IJDCST @Nov-Dec, Issue- V-3, I-1, SW-92
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Access control in Cloud Computing based on group key Management Policies

V. Mohan Krishna[1] , D.HariKrishna[2] , Dr. K. Rama Krishnaiah[3]

[1] Dept. of CSE, Nova College of Engineerng & Technology,Vijayawada,AP,India.

[2]Assistant Professor, Nova College of Engineerng & Technology,Vijayawada,AP,India.

[3] Professor & Principal, NVR College of Engineering and Technology, Tenali,AP,India.

ABSTRACT: Cloud File Storage requires users to entrust their valuable data to cloud providers. With respect to increasing security and privacy concerns on outsourced data in clouds, earlier several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; Later due to their inflexibility in implementing complex access control policies and to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, hierarchical attribute-set-based encryption (HASBE) with a hierarchical structure of users was developed. Although HASBE achieves scalability due to its hierarchical structure its expiration time model to deal with user revocation is not feasible practically because it reflects "One Size Fits All" approach which is quiet contradictory. Considering these facts we propose to implement a new scheme called broadcast group key management (BGKM) that uses dynamic key generation based on identity attributes and shared information instead of the expiration time model of HASBE. An implementation of the proposed scheme and shows that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing.

Index Terms: HASBE, ABE, BGKM, CP-ASBE.

2. INTRODUCTION

Cloud computing is another registering standard that is based on virtualization, parallel and dispersed registering, utility processing, and administration arranged structural planning [1]. In the last a few years, distributed computing has risen as a standout

amongst the most persuasive ideal models in the IT business, and has pulled in far reaching consideration from both the scholarly world and industry, Cloud processing holds the guarantee of giving registering. Access control is a fantastic security theme which goes once again to the 1960s or early 1970s [4], and different access control models have been proposed from that point forward. Among them, Bell-La Padula (BLP) [5] and BiBa [6] are two acclaimed security models.

In this paper, we propose various attribute property set-based encryption (HASBE) plan for access control in distributed computing. HASBE broadens the cipher-text approach property set-based encryption (CP-ASBE, or ASBE for short) conspire by Bobba et al. [9] with a various leveled structure of framework clients, to accomplish adaptable, flexiblem and fine-grained access control.

3 REVIEWS ON LITERATURE

In this section, we survey the thought of trait based encryption (ABE), and give a short diagram of the ASBE conspire by Bobba et al. After that, we analyze existing access control plans focused around ABE.

1. Attribute-Based Encryption

The thought of ABE was initially presented by Sahai and Waters [10] as another system for fluffy character based encryption. The essential downside of the plan in [10] is that its edge semantics needs expressibility.

{Dept : CS,Role : Grad – Student,
{CourseID : 101,Role: TA},
{CourseID : 525, Role : Grad – Student}}.

Example for representing a key structure

The above sample speaks to a key structure appointed to a graduate understudy in CS division of a college, who is the TA for course 101 and has selected in course 525. It can be seen that the same property can be doled out different qualities, e.g., the quality "Part" is appointed worth "TA" and "Graduate Student" in diverse sets. This peculiarity renders ASBE more adaptable and adaptable in supporting numerous reasonable situations. In this illustration, the graduate understudy holding such a private key ought not have the capacity to join the trait "Part: TA" with "CourseID: 525" in order to get to course evaluations of different understudies who select in course 525. Such a peculiarity can't be actualized with the first CP-ABE calculation.

2. Access Control Solutions for Cloud Computing

The customary technique to secure touchy information outsourced to outsiders is to store scrambled information on servers, while the unscrambling keys are unveiled to approved clients just. Next, this methodology needs versatility and adaptability; as the quantity of approved clients gets to be huge, the arrangement won't be effective any longer. ABE turns out to be a good technique for realizing scalable, flexible, and fine-grained access control solutions [7].

System Model and Assumptions

As portrayed in Fig. 1, the distributed computing framework under thought comprises of five sorts of gatherings: a cloud administration supplier, information managers, information shoppers, various space powers, and a trusted power.

Fig 1: System model.

4. EXISTING SYSTEM

Uses web applications driven with cloud architecture, Uses SAAS based cloud computing applications over web that acts as a cloud server. The client is definitely user's browser, Cloud users in the first place want to make sure that their data are kept confidential to outsiders, including the cloud provider and their potential competitors. This is the first data security requirement. Data confidentiality is not the only security requirement. Flexible and fine-grained access control is also strongly desired in the service-oriented cloud computing model. For example a health-care information system on a cloud is required to restrict access of protected medical records to eligible doctors only. And as another example a customer relation management system running on a cloud may allow access of customer information to high-level executives of the company only. This kind of approach is called a flexible and fine grained access.

To achieve flexible and fine-grained access control, a number of following schemes have been proposed more recently. They are: Principles of policy in secure groups-(Reference paper 12),Security policy reconciliation methods-(Reference paper 13), Unified schemes for resource protection in automated trust negotiation-(Reference paper 14), Automated trust

negotiation using cryptographic credentials- (Reference paper 15).

PROBLEM FORMULATION

Unfortunately, these schemes are only applicable to systems in which data owners and the service providers are within the same trusted domain. Since data owners and service providers are usually not in the same trusted domain in cloud computing, a new access control scheme employing attributed-based encryption is proposed, which adopts the so-called key-policy attribute-based encryption (KP-ABE) or cipher text-policy ABE (CP-ABE) to enforce fine-grained access control. List of some of the major key attributes of cloud computing are as follows.

1. Cloud computing offerings are services, not products
2. Cloud computing allows customers to increase and decrease the number of users that have access to services, exponentially
3. Cloud computing allows customers to provision new services to users instantly or within hours
4. Cloud computing turns computing resources into operational expenses rather than capital expenditure
5. Cloud computing enables organizations to pay for computing resources based on consumption of the resources in question
6. Cloud computing allows multiple, diverse customers to share computing resources
7. Cloud computing service enhancements, such as updates, are automatic
8. Cloud computing resources can be accessed using any Internet-enabled device, from any location
9. Cloud computing integrates security into services
10. Cloud computing eliminates the need for support contracts
11. Cloud computing costs less than on-premise alternatives

12 Cloud computing allows the purchase of services without human interaction

13. Cloud computing integrates automatic backup into services
14. Cloud computing services are delivered from remote locations
15. Cloud computing services are delivered by a third party
16. Cloud computing services are delivered via the Internet or via an IP VPN

However, these schemes falls short of flexibility in attribute management and lacks scalability in dealing with multiple-levels of attribute authorities and have complicated expressions while describing access policies. So a better is required to initiate attribute based security policies.

4 PROPOSED SYSTEM

Uses web applications driven with cloud architecture, Uses SAAS based cloud computing applications over web that acts as a cloud server. Proposes a hierarchical attribute-set-based encryption (HASBE) scheme for access control in cloud computing. HASBE extends the cipher text-policy attribute-set-based encryption (CP-ASBE, or ASBE for short) scheme with a hierarchical structure of system users, so as to achieve scalable, flexible and fine-grained access control. HASBE extends the ASBE algorithm with a hierarchical structure in such a way that it improves scalability and flexibility while at the same time retaining the features of fine-grained access control of ASBE which is quiet efficient. The scheme provides full support for hierarchical user grant using Tree access policies, file creation, file deletion, and user revocation in cloud computing that is not available in earlier approaches. Compared to earlier approaches this scheme has a lesser computation overhead.

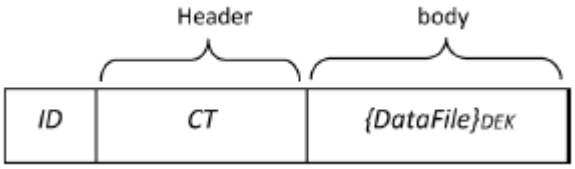

Fig 2: Format of a data file on the cloud.

Thus, HASBE is expected to have the same security property as CP-ABE, which has been proven to be secure under the generic bilinear group model and the random oracle model.

Performance Analysis

We analyze the computation complexity for each system operation in our scheme as follows.

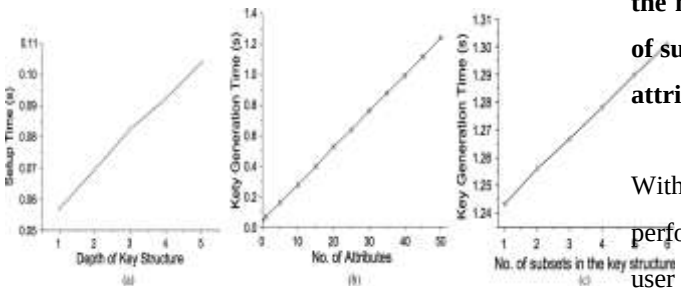

Fig 3: Experiments on system setup and top-level domain authority grant. (a) Setup operation; (b) top-level domain authority grant (the number of subsets in the key structure is 1); (c) top-level domain authority grant (the total number of attributes in the key structure is 50).

IMPLEMENTATION

We have implemented a multilevel HASBE toolkit based on the toolkit (http://acsc.csl.sri.com/cpabe/) developed for CP-ABE [8] which uses the Pairing-Based Cryptography library (http://crypto.stanford.edu/pbc/). Then comprehensive experiments are conducted on a laptop with dual core 2.10-GHz CPU and 2-GB RAM, running Ubuntu 10.04. We make an analysis on the experimental data and give the statistical data. Similar to the toolkit, our toolkit also provides a number of command line tools [8].

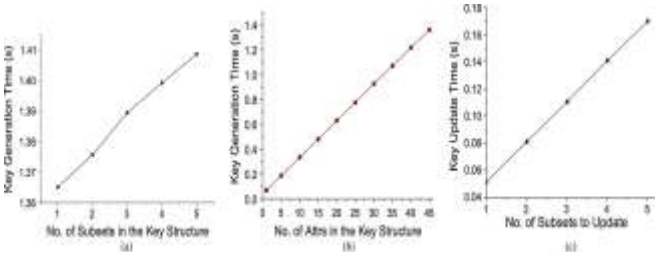

Fig 4: Experiments on new user/domain authority grant and key update. (a) New user/domain authority grant (the total number of attributes in the master secret key of DA is 50 and the total number of attributes is 45); (b) new user/domain authority grant (the total number of attributes in the master secret key of DA is 50 and the number of subsets is 1); (c) key update (the total number of attributes in the original private key is 50).

With the command , a domain authority DA can perform *New User/Domain Authority Grant* for a new user or another domain authority in his domain. The cost depends on the number of subsets and attributes to be delegated. Assume the domain authority DA has a private key with 50 attributes.

the cost grows linearly with the number of subsets to be delegated as shown in Fig. 4(a), the cost also increases linearly with the number of attributes in the subset as in Fig. 4(b), the cost is linear with the number of the subsets, as shown in Fig. 4(c).

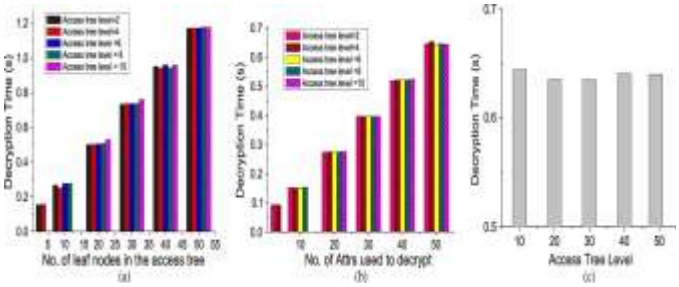

Fig 5: Experiments on file creation and decryption. (a) Encryption/new file creation; (b) decryption/file access (there is 1 subset with 50 attributes in the private key);

(c) decryption/file access (there is 1 subset with 50 attributes in the private key and the number of attributes used for decryption is 50).

Prior approaches are to encrypt documents satisfying different policies with different keys using a public key cryptosystem such as hierarchical attribute-set-based encryption (HASBE).

Limitations of HASBE are:

- It cannot efficiently handle dynamic adding/revoking users or identity attributes, and policy changes;
- It requires keeping multiple encrypted copies of the same documents; that incurs high computational cost for cloud service provider.

Without utilizing public key cryptography and by allowing users to dynamically derive the symmetric keys at the time of decryption, we can address the above issues. We propose to implement a new key management scheme called broadcast group key management (BGKM). The idea of BGKM is to give some secrets to users based on the identity attributes they have and later allow them to derive actual symmetric keys based on their secrets and some public information.

A key advantage of the BGKM scheme is that adding users/revoking users or updating access control policies can be performed efficiently by updating only some public information. This is an efficient approach for fine-grained encryption based access control for documents stored in a cloud file storage server.

CONCLUSION:

To increasing security and privacy concerns on outsourced data in clouds, earlier several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; Later due to their inflexibility in implementing complex access control policies and to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, hierarchical attribute-set-based encryption (HASBE) with a hierarchical structure of users was developed. Its hierarchical structure its expiration time model to deal with user revocation is not feasible practically because it reflects “One Size Fits All” approach which is quiet contradictory, we propose to implement a new scheme called BGKM that uses dynamic key generation based on identity attributes and shared information instead of the expiration time model of HASBE, An implementation of the proposed scheme and shows that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing.

REFFERENCES:

[1] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, “Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility,” *Future Generation Comput. Syst.*, vol. 25, pp. 599–616, 2009.

[2] Amazon Elastic Compute Cloud (Amazon EC2) [Online]. Available: http://aws.amazon.com/ec2/

[3] Amazon Web Services (AWS) [Online]. Available: https://s3.amazonaws.com/

[4] A. Ross, “Technical perspective: A chilly sense of security,” *Commun.ACM*, vol. 52, pp. 90–90, 2009.

[5] D. E. Bell and L. J. LaPadula, Secure Computer Systems: Unified Exposition and Multics Interpretation The MITRE Corporation, Tech. Rep., 1976.

[6] K. J. Biba, Integrity Considerations for Secure Computer Sytems The MITRE Corporation, Tech. Rep., 1977.

[7] S. Yu, C. Wang, K. Ren, and W. Lou, "Achiving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE INFOCOM 2010*, 2010, pp. 534–542.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Security and Privacy*, Oakland, CA, 2007.

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

[10] A. Sahai and B. Waters, "Fuzzy identity based encryption," in *Proc. Acvances in Cryptology—Eurocrypt*, 2005, vol. 3494, LNCS, pp. 457–473.

About Authors:

I am V. Mohan Krishna, pursuing my Mtech in Nova College of Engineering & Technology, Vijayawada. My Interest are research in Software Engineering & Data mining.

Mr. Hari Krishna.Deevi is a qualified persion Holding M.Sc(CSE) & M.Tech Degree in CSE from Acharya Nagarjuna university, He is an Outstanding Administrator & Coordinator. He is working as an Assistant Professor in NOVA College of Engineering Technology .He guided students in doing IBM projects at NOVA ENGINEERING College. Who has Published 10 research Papers in various international Journals and workshops with his incredible work to gain the knowledge for feature errands.

Dr. K. Rama Krishnaiah is a highly qualified person, an efficient and eminent academician. He is an outstanding administrator; a prolific researcher published 33 research papers in various International Journals and a forward looking educationist. He worked in prestigious K L University for 11.5 years and he contributed his service for NBA accreditation in May 2004, Aug 2007 with 'record rating', ISO 9001:2000 in 2004, Autonomous status in 2006, NAAC accreditation of UGC in 2008 and University status in 2009. Later on he worked as Principal at Nova College of Engineering and Technology, Vijayawada for a period of 3.5Yrs. He took charge as the Principal, NVR College of Engineering and Technology, Tenali in May 2014.