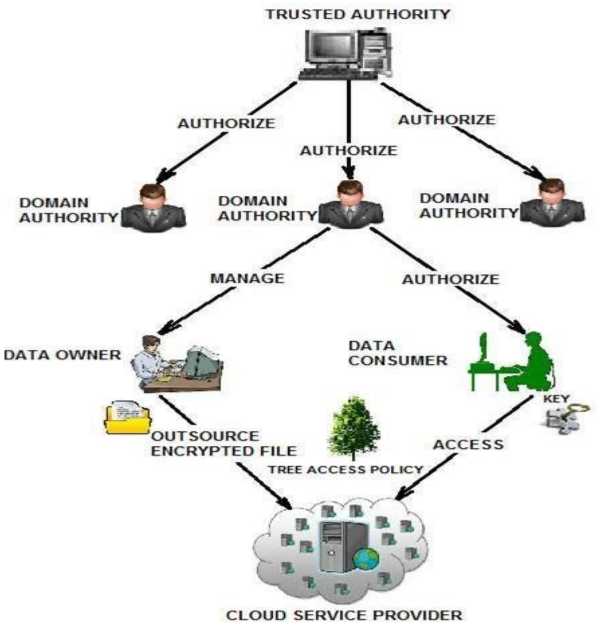

Fig 1. System Model.

Fig. 1 shows the designed model for the system. GASBE extends the ASBE algorithm with a graded structure to improve scalability and flexibility while at the same time inherits the feature of fine- grained access control of ASBE. Schemes employing attribute- based encryption (ABE) has been proposed for access control of outsourced data in cloud computing. On the one hand, the outsourced computation workloads often contain sensitive information, such as the business financial records, proprietary research data, or personally identifiable health information etc. Formal Security Model: Before giving a formal proof for the proposed scheme, combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing so as to provide end to-end data confidentiality assurance in the cloud and beyond. However, ordinary data encryption techniques in essence prevent cloud from performing any meaningful operation of the underlying plaintext data, making the computation over encrypted data a very hard problem. On the other hand, the operational details inside the cloud are not transparent enough to customers.

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. Each data owner/consumer is administrated by a domain authority. A domain authority is managed by its parent domain authority or the trusted authority. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner as shown in Fig. 1.

The trusted authority is the root authority and responsible for managing top-level domain authorities. Each top-level domain authority corresponds to a top-level organization, such as a federated enterprise, while each lower-level domain authority corresponds to a lower-level organization, such as an affiliated company in a federated enterprise. Data owners/consumers may correspond to employees in an organization. Each domain authority is responsible for managing the domain authorities at the next level or the data owners/consumers in its domain.

2. Security Model:

To combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing. so as to provide end to- end data confidentiality assurance in the cloud and beyond. However, ordinary data encryption techniques in essence prevent cloud from performing any meaningful operation of the underlying plaintext data, making the computation over encrypted data a very hard problem. On the other hand, the operational details inside the cloud are not transparent enough to customers. As a result, there do exist various motivations for cloud server to behave unfaithfully and to return incorrect results, i.e., they may behave beyond the classical semi hones model.

We assume that the cloud server provider is untrusted in the sense that it may collude with malicious users to harvest file contents stored in the cloud for its own benefit. In the hierarchical structure of the system users given in Fig. 1, each party is associated with a public key and a private key, with the latter being kept secretly by the party. The trusted authority acts as the root of trust and authorizes the top-level domain authorities. A domain authority is trusted by its subordinate domain authorities or users that it administrates, but may try to get the private keys of users outside its domain.

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. In addition, we assume that communication channels between all parties are secured using standard security protocols, such as SSL.

3. Access Structure:
To enforce this kind of access control, we utilize KP-ABE to escort data encryption keys of data files. Such construction enables us to immediately enjoy fine-grainedness of access control. Specifically; such an issue is mainly caused by the operation of user revocation, which inevitably requires the data owner to re-encrypt all the data files accessible to the leaving user, or even needs the data owner to stay online to update secret keys for users.

To resolve this challenging issue and make the construction suitable for cloud computing, we uniquely combine PRE with KP-ABE and enable the data owner to delegate most of the computation intensive operations to Cloud Servers without disclosing the underlying file contents. Such a construction allows the data owner to control access of his data files with a minimal overhead in terms of computation effort and online time, and thus fits well into the cloud environment. Data confidentiality is also achieved since Cloud Servers are not able to learn the plaintext of any data file in our construction.

For further reducing the computation overhead on Cloud Servers and thus saving the data owner’s investment, we take advantage of the lazy re- encryption technique and allow Cloud Servers to “aggregate “computation tasks of multiple system operations. As we will discuss in section V-B, the computation complexity on Cloud Servers is either proportional to the number of system attributes, or linear to the size of the user access structure/tree, which is independent to the number of users in the system.

Scalability is thus achieved. In addition, our construction also protects user access privilege information against Cloud Servers. Accountability of user secret key can also be achieved by using an enhanced scheme of KP-ABE.

4. GASBE Scheme:
The proposed GASBE scheme seamlessly extends the ASBE scheme to handle the hierarchical structure of system users [1] The trusted authority is responsible for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities domain authority is responsible for delegating keys to subordinate domain authorities at the next level or users in its domain. Each user in the system is assigned a key structure which specifies the attributes associated with the user’s decryption key. We are now ready to describe the main operations of GASBE: System Setup, Top-Level Domain Authority Grant, New Domain Authority/User Grant, New File Creation, User Revocation, File Access, and File Deletion.

5. Advantages of GASBE Scheme:

- Scalability
- Flexibility
- Fine-grained access control
- Efficient User Revocation
- Expressiveness

IV. SECURITY PROOF AND DISCUSSION

1. Security Proof:
In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, their methods are secure against collusion attacks.

Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user’s keys; while in their system attributes are used to describe a user’s credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC).

We introduce the concept of Distributed Attribute-Based Encryption (DABE), where an arbitrary number of parties can be present to maintain attributes and their corresponding secret keys. This is in stark contrast to the classic CP-ABE schemes, where all secret keys are distributed by one central trusted party. They provide the first construction of a DABE scheme; the construction is very efficient, as it requires only a constant number of pairing operations during encryption a nddecryption.

V. CONCLUSION

In our paper, we introduce the GASBE system for realizing accessible, stretchy, and fine-grained access control in cloud computing. The GASBE scheme faultlessly incorporates a graded structure of system users by applying a assignment algorithm to ASBE.

GASBE not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of element. We formally proved the security of GASBE based on the security of CP-ABE. We implement the proposed scheme, and conducted complete presentation analysis and estimate, which showed its efficiency and advantages over existing schemes.

REFERENCES

[1] HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE IEEE 2010.

[2] Multi-Authority Attribute Based Encryption, Melissa Chase Computer Science Department Brown University Providence, RI 02912 mchase@ cs.bro wn.edu.

[3] 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, 2016.