Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Hierarchical CP-ASBE Scheme in Cloud Computing for fine-Grained Access Control with Scalability and Flexibility

V. S. Dhumal
Student of M.E [Computer]
In RMD Sinhgad School of Engineering,
Pune University, Maharashtra, India

Prof. D. N. Rewadkar
Associate Professor & Head Of Department
in RMD Sinhgad School of Engineering,
Pune University, Maharashtra, India

Abstract— Cloud computing has widespread use in IT industry. Many Companies like Google, Microsoft, and IBM uses cloud to deliver services to its users because of its reliability, scalability and remote access. A cloud service provider (CSP) is an entity in cloud computing, associated with the Organization has different roles and capabilities. A cloud service provider is limited to organization so it's vulnerable to attacks. When requested data from the user is retrieved from CSP, Organization needs to secure their data & CSP. Access to CSP should be flexible so that it can adapt the different conditions easily. To maintain data integrity on CSP, Attribute based encryption (ABE) with KP-ABE and CP-ABE can be used with access control implementation for cloud computing. But these schemes also lack of scalability and flexibility so CP-ASBE scheme is described. A review of the all fine grained access control solution is presented. Existing system suffers from system performance, Data Security and flexible access control. A Hierarchical Attribute set-based-encryption scheme is proposed to deal with the issues in the existing system to achieve fine grained, flexible and scalable access control.

Keywords— Cloud service provider (CSP), Attribute based encryption, Attribute set-based-encryption, fine grained access control, Scalable access control, HASBE

I. INTRODUCTION

Cloud computing is a model where user access computing resources and applications being delivered in the internet cloud remotely. Configurable computing resources like servers, networks, services etc. are efficiently used with the help of cloud service provider (CSP). Cloud computing has widespread use in IT industry. Many Companies like Google, Microsoft, and IBM uses cloud to deliver services to its users. The characteristics of cloud computing include reliability, scalability, remote access. Cloud-based communications services are deployed using deployment models like a private cloud of any organization, public cloud available on the internet and Hybrid cloud providing the combined services from private and public cloud which is shown in Fig 1, which enable businesses to integrate it into various business applications. After establishing the cloud its computing services are deployed in terms of business model. The Fig 2 represent these service models with example.

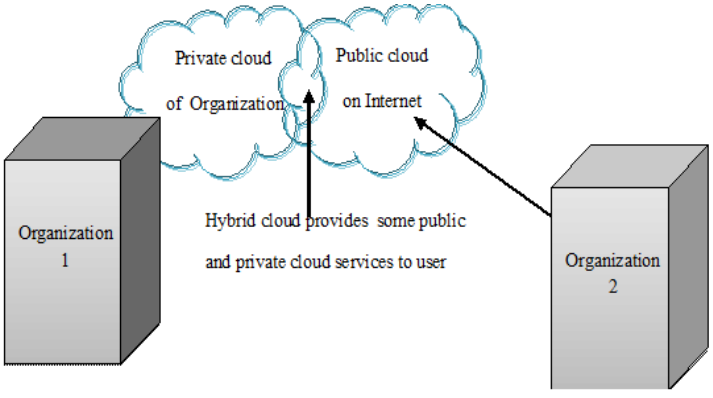

Fig 1. Deployment Models for Cloud Computing

The Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) are primary service models.

• **Software as a Service (SaaS)** — Here interaction between the consumer and the service is hosted as part of the service in the cloud. Salesforce's Customer Relation Management (CRM) System is SaaS System.

• **Platform as a Service (PaaS)** — Here consumer can deploy their own software's and applications in the cloud. Google App Engine [2] and Yahoo Pig are representatives of PaaS systems.

• **Infrastructure as a Service (IaaS)** — in this service model consumer can control and manage the system but they can't control the infrastructure of the cloud. Amazon's EC2 [3], Amazon's S3 [4], and IBM's Blue Cloud [5] are Iass Systems.

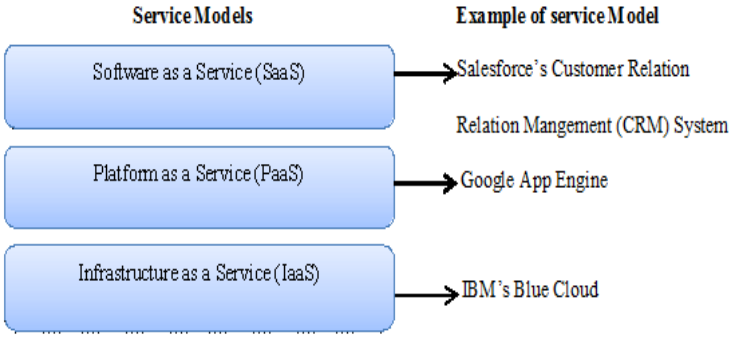

Fig 2. Service Models for Cloud Computing

II. BACKGROUND

Data security and Privacy in cloud computing is the main Security concern as cloud computing's data storage is based on internet. This data management is done by the Internet cloud service provider via the internet only. A cloud service provider is an entity in cloud computing which take data from the users so that data will be stored & utilized for a variety of applications including various areas like business, Education etc. Cloud service provider (CSP) is associated with the Organization. The organization can define the roles and capabilities of it. An organization can decide what kind of services should be provided by the cloud service provider. A cloud service provider is limited to organization so it's vulnerable to attacks. When requested data from the user is retrieved from CSP, Organization needs to secure their data & CSP . Access to CSP should be flexible so that it can adapt the different conditions easily. The organization can define an access control policy which defines a mapping between the authorized Groups and secure actions in the organization.
For flexible and fine grained access control Bell-La Padula have proposed an access control model having three major facets--a descriptive capability (the elements), general mechanisms (the limiting theorems), and specific solutions (the rules). The model assumes the different modes which are called as access attributes [6]. K.J. Biba has explicitly addressed the Integrity protection problem with the solution of Access control policies providing effective protection were identified for each [7]. P. D. McDaniel and A. Prakash has presented a model and language for the specification and reconciliation of security policies. Policy in this model defines interdependent statements of provisioning (session configuration) and authorization [8]. T. Yu and M. Winslett has proposed UniPro, a Unified Resource Protection Scheme to give access control policies providing the protection needed during trust negotiation [9]. J. Li, N. Li, and W. H. Winsborough defined automated trust negotiation (ATN) which supports the combined use of several cryptographic credential schemes and protocols to provide capabilities that are useful in various negotiation scenarios [10].
But drawback of these entire proposed schemes is that, it is limited to service providers and Data source within the same Authorized domain. Cloud computing generally has Data source and Service provider from different domains; Vipul Goyal *et al* has proposed the attribute based encryption [11]. It uses key-policy attribute based encryption (KP_ABE) to enforce fine-grained access control. But this scheme also has the limitation of flexibility and lack of scalability. Brent Waters *et al* introduced Ciphertext-Policy Attribute Encryption (CP-ABE) under concrete and non-interactive cryptographic assumptions in the standard model [12].

Hierarchical attributes-set-based encryption (HASBE) proposed by Zhiguo Wan *et al* is extended version of CP-ABE & ASBE. In this scheme users can be arranged hierarchically to achieve fine-grained access control [1].

III. RELATED WORK

As cloud based applications and data is managed by the internet. To maintain data integrity all data can be stored in encrypted format. But Encrypted data limit the user accessibility at a fine grained level. To overcome this problem Sahai and Waters [12] introduced the concept of Attributed-Based Encryption (ABE). In an ABE system, Ciphertexts are not encrypted to one particular user. With the ABE system Ciphertext & user's decryption keys are associated with a set of attributes. A user is able to decrypt a Ciphertext only if there is a match between the user's decryption key and the Ciphertext. A user's keys and Ciphertexts are labeled with sets of descriptive attributes and a particular key can decrypt a particular Ciphertext only if there is a match between the attributes of the Ciphertext and the user's key. This ABE system is extended in two forms based on the policy adopted for encryption.

A. KP-ABE: Key-policy attribute-based encryption

This system uses a set of descriptive attributes and each Ciphertext is labeled by the Encryptor. An access structure associated with Each private key specifies which type of Ciphertext the key can decrypt. As the private key specifies the access structure & Ciphertext is associated with a set of attributes, this scheme is called as a Key-Policy Attribute-Based Encryption (KP-ABE).

In KP-ABE tree access structure user's decryption key is associated with it. The tree where the intermediate nodes are associated with the attributes. A user is able to decrypt a Ciphertext if the attributes associated with a Ciphertext satisfy the key's access structure [13].

B. CP-ABE: Ciphertext-policy attribute-based encryption

In this scheme, the roles of Ciphertext and decryption keys are exactly opposite to their roles defined in KP-ABE scheme. Here Ciphertext is encrypted with a tree access policy & decryption key is created with a set of attributes [1].

But as many organization's data is shared on CSP to provide flexibility in access, CP-ABE has some limitations under some issues. The first issue is regarding performance, the encryption system used to store data degrade system's high performance due to remote access of the user. For big scale organization an authorized group is responsible for the decryption key management of user which make decisions independent of the structure and semantics of the attributes of the users. Also this has a lack of support to the dynamic revocation of user which leads to the huge storage of decryption keys which leads lack of flexibility.

C. CP-ASBE: Ciphertext-policy attribute set based encryption

In The above mentioned CP-ABE scheme decryption key has support to known attributes arranged in some logical order in only one set. So users can use all possible combinations of the attributes from the single set itself to satisfy Ciphertext policy. To deal with this drawback, Bobba *et al* Ciphertext attributes set encryption scheme is introduced. This organizes user attributes into a recursive set structure [14].

{Employee: Ifica, Post: Auditor, Business Analyst,
{Project Id: 121, Post: Auditor }
{Project Id: 230, Post: Business Analyst}}

The above example represents the recursive employee structure of depth 2, One Employee of Ifica Company can be Auditor for ProjectId 121 and he can be also work as a Business Analyst for ProjectId 230. So a single attribute "Post" can be assigned to multiple values. So from the above example we can say that ASBE support flexibility.

ASBE can enforce dynamic constraints on combining attributes to satisfy a policy which results in greater flexibility in access control. As a recursive attribute set is assigned to a user in the ASBE scheme, attributes from the same set can be easily combined, while attributes from different sets can only be combined with the help of translating items using ASBE. This problem can be solved simply by assigning multiple values of the group of attributes in different sets. Existing ABE schemes are not suitable for some applications where efficient ciphertext policy encryption of ABSE is more effectively used. ASBE's capability of assigning multiple values for the same attribute enables it to solve the user revocation problem efficiently, which is difficult in CP-ABE [1].

D. Review of Fine-grained Access Control Solutions

As data security of a Cloud Service Provider is the prime concern of any organization. To secure information cryptography can be effectively used, in which all data on CSP will be stored in the encrypted format. But encryption of all available data can degrade the system performance and also it needs trusted key management system. Here review of the three proposed schemes for fine-grained access solution is described.

I. KP-ABE: Key-policy attribute-based encryption access control solution

Shucheng Yu *et al* solved the above mentioned problems to achieve fine grained access by a combined system between key policy attribute-based encryption (KP-ABE), Proxy encryption (PRE) and lazy re-encryption [15].

In this system they have assumption that every user in the system has their own pair of public-private keys. This key pair is used as a digital signature for ensuring authentication, non-repudiation and integrity. Using keys users can validate the authorized data. With the help of private-public key encryption communication can be effectively done between communicating parties. In the proposed system by Shucheng Yu *et al* a fine grained access control is achieved by KP-ABE. Here KP-ABE encrypt each file with a symmetric data encryption key (DEK) then public key associated with the set of attributes is used to encrypt it. The encrypted data encryption key and the set of attributes of KP-ABE are stored with the encrypted data file. The users can decrypt the encrypted data file only, if they able to decrypt the encrypted DEK. Though this system achieves scalability but also suffer from the problem of deciding exactly who will decrypt the data. So it's not suitable for some applications where many users are included with different attributes.

II. HABE: Hierarchical attribute-based encryption access control solution

Guojun Wang *et al* proposed a scheme by combining the hierarchical identity-based encryption (HIBE) system and the ciphertext-policy attribute-based encryption (CP-ABE) system applying proxy re-encryption and lazy re-encryption to provide fine-grained access control and full delegation [16]. This system assumes that, "All attributes in one conjunctive clause are administrated by the same domain master". So multiple domain masters (DMs) administer the same attribute according to specific policies, which is practically difficult to implement. Also HABE also have limitation as it does not support multiple value assignments & compound attributes.

III. HASBE: Hierarchical attribute-set-based encryption access control solution

Zhiguo Wan *et al* proposed the HASBE scheme for implementing scalable, flexible and fine-grained access control in cloud computing. The HASBE scheme includes a hierarchical structure of system users by applying a delegation

algorithm to ASBE. Because of flexible attribute set combinations HASBE supports compound attributes. Using multiple value assignments of attributes HASBE also achieves efficient user revocation. [1].

IV. EXISTING SYSTEM

In general user sends the request to CSP for information retrieval as shown in Fig 3. But data need of every user request depends on their requirement. So it's not flexible to provide access to the whole data. If full access right is granted to every user for complete data it will take too much time to execute that query and fetch all data. Due to that system response time will increase which will effect on system performance. In the existing system if malicious user hack the server, there may be chances for data easily understood by hackers.

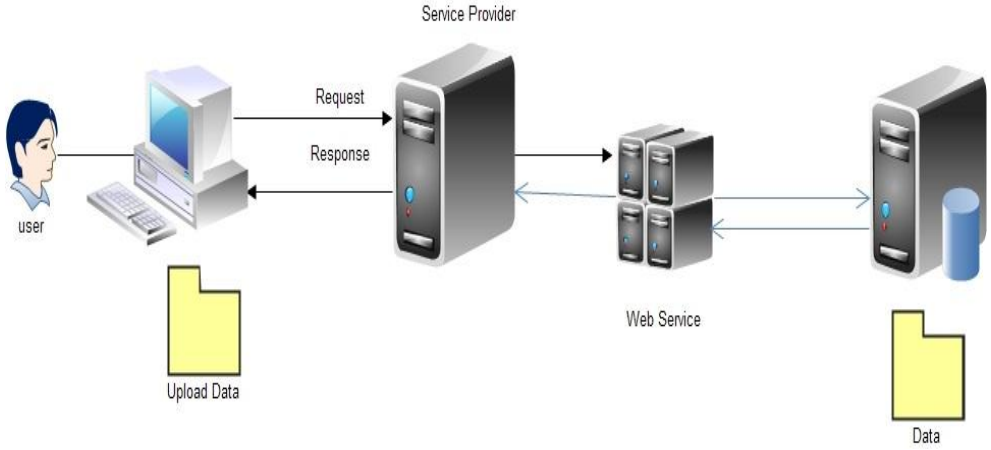

Fig 3. The typical scenario to access information using cloud service provider

V. PROPOSED SYSTEM

To deal with the existing system problem organization can be divided among different groups and access rights can be assigned to the user according to their role in organization. By doing this flexibility can be achieved while accessing the information. Encryptor is the entity within the proposed system which upload data in the Encrypted HASBE Cloud service provider. Encryption of the data is performed to maintain data security. Along with the encryption it can modify encrypted files and assign the access rights to file according to the role of the user in the system. It specifies the ciphertext policy. The user is administrated by Authorized Administrator. Only authorized user can access data file using encrypted key. Authorized Administrator grants the privileges to the user to access data. Encrypted HASBE Cloud Service Provider is the cloud data storage of encrypted data files. These files are shared for access among the users. Only authorized user access data by downloading encrypted files and decrypt it from Encrypted HASBE Cloud Service Provider. Authorized Administrator is the main authority responsible for administration of user and Encryptor. It distributes the decryption keys to the users according to the key structure of the user. The key structure attributes assigned to the user specifies User's decryption key attributes.

In our proposed system we will use hierarchical CP-ASBE structure. So instead of providing access to complete data, users will be allowed to fetch only that data which is essential and according to their role in organization. We will not fetch all data so it takes less time for fetching data. So system response time is very less due to which system performance is increased. We will perform encryption before storing data so even if data get hacked by hacker data cannot be easily understood by hackers.

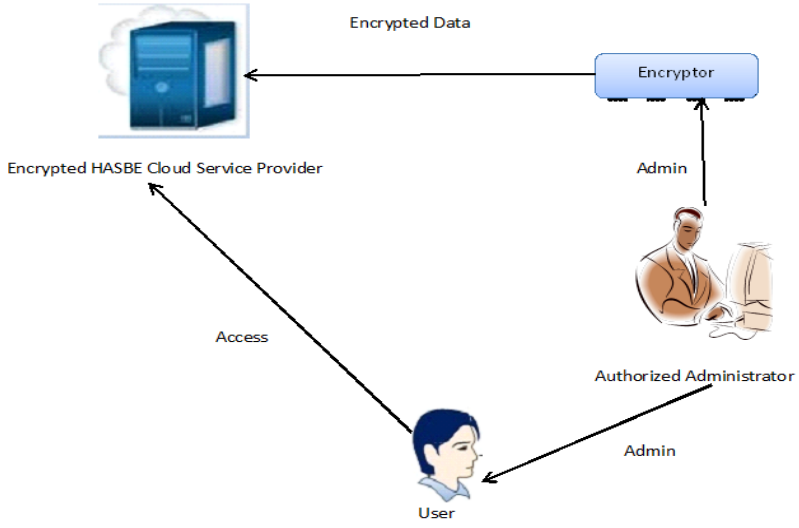

Fig 4. Proposed system model of HASBE Cloud Service Provider

VI. CONCLUSION

Cloud computing is a model where user access computing resources and applications being delivered in the internet cloud remotely. A cloud service provider is an entity in cloud computing which take data from the users so that data will be stored & utilized for a variety of applications including various areas like business. An organization needs not only to secure their data & Cloud service provider but also it should provide flexible access to CSP so that it can adapt the different conditions easily. Here to maintain data integrity ABE, KP-ABE, CP-ABE, CP-ASBE schemes are discussed with their strengths cons and pros. Different fine grained access control solutions are discussed here. In this paper, Hierarchical CP-ASBE scheme is proposed to address issues of data security, system performance and flexible access to the cloud service provider (CSP) of the existing system.

REFERENCES

[1] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", in *IEEE Transactions on information forensics and security, Vol. 7, No. 2,* in April 2012

[2] Google App Engine [Online]. Available: http://code.google.com/ appengine/

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

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

[5] R. Martin, "IBM brings cloud computing to earth with massive new data centers," *InformationWeek* Aug. 2008 [Online]. Available:http://www.informationweek.com/news/hardware/data_centers/209901523

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

[7] K. J. Biba, "Integrity Considerations for Secure Computer Systems", *The MITRE Corporation, Tech. Rep.,* 1977.

[8] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," *in Proc. IEEE Symp. Security and Privacy, Berkeley, CA,* 2002.

[9] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," *in Proc. IEEE Symp. Security and Privacy,Berkeley, CA,* 2003.

[10] J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials," in *Proc. ACM Conf. Computer and Communications Security (CCS),* Alexandria, VA, 2005.

[11] 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.

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

[13] 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.

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

[15] 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.

[16] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," *in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago,IL,* 2010.

