ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Taxonomy Attribute Set Based Authentication and Flexible Access Control for Cloud Storage

Ravindra.B. Pandit[1,] Ritesh Thakur[2]

M. E Student, Department of Computer Engineering, Institute of Knowledge College of Engineering, Shirur, Pune, Savitribai Phule Pune University, Pune, India.[1]

Professor, Department of Computer Engineering, Institute of Knowledge College of Engineering, Shirur, Pune, Savitribai Phule Pune University, Pune, India.[2]

ABSTRACT: Cloud computing is known as “Utility”. Cloud computing enabling users to remotely store their data in a server and provide services on-demand. Since this new computing technology requires user to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. We can increase security on access of the data in the cloud. However there are security concerns on outsourced data as the cloud servers are treated as untrusted. To overcome this problem many Attribute Based Encryption (ABE) techniques came into existence for secure access control. These techniques suffer from problems in implementing flexible access control mechanisms. A hierarchical attribute based solution which provides fine grained access control besides making it scalable. In this paper we implement this security scheme and build a prototype application that demonstrates the proof of concept. The empirical results revealed encouraging results.

KEYWORDS: Authentication, Third party audit, cloud storage, cloud service provider, Access control.

I. INTRODUCTION

Now a day’s cloud storage is gaining popularity due to it offers a flexible on-demand data outsourcing service with appealing benefits: relief of the burden for storage management, universal data access with location independence, On the need of sharing confidential corporate data on cloud servers, it is imperative to adopt an efficient encryption scheme with a fine-grained access control to encrypt outsourced data. Hierarchical Attribute Based Encryption, as one of the most promising encryption systems in this field, allows the encryption of data by specifying an access control policy over attributes, so that only users with a set of attributes satisfying this policy can decrypt the corresponding data. The hierarchical Attribute Set-Based Encryption (HASBE) scheme is for accessing control in cloud computing and extended the cipher text policy attribute set based encryption. Hierarchical Attribute Based Encryption security for data’s based on public key and master key with the help of Domain Authority Check.

II. PROBLEM STATEMENT

Cloud computing has emerged as one of the most important paradigms in the IT industry for last few years. In general data owners and service providers are not in the same trusted domain in cloud computing. Service providers should not be a trusted one anyhow they are all third party. The system focuses on a novel technique to Hierarchical Attribute Set Based Encryption (HASBE); it is driven by the Cipher Policy attribute-based encryption (CP-ABE) with a hierarchical structure of cloud users.

III. OJECTIVES

- To achieve scalability due to its hierarchical structure and also supports fine-grained access control in compound attributes of HASBE with high flexibility.

DOI: 10.15680/IJIRCCE.2016. 0405265

- To solve the user revocation problem in existing access control systems by assigning different expiration times.
- A ciphertext-policy attribute-based encryption (CP-ABE) is proposed to enforce access control of encrypted data.
- To achieve efficient user revocation time, the flexible multiple values attribute set combinations is used.

IV. RELATED WORK

In this section, we review the notion of attribute-based encryption (ABE), and provide a brief overview of the ASBE scheme by Bobba et al. After that, we examine existing access control schemes based on ABE. Attribute-Based Encryption The notion of ABE was first introduced by Sahai and Waters [17] as a new method for fuzzy identity-based encryption. The primary drawback of the scheme in [17] is that its threshold semantics lacks impressibility. Several efforts followed in the literature to try to solve the expressibility problem. In the ABE scheme, ciphertexts are not encrypted to one particular user as in traditional public key cryptography. Rather, both cipher texts and users' decryption keys are associated with a set of attributes or a policy over attributes. A user is able to decrypt a cipher text only if there is a match between his decryption key and the cipher text. ABE schemes are classified into key-policy attribute- based encryption (KP-ABE) and cipher text-policy attribute- based encryption (CP-ABE), depending how attributes and policy are associated with ciphertexts and users' decryption keys. In a KP-ABE scheme [12], a ciphertext is associated with a set of attributes and a user's decryption key is associated with a monotonic tree access structure. Only if the attributes associated with the ciphertext satisfy the tree access structure, can the user decrypt the ciphertext. In a CP-ABE scheme [14], the roles of ciphertexts and decryption keys are switched; the ciphertext is encrypted with a tree access policy chosen by an encryptor, while the corresponding decryption key is created with respect to a set of attributes. As long as the set of attributes associated with a decryption key satisfies the tree access policy associated with a given ciphertext, the key can be used to decrypt the ciphertext. Since users' decryption keys are associated with a set of attributes, CP-ABE is conceptually closer to traditional access control models such as Role-Based Access Control (RBAC) [14]. Thus, it is more natural to apply CP-ABE, instead of KP-ABE, to enforce access control of encrypted data. However, basic CP-ABE schemes (e.g., [14]) are far from enough to support access control in modern enterprise environments, which require considerable flexibility and efficiency in specifying policies and managing user attributes [16]. In a CP-ABE scheme, decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies. To solve this problem, Bobba et al. [16] introduced ciphertext-policy attribute-set-based encryption (CP-ASBE or ASBE for short). ASBE is an extended form of CP-ABE which organizes user attributes into a recursive set structure.

V. PROPOSED WORK

The objective of this work is to expand HASBE scheme is to realize scalable, supple, and fine grained access control in cloud computing. The HASBE method flawlessly integrates a hierarchical structure of scheme customers by concerning an allocation algorithm to ASBE. HASBE not only maintains compound attributes due to flexible attribute set combinations, but also attains efficient user revocation because of multiple value assignments of attributes. We properly proved the security of HASBE based on the security of CP ABE. To end with, we realized the suggested proposal, and accomplished complete performance analysis and evaluation, which demonstrated its effectiveness and benefits over obtainable schemes. The scope of the project is to build up a new computing technology necessitates users to hand over their precious data to cloud providers, thereby raising safety and confidentiality concerns on outsourced data.

Several methods utilizing attribute based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; though, most of them suffer from hardness in implementing complex access control policies. Even though the great profits brought by cloud computing paradigm are exciting for IT companies, academic researchers, and possible cloud users, security problems in cloud computing turn out to be serious obstructions which, devoid of being suitably addressed, will prevent cloud computing widespread applications and practice in the future. One of the famous safety concerns is data security and privacy in cloud computing due to its Internet based data storage and management. Users have to give up their data to the cloud service provider for storage and business operations in cloud environment, while the cloud service supplier is usually a commercial enterprise which cannot be totally trusted.

Data characterizes an extremely important asset for any group of organization, and endeavor users will face serious consequences if its confidential data is disclosed to their business competitors. Thus, cloud users in the first place want to make sure that their data are kept secret to outsiders, together with the cloud provider and their possible contestants. This is the first data security requirement.

VI. IMPLEMENTATION DETAILS

The main operations that we need to perform in this section are system setup, data owner grant, data user grant, generating new file, data integrity check, file access, availability check and file deletion.
For security purpose, the proposed scheme consists of 3 keys: Private, Public and Master key. Public key is used in encryption of data, Private and public key is used to decrypt the data and Master key is used for accessing the allowable data.

Setup (d): Here d is the depth of key structure. By taking input a depth parameter d. It gives a public key (PK) and master key (MK).

KeyGen (MK, u, A): By taking the input as master key (MK), user identity and attributes of key structure, it gives private key PRK for user u.
Encrypt (PK, M): By taking the public key (PK), and a message (M), as input. It outputs a cipher-text (CT).

Decrypt (CT, PRK): By taking cipher-text (CT) and private key of user (PRK) as input, it outputs a message (M). If the attributes associated with the user private key (PRK) matches with the access structure of cipher text (CT), then it outputs a message M which is the original correct message. Otherwise, m is null. The modules we consider to perform the above operations are Data Owner Module, Data Consumer Module, Cloud Server Module, Attribute based key generation Module

In our proposed system the cloud server supplier is untrusted in the sense that it may collude with spiteful users (short for data owners/data consumers) to yield file comfortable accumulated in the cloud for benefit. In the hierarchical structure of the system users, each party is related with a public key and a private key, with the latter being reserved clandestinely by the party. The conditioned authority acts as the root of trust and allows the top-level domain authorities. A domain authority is trusted by its lesser domain authorities or users that it controls, but may try to get the private keys of users outside its domain. Users may trying to access data files either within or outside the scope of their access privileges, so malevolent users may collude with each other to get sensitive files beyond the privileges. Implementation in detail as follow.

Step 1: This step can use current e-commerce or other services which have already securely verified the user's registration, such as symmetric key-based challenge and reply login verification, or through a One-Time Password.
Step 2: In this step, the CRM Service System transmits the user ID to the Storage Service System where it searches for the user's data. This data is encrypted so, once found, a request must be sent to the Encryption/Decryption Service System along with the user ID.
Step 3: It shows the Storage Service System executing the transmission of encrypted client data and the user ID to the Encryption/Decryption Service System.
Step 4: The Encryption/Decryption Service System uses the received user ID to index the user's data decryption key, which is then used to decrypt the received data. Using the correct decryption key to decrypt the data is critical to restoring the data to its original state.
Step 5: The decrypted client data is provided to the CRM Service System which then displays the client data to the user.
Step 6: The implementation of the Data Retrieval Program. Earlier to distribution the decrypted client data, the Encryption/Decryption Service System and the CRM Service System can launch a secure data transmission channel to securely broadcast the decrypted client data. After the decrypted client data is sent, the Encryption/Decryption Service System is not permitted to preserve the decrypted data and any unencrypted data must be deleted to avoid the encrypted data and the decryption key from being stored in the equivalent system. This is a critical factor in ensuring the privacy of user data.

Step 7: Retrieval process vice versa of the above process.

VII. SYSTEM MODEL

As mentioned in the model Fig.1 we are concerned to implement following main responsibilities: Data Owner, Data Consumer, Domain Authority, and Trusted Authority. User stores data on the cloud which can be retrieved by decrypting the same through a private key provided. This keeps the private data confidential

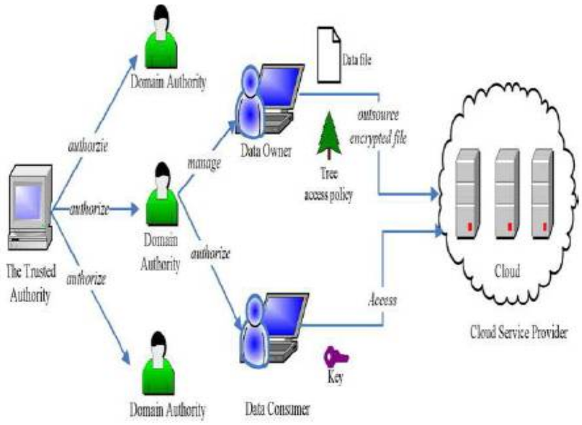

Fig 1. HASBE System Model

User gets that key he can access it like a password at the time of login. User will store all data by encryption public key and user can retrieve decrypted data which uses same public key and private key. After that, if user wants to see his own data then he uses the allotted private key and password. When manager wants to access employee's attribute then master key is used, which is generated by choosing the accessible attributes. If any lower authority is absent then higher authority is responsible for all work related to lower authority. When user is transferred from one location to another location, then all his data is updated in database itself. The manager will assign tasks and guide the employees working under him. Hence the management of assignment of tasks to employees should be done in a manner that is known to himself and respective employee with the permission of CEO in public domain. Also at the time of viewing of his personal information using private domain should be such that he could access it rather than some unauthorized user.

VI. SYSTEM OVERVIEW

HASBE provides flexibility, Scalability and Fine-grained access control with efficient user revocation .The Domain Hierarchy of the HASBE is very complex and there is no Sub-Domain Level user hierarchy that lead to system was showing complete data related to the requested query even though the employee required some of the data. Due to this, the time to fetch and execute the query was too long. This increased the system response time thereby degrading the system performance. There is also the data was encrypted but the decryption was not restricted to that specific user as keys were not distributed in an efficient way resulting in retrieval of wrong data or incomplete requested data thus increasing chances of hacking. Incase if a lower level authority is absent or is on leave, work is completely stopped and is delayed for the leave duration. Into the proposed system, we enhance Domain Hierarchy by creating Sub-domain for the user that reduces the complexity of the user level hierarchy. Here we are going to create the sub-domain inside the user level hierarchy based on the role of the user.it mean we are going to use role based strategy inside the hierarchy to create the sub-domain that's help at the time of data displaying phase .we can get only required data instead of entire data because of the sub-domain based on role. That's help to improve the system.

VII. RESULT AND DISCUSSION

RESULTS FOR EXPERIMENTAL CASES-

1. **Data Confidentiality** As we store the data in encrypted form on cloud, and keep the keys and the algorithm itself, unknown from Cloud server, it is next to impossible for the server to either learn the data or to misuse them.
2. **Security options** As all the data to be stored on Cloud may not be highly sensitive, we take inputs from the data owner himself, and accordingly select cryptographic algorithms for him.
3. **Lightweight Verification** For integrity verification, cloud user/requestor can send request (in form of challenge) to cloud server for computing and submitting hash code of his encrypted file. Upon checking some validations, cloud server computes a hash code of the file and returns the same to the requestor (in form of response). The size of this code is very small (in terms of few bytes) which reduces communication overhead. Also note that, computing the hash code is an offline function at cloud server side. In this way, we save computation plus communication time, hence improve performance.
4. **Key Management**
5. We have used the hybrid approach of using a combination of symmetric and asymmetric key encryption. Data encryption is done in a symmetric way and the key used for it is transferred to the data requester in an asymmetric way. Hence, utilizing secure approach for data encryption and fast operation for key transfer is adopted.
6. **Access Rights** Access rights can be granted from data owner to data requester with the help of small SQL grant operations. In case of revoking a grant, again the same kind of SQL revoke statement can be used. Important, thing here to mention is, in case of granting operation, data owner may be talking to data requester, but in case of revoking the rights, it will issue instructions directly to Cloud server, of course through SQL statement. Hence, it is quite a simple operation. We have provided some operational algorithms to offer an effective flexible security options using Modern symmetric encryption schemes which provide confidentiality based on sensitivity of user‘s data as well integrity verification with low computation cost on Client. TPA Auditing Manager generate a key pair using a public key encryption scheme in single Step which is used for encrypt the data during transmission.
7. **Public key sharing** public key sharing is handled with public key cryptography, to achieve faster performance and low computational overhead. In Last TPA Auditing Manager Analysis part this research compare the proposed model with some available approaches and from the analysis we can say the proposed model provides almost all the features which is required to make a complete solution.

VII. CONTRIBUTION

The contribution of the paper is multifold. First, we show how the HASBE extends the ASBE algorithm with a hierarchical structure to improve scalability and flexibility while at the same time inherits the feature of fine-grained access control of ASBE. Second, we demonstrate how to implement a full-fledged access control scheme for cloud computing based on HASBE. The scheme provides full support for hierarchical user grant, file creation, file deletion, and user revocation in cloud computing.

VIII. CONCLUSION

Thus, we efficiently provide a Domain level user Hierarchy and fine grained access control with flexibility and scalability with a hierarchical structure in our HASBE system. Our contribution to this paper will be providing security and reduce the complexity of the user level hierarchy by providing sub-domain level hierarchy. And there is also efficiently user revocation it’s also efficiently handle the access control when lower level of the authority is absent and update the data periodically when user move to one place to the other place.

REFERENCES

[1] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE ," HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing"in IEEE transection on information forensic and security ., vol. 7, no. 2, April 2012

[2] Sanchal Ramteke, Purva modi, Apurva Raghojiwar, Vijaya Karad, Prof.P.D. Kale.,"HASBE: Hierarchical Attribute based solution for flexible and scalable access control in cloud computing-in International Journal of Scientific and Research Publications, Volume 4, Issue 1, January 2014

[3] Rajanikanth aluvalu,lakshmi Muddana," A Survey on Access Control Models in Cloud Computing"-in Springer International Publishing, Advances in Intelligent Systems and Computing 337, DOI: 10.1007/978-3-319-13728-5_7.

[4] N.krishna. L.Bhavani," HASBE: A Hierarchical Attribute Set Based Encryption For Flexible, Scalable And Fine Grained Access Control In Cloud Computing-International Journal of Computer & Organization Trends –Volume 3 Issue 9 – Oct 2013.

[5] Md.Akram Ali, Ch.Pravallika, P.V.S. Srinivas," Multi-Attribute Based Access Control Policy Enforcement for File Accesses in Cloud"-in International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 5, September 2013

[6] John Bethencourt, Computer Sciences Department Carnegie Mellon University," Intro to Bilinear Maps"

[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption," inProc.EUROCRYPT, 2005, pp. 457473

[8] 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.

[9] J. Bettencourt, A. Sahai, and B.Waters"Ciphertext-policy attribute based encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007.

[10] Q. Liu, G. Wang, and J. Wu, "Time based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences .In Press, 2012.

[11] S. Gokuldev, 2S.Leelavathi 1Associate Professor, 2PG Scholar Department of Computer Science and Engineering SNS College of Engineering, Coimbatore, India," HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control by Separate Encryption/Decryption in Cloud Computing"-in International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013

[12] Zhibin Zhou and Dijiang Huang Arizona State University On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption

[13] Minu George1, Dr. C.Suresh Gnanadhas2, Saranya.K3," A Survey on Attribute Based Encryption Scheme in Cloud Computing"-in International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2013

[14] B. Raja Sekhar,B. Sunil Kumar, L. Swathi Reddy, V. PoornaChandar," CP-ABE Based Encryption for Secured Cloud Storage Access"-in International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September-2012

[15] Mauro José A. de Melo, Zair Abdelouahab," A STUDY OF ACCESS CONTROL IN CLOUD COMPUTING ENVIRONMENT" in International Journal of Computers & Technolog Volume 3 No. 3, Nov-Dec, 2012