A Brief Survey on Encryption Schemes in Cloud Environments

S.M. Hema Latha [#1], S.Ganesh[*2],
[#1]ME(CSE), *[2] Assistant Professor
Fatima Michael College of Engineering and Technology

Abstract*—For the last two years cloud computing is a important in the IT industry. In cloud computing data owners and service providers are not in the same trusted domain so the Service providers should not be a trusted one and they are all third party.It focuses on a technique to Hierarchical Attribute Set Based Encryption (HASBE); it is proposed by the Cipher Policy attribute-based encryption (CP-ABE).It achieves both flexibility and fine-grained access control of data in cloud not only the scalability. It stores the data in encrypted form for privacy protection. Cloud system is responsible for both tasks on storage and encryption or decryption of data. In this paper I provide a technique called Hierarchical Attribute set based Encryption(HASBE) to give security and fine grained access control to the users of cloud computing . It was an enhancement for the technique called Attribute based Encryption(ABE) which is inflexible to handle complex control.*

Keywords: *Cipher Policy attribute-based encryption (CP-ABE), Hierarchical Attribute Set Based Encryption (HASBE), Cloud Computing.*

I. INTRODUCTION

Cloud Computing has become a significant technology that delivers dynamically scalable IT resources over the internet[1]. Cloud Computing is popular because of its infrastructure that is in the form of a cloud. Presently users are interested to access a content independently through internet rather than accessing in their own systems. It provide independent access by storing data in a cloud. This infrastructure of a cloud consists of cloud service providers who provides cloud to store the data and consumers who upload the data and can download from anywhere and by using any supporting device. Some of the advantages of Cloud Computing are it reduces cost expenditure by providing some services and also reduces complexity and maintenance with less operational risk, scalability and flexibility.

Several service-oriented cloud computing models have been proposed.

Infrastructure-as-a-Service(IaaS)

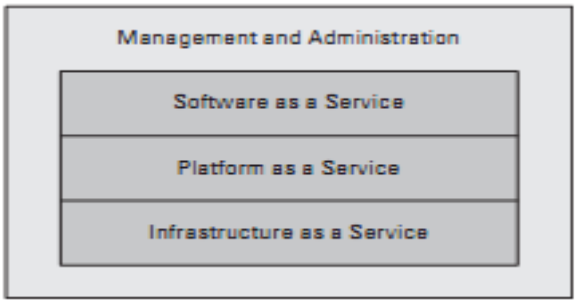
This service gives infrastructure as a service.It provides with the raw storage and networking. mainly it provide on-demand resources for large pools of storage such as virtual-machine disk image library, virtual local area network, firewalls, ip addresses. There is no need to buy any servers, data-centre space or network equipments for storage of the data. It also provides a set of APIs for management and interaction with the infrastructure by customers. Examples of IaasAmazon EC2[3], HP cloud, Racspace cloud, Oracle Infrastructure as a Service.

Software-as-a-Service(SaaS)

SaaS is a software delivery method that provides access to software and its functions remotely as a Web-based service. Software as a Service allows organizations to access business functionality at a cost typically less than paying for licensed applications since SaaS pricing is based on a monthly fee. Also, because the software is hosted remotely, users don't need to invest in additional hardware. Saas application Configuration and customization, Accelerated feature delivery, Open integration protocols.

Platform-as-a-Service(PaaS)

Platform as a service (PaaS) is a category of cloud computing services that provides a computing platform and a solution stack as a service.[1] Along with software as a service (SaaS) and infrastructure as a service (IaaS), it is a service model of cloud computing. In this model, the consumer creates the software using tools and/or libraries from the provider. The consumer also controls software deployment and configuration settings. The provider provides the networks, servers, storage, and other services.[2] Types: Add-on development facilities, Stand alone development environments, Application delivery-only environments, Open platform as a service.



II .LAYERED MODEL OF CLOUD COMPUTING

The cloud computing architecture can be modeled into various layers based on the service they provide to the end users..The Application Layer forms the visible part of the cloud application and the layers underneath are virtualized for the end user. A few examples of applications in this layer include GoogleDocs, YouTube etc. The Hardware Layer consists of the physical hardware needed to carry out the user applications in the cloud environment [6]. This layer provides the scalability and flexibility to the cloud. The Platform Layer is built on the top of infrastructure layer which offers a computing platform as a service [6]. This

layer enables the consumers to run their applications in the cloud without buying the needed hardware and software [7].

2 .Cloud Models

Based on the location where the cloud is hosted, we can classify clouds into four types –private, public, hybrid and community cloud [8].

2.1 Public Cloud

A public cloud is one in which the services and infrastructure are provided off-site over the Internet. Standardized workload for applications is used by lots of people, such as e-mail. Need to test and develop application code. It has SaaS (Software as a Service) applications from a vendor who has a well-implemented security strategy. Need incremental capacity (the ability to add computer capacity for peak times). Many IT department executives are concerned about public cloud security and reliability.

2.2 Private Cloud

A private cloud is one in which the services and infrastructure are maintained on a private network. Business is your data and your applications. Therefore, control and security are paramount. Business is part of an industry that must conform to strict security and data privacy issues. Company is large enough to run a next generation cloud data center efficiently and effectively on its own.

2.3 Hybrid Cloud

A hybrid cloud includes a variety of public and private options with multiple providers. By spreading things out over a hybrid cloud, you keep each aspect at your business in the most efficient environment possible. company wants to use a SaaS application but is concerned about security. Your SaaS vendor can create a private cloud just for your company inside their firewall. They provide you with a virtual private network (VPN) for additional security.

2.4 Community Cloud

The goal of a community cloud is to have participating organizations realize the benefits of a public cloud -- such as multi-tenancy and a pay-as-you-go billing structure -- but with the added level of privacy, security and policy compliance usually associated with a private cloud. The community cloud can be either on-premises or off-premises, and can be governed by the participating organizations or by a third-party managed service provider (MSP).

III.RELATED WORK

Cloud computing became more important in IT industry these days, It provide security to the cloud. Cloud service providers keep on maintaining the data without loss. In private cloud it is responsible for the organization that owns the cloud to keep the data safe from any other un authorized software. In public clouds with the help of internet customer can access cloud data so it is a chances to loss or theft of data.. Cloud should provide fine grained access to the customers. To overcome these security issues and to achieve flexible and fine grained access so many security models have been proposed. *yu et al* proposed a model known as attribute based encryption.By using the encryption Techniques for uploading and downloading the data. Access control is a major issue.

Attribute based encryption(ABE)[12]:

The concept of **attribute-based encryption** was first proposed in a landmark work by Amit Sahai and Brent Waters [1] and later by Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters.[2] It is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). In a such system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. A crucial security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access

Identity based encryption(IBE):

IBE is a public-key encryption system in which an arbitrary string can be used as the public key[9].The concept was formulated by Adi Shamir in 1984.The security demand are Semantic security against an adaptive chosen ciphertext attack. No polynomially bound adversary wins the following game with non-negligible advantage. Examples: user's e-mail address, current-date.

Fuzzy-identity based encryption(FIBE):

In this scheme allows for an identity, ω, to decrypt a ciphertext encrypted with an identity, ω'. We view identities as a set of descriptive attributes. In FIBE the Applications are, IBE system that uses biometric identities. "attribute-based encryption" .

Key-Policy Attribute based Encryption (KP-ABE):

In encryption scheme the cipher text is provided with set of attributes and it associated the users with an any monotonic tree access structure. It is a public key cryptographic method. It associates the set of attributes to the message by encrypted with the corresponded public key components. A user can able to decrypt if and only if the data attributes satisfy his access structure. The drawbacks of this scheme it includes lack of flexibility in attribute management and lack of scalability in dealing with the multiple levels of attribute authorities.

Ciphertext-Policy attribute based encryption (CP-ABE):

In CP-ABE the Type of identity-based encryption are, One public key and Master private key used to make more restricted private keys. But very expressive rules for which private keys can decrypt which ciphertexts Private keys have "attributes" or labels Ciphertexts have decryption policies.

Cipher Text Policy Attribute Set Based Encryption

Ciphertext Policy Attribute Set Based Encryption (CP-ASBE)- is a derived form of CP-ABE. It represent user attributes as a monolithic set and allows users to impose dynamic constraints. In a CP-ABE scheme, decryption keys only support user attributes and organised 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, ciphertext-policy attribute-set-based encryption is introduced. ASBE is an extended form of CP-ABE which organizes user attributes into a recursive set structure. Specifically CP-ASBE allows, User attributes to be organized into a recursive family of sets. Policies that can selectively restrict decrypting users to use attribute within a single set or allow them to combine attributes from multiple sets.

Hierarchical Identity based Encryption(HIBE):

It has two level schemes of HIBE, it consists of a root private key generator(PKG), domain PKGs and users, which all are associated with the primitive Ids(PIDS) these are arbitrary strings. In a 2-HIBE, users will retrieve their private key from their domain PKG. It can compute the private key of any user in their domain and it need to provide previously requested their domain secret key from the root PKG. In this, the cryptosystems also includes a trusted third party and allows a hierarchy of certificate authorities: the root certificate authority will issue certificates for the other certificate authorities, who can turn into issue certificates for users in their respective domains. It does not allow such structure to original system.

Hierarchical Attribute Set Based Encryption(HABE)

In HABE, to achieve fine grained access control in cloud storage services by combined hierarchical identity based encryption(HIBE) and CP-ABE[7]. It also supports fine grained access control and fully delegate the computation to the cloud providers. It has same attribute it may be administrate by multiple domain masters according to specific policies, which is difficult to implement. It consists of five types of parties: a cloud service provider, data owners, data consumers, a number of domain authorities and a trusted authority. To provide a data storage service the cloud will manage the cloud service provider. Data owners will encrypt their data files and store them in the cloud to share with data consumers. Data consumers will downloaded the encrypted data files to access shared data files. Each domain authority is responsible for managing the domain authorities at the next level or the data owners/consumers in its domain. The trusted authority is the root authority and responsible for managing top-level domain authorities.

TABLE I

COMPARISON OF DIFFERRENT ENCRYPTION SCHEMES

Techniques/ Parameters	**IBE**	**KP-ABE**	**CP-ABE**	**CP-ASBE**	**HIBE**	**HASBE**
Access Control	Very Low	Low High if Associated with reencryption strategies	Average Realization of complex Access Control	Higher than CP-ABE,KP-ABE	moderate	Very high
Efficiency	Medium	Average High for broadcast Type encryption and decryption	Average Not efficient for modern environments	Better than CP-ABE Less collusion attacks	Better Lower when compared with ABE schemes	High efficiency And flexibility
Computational overheads	very Low	Medium High	Average	Lower than CP-ABE	More Higher	Less overheads

1) Scalability:

Instead of top level domain authority, ASBE with hierarchical structure by providing the private key generation operation to lower level domain authorities. Cloud security offers organizations, both big and small, the opportunity to scale their computing resources whenever they deem it necessary. This is done by either increasing or decreasing the required resources. Finally it is a hierarchical structure provides scalability over ASBE

2) Flexibility:

HASBE organizes user attributes into a recursive set structure .It allows users to maintain dynamic constraints .It may combined to satisfy a policy. For the given attribute HASBE can support compound attributes and multiple numerical assignments.

3) Fine-grained access control:

Ciphertext is encrypted with a tree access policy by an encryptor and decryption key. HASBE provides dynamic access structure for users to provide fine-grained access control. Usual solution: fine-grained authorization handled by application programs Application-layer access control limitations: Complex, redundant code, Malicious/careless programmers, SQL injection problems, Application code runs in "super-user" mode always, Repeated security logic. Solution: access control inside database, Fine-grained+scalable+confidential access control: open challenge, An extremely challenging issue: implementing user revocation.

4) Efficient user revocation:

User revocation is achieved b expiration time as an attribute to each user's key.we can update users key by adding new expiration_time to the existing one.low level domain is responsible for authorities to keep information of the users key.Instead of generating and distributing the key every time needed. Combine proxy re-encryption with KP-ABE and delegate most of the computational task to Cloud Servers Cloud Servers keep a partial copy of each user's secret key, i.e., secret key components of all but one (dummy) attributes. When the data owner redefines attributes revoke a

user, he also generates corresponding proxy re-encryption keys and sends them to Cloud Servers. Finally HASBE become more efficient..

5) Expressiveness: In HASBE, users key is associated with set of attributes, So HASBE is conceptually closer to traditional access control methods such as Role Based Access Control(RBAC). .HASBE not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of attributes.

IV. Conclusion

This paper surveys different encryption schemes used in clouds. Many encryption schemes like KP-ABE, CP-ABE,HIBE,HASBE are discussed in which all the schemes are concentrated in efficient access control. . In KPABE scheme, attribute policies are associated with keys and data is associated with attributes. Only the keys associated with the policy that is satisfied by the attributes associating the data can decrypt the data. In CP-ABE schemes, attribute policies are associated with data and attributes are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data.This scheme realizes scalable, flexible and fine grained access control in cloud computing. HASBE not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of attributes.

References

[1] R. Buyya, C. ShinYeo, J. Broderg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility".

[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] 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

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

[6] "Cloud Computing: The Next Great Technological Innovation, the Death of Online Privacy, Or Both?" Derek Constantine.

[7] "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0".pdf

[8] "A Hand Book of Cloud Computing" Borko Furht, Armando Escalante.

[9] A. Ross, "Technical perspective: A chilly sense of security," *Commun. ACM*, vol. 52, pp. 90-90, 2009.

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

[11] K. J. Biba, Integrity Considerations for Secure Computer Sytems TheMITRE Corporation, Tech. Rep., 1977.

[12] 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)*, Alexan- dria, VA, 2006.

[13] 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.

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

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

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

[17] G. Wang, Q. Liu, and J. Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services," in *Proc. ACM Conf. Computer and Communications Security (ACM CCS)*, Chicago, IL, 2010. 1962

[18] M. Pirretti, P. Traynor, P. McDaniel and B. Waters, "Secure Atrribute-Based Systems", *ACM conference on Computer and Communications Security (ACM CCS)*, 2006.

[19] A. Kapadia, P. Tsang and S. Smith, "Attribute-based publishing with hidden credentials and hidden policies", *NDSS*, 2007.

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

[21] Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran,"Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption", July 27, 2009

[22] Dan Boneh, Xavier Boyen, Eu-Jin Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext", *Advances in Cryptology—EUROCRYPT 2005*, volume 3493.