Asian Journal of Convergence in Technology **Volume V Issue I**
ISSN NO: 2350-1146 I.F-5.11

A Review Paper on Attribute-Based Encryption for Message Privacy In Cloud

Prof. Jyoti Yogesh Deshmukh, Assistant Professor, Department of Computer Engineering, JSPM's BSIOTR, Wagholi, Pune, India-412207, **Dr. Gayatri M. Bhandari**, Head of Department, Department of Computer Engineering, JSPM's BSIOTR, Wagholi, Pune, India-412207

Abstract— The notion of attribute-based encryption (ABE) was proposed as an economical alternative to public-key infrastructures. It is the set of descriptive attributes, used as an identity to generate a secret key, as well as serving as the access structure that performs access control. ABE is also a useful building block in various cryptographic primitives such as searchable encryption. . It successfully integrates Encryption and Access Control and is ideal for sharing secrets among groups, especially in a Cloud environment. Most developed ABE schemes support key-policy or ciphertext-policy access control in addition to other features such as decentralized authority, efficient revocation and key delegation. This paper surveys mainstream papers, analyzes main features for desired ABE systems, and classifies them into different categories. With this high-level guidance, future researchers can treat these features as individual modules and select related ones to build their ABE systems on demand.

For ABE, it is not realistic to trust a single authority to monitor all attributes and hence distributing control over many attribute-authorities is desirable.

A multi-authority ABE scheme can be realized with a trusted central authority (CA) which issues part of the decryption key according to a user's global identifier (GID). However, this CA may have the power to decrypt every cipher text, and the use of a consistent GID allowed the attribute-authorities to collectively build user's attributes. Decentralized ABE scheme can eliminate the burden of heavy communication and collaborative computation. It is observed that privacy-preserving decentralized key-policy ABE scheme has claimed to achieve better privacy for users and is provably secure in the standard model

Keywords— Attribute-based Encryption, Global Identifier, Privacy, Decentralized Authority, Access Control.

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (Eg: Network, Servers, Storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1]. It consists of various essential characteristics like: On demand access, ubiquitous access, multitenancy, elasticity, measured usage, resiliency. In On-demand access the user can use the computing resources in pay per usage manner. Ubiquitous access represents the ability to access wide range of devices, transport protocols, interfaces and various security technologies in the cloud environments.

Multitenancy enables the different consumers to share the various cloud storage services. Elasticity is the ability of a cloud to straightforwardly scale IT resources as required by the cloud consumer or cloud provider. Measured utilization speaks to the capacity of a cloud platform to monitor the use of its IT resources, fundamentally by cloud consumers. Resiliency refers to redundant IT resources within the same cloud or across multiple clouds. Three common cloud delivery models are widely used and established: Infrastructure-as-a-Service (IaaS), Platform as- a-service (PaaS), Software-as-a-Service (SaaS).IaaS delivery model comprised of infrastructure centric IT resources that can be accessed and managed via cloud service based interfaces and tools. PaaS depends on the existing environment that creates a set of tools used to support the entire applications. SaaS provides reusable cloud service widely available to a range of cloud consumers.

Basically three types of cloud deployment models are public cloud, private cloud and hybrid cloud.

Public cloud is owned by a third party cloud which is accessible by everyone in the cloud environment. Private cloud is owned by single organization where boundaries are defined. Hybrid cloud is a combination of public and private cloud models.

Cloud computing is a kind of distributive computing that represents the utilization models for remotely provisioning scalable and measured resources [12]. When the business data is moved to the cloud, then the security issue will rise, like data security becomes shared with the cloud service provider. Basic terminologies used in the cloud are: cloud provider provides the cloud based IT resources. Cloud consumer uses the cloud based IT resources. Cloud auditor evaluates the security controls, privacy impacts and performance.

Fundamental security terms relevant to cloud computing are:

1. Confidentiality: It allows authorized parties to access the data or resources that are it restricts the unauthorized access to data in transit and storage.
2. Integrity: It will prevent the unauthorized users from altering the data which is stored or transmitted in the cloud.
3. Availability: It allows the data to be accessible and usable during the specific period of time.
4. Scalability: Capability to handle the users added in the network dynamically without any disruption of service.
5. User revocation: If user leaves the network the scheme should revoke his access rights from the network directly.

Otherwise the user can't use the data stored and the access is revoked.

6. Collision resistant: Users can't decipher the encrypted data with their own attributes since the attributes are related to polynomial random encryption function.

7. Access Tree: Based on the attributes, the access tree is generated. The access tree is comprised of nodes. The leaf nodes are represented as attributes and the intermediate nodes are represented using gates likes AND, OR, etc.

Cloud Data security Techniques

Data in readable form is known as plaintext. When the plaintext is transmitted over the network is vulnerable to unauthorized access. Encryption techniques are used to preserve the data confidentiality and integrity of data. Encryption converts the plain text into unreadable format called cipher text. To retrieve the plaintext back the receiver has to decipher it using decryption technique. The key is used along with the techniques for conversion. Basically the encryption technique is classified into symmetric encryption and asymmetric encryption.

Symmetric Encryption

This is also known as classical encryption technique or shared secret key cryptographic technique which is performed by the authorized parties. The messages are encrypted and decrypted using the same secret key.

Asymmetric Encryption

This is also known as public key cryptography. Two different keys are used: Public key and Private Key. Public key is known to all and the private key is known only to the owner. If the message is encrypted using private key then it can only be decrypted with the corresponding public key. If the message is encrypted using public key then it can be decrypted using its private key counterpart.

Attribute Based Encryption (ABE)

ABE is a public key cryptography which follows one to many encryptions. The encrypted data are stored in third party trusted distributed servers. ABE reduces the various limitations of classical encryption techniques like symmetric and asymmetric encryption techniques. ABE solves the problems of security and access control issues in cloud environment.

This paper provides the literature survey of several ABE techniques with merits and demerits of various preliminary schemes.

II. RELATED WORK

Fuzzy Identity based encryption is a set of descriptive attributes [1]. For decryption of ciphertext encrypted with an identity allowed by a private key for an identity, there should be identity match of both. In this scheme biometric inputs are considered as identities which are used to enable encryption. This scheme has error tolerance property because of biometric identities, which intrinsically will have some noise each time they are sampled. The manufacture is an IBE of a message under numerous attributes that invent a (fuzzy) identity. Multiauthority system, there are many authorities. That's why any party can act as authority and there is establishment of initial set of common reference parameters. Any party can be ABE authority, only the
thing it have to create a public key and on request issue private keys to different users according to their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. The largest technical hurdle is to make it collusion resistant. As the system is multiauthority, users will come from completely different authority. There can be possibility of collusion attack due to multiauthority system, so prevention technique is there to tie keys together. This system is secure using the recent dual system encryption methodology where the security proof works by first converting the ciphertext and private keys to a semi-functional form and then comes security. The fully functional IBE scheme has chosen ciphertext security in the random oracle model assuming a variant of the computational Diffe-Hellman problem [4]. This system is based on bilinear maps between groups. The fine combination on elliptic curves is an example of such a map. Specific definitions for protected identity based encryption schemes and a number of applications for such systems are the outcomes of this system.

III. LITERATURE SURVEY

By assuming the trusted cloud service provider provides security also to the large amount of sensitive and valuable data stored. ABE algorithms can be used for protecting the confidentiality of the stored data and also ABE provides the access control mechanism for data on the cloud. In cloud environment, data confidentiality is important to defend against insider attack, collision attack and denial of service attack. This section provides the existing attribute based encryption mechanisms in cloud environment.

Attribute Based Encryption (ABE)

ABE was introduced by Sahai and Waters [2] in 2005. It is a public key based one to many encryptions that allows user to encrypt and decrypt the data based on user attributes. The secret key and cipher text are dependent on the user attributes. The decryption of ciphertext is possible only if the set of attributes of user key matches with the attributes of ciphertext. Decryption can be done only when the number of matching keys is equal to the mentioned threshold level. ABE algorithm consists of four steps: Setup, key generation, encryption and decryption. Collision resistance is a crucial feature of ABE. An opponent that holds multiple keys can access the data if the individual key matches.

Drawbacks: For encryption, the Data owner has to use every authorized user's public key so it increases the computation overhead. This method is restricted because it uses access of monotonic attributes to control user's access to the system.

1. Identity Based Encryption (IBE)

It was proposed by Shamir in 1984[3].In Identity Based Encryption (IBE) the secret key and the attributes are based on the identity of the user. For example, email id is the identity of the user. Trusted third party will generate the private key.
Drawbacks: If the trusted third party gets compromised then there is no security for the system. The user privacy can't be preserved using IBE.

2. Key Policy Attribute Based Encryption (KP-ABE)
It was proposed by Goyal et al.[4]. Every user is allocated with some access tree over set of attributes. Ciphertexts are based on the set of attributes and the private key is based on the monotonic access structure that controls which ciphertexts a user can decrypt. This is designed for one to many communications. Decryption can be done only when the attribute set satisfies user's access structure. It supports access control scheme.
Drawbacks: Data owner cannot decide who can decrypt the encrypted data. It can only choose descriptive attributes for the data. It is not suitable for broadcasting applications because the data owner has to trust the key issuer.

3. Expressive Key Policy ABE (EKP-ABE)
It is the extended version of KP-ABE; the non-monotonic access structures [5] are used. Non-monotonic access structure uses contradicted gates such as NOT in the access structure. It is more flexible to restrict the unauthorized usage of data.
Drawback: The overhead is increased because of negative attributes which is not relevant to the encrypted data.

4. Ciphertext Policy ABE (CP-ABE)
It is a reverse version of KP-ABE [6]. In CP-ABE, ciphertext is associated with an access structure and user's private key is based on set of attributes. A user is able to decrypt the ciphertext only if set of attributes associated with users private key satisfies the access policy associated with the ciphertext. CP-ABE is more secured even the trusted third party is compromised.
Drawbacks: CP-ABE doesn't fulfill the enterprise needs of access control mechanism. Decryption keys support user attributes that are organized logically as a single set.

***5. Hierarchical Attribute Based Encryption (*HABE)**
The HABE was proposed by Wang et al. [7]. This model consists of a root master that corresponds to the trusted third party, multiple domain master in which top level domain masters corresponds to multiple enterprise users and numerous users that corresponds to all personnel in an enterprise. This scheme user's hierarchical generation of keys. It uses randomized polynomial time algorithm. It supports secured access control, scalability and fully delegation. It can share the protected data for users in a cloud in an enterprise environment. It supports proxy re-encryption scheme.
Drawbacks: It is very difficult to implement in real-time environment. The same attribute will be used by multiple domain masters.

6. Multiple Authorities ABE (MAABE)
This method uses multiple authorities and the user attributes are distributed to various authorities. Suppose [8] it consists of N multiple attribute authorities and one central authority. The data can be decrypted by the user under attribute set A and decryption keys for an attribute set Au. It allows any independent authorities to distribute private keys and to handle faulty or lost authorities.
Drawbacks: Difficulty in multi-authority scheme is it requires authority's to maintain disjoint sets of attributes.

7. File Hierarchy Attribute Based Encryption (FH-ABE)
This method uses file hierarchy based encryption techniques. The files are encrypted based on the layered access structure. Both cipher text storage and time costs of encryption are saved [9].
Drawback: The FHABE scheme is proved to be secure under the standard assumption.

8. Ciphertext policy Weighted ABE (CPWABE)
This scheme assigns [10] weight to the attributes based on the preference defined in the access control structure. Users will have assigned the weight to their attributes. The data owner will encrypt the data based on the attributes. The private key is based on weighted access structure and the decryption [11] is possible only when the ciphertext and the weighted attribute matches with the weighted access structure. It solves the keyescrow problem by using weighted attributes.
Drawback: Cost of computation is increased.

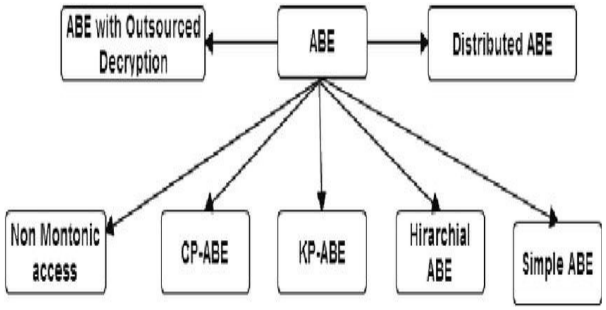

Fig. 1: Types Of ABE

IV. PROPOSED WORK

The existing attribute based encryption schemes for data security are using symmetric encryption techniques, the ciphertext is not hidden. Multi-authority file hierarchy based hidden CP-ABE can be used for hiding the ciphertext policy and single point of failures can be avoided. The access

structure can be designed in an hierarchical way to reduce the size of the ciphertext. At the same time storage cost can be reduced. The asymmetric encryption algorithms can be used with the attribute based encryption to increase the security of the data in the cloud environment.

CONCLUSION

The scheme of distributed key policy attribute based encryption provides security to the messages in distributed networking environment. The policy set for every message will differentiate another message depending on their attributes provided. This policy will help to generate keys for encryption of particular message generated by owner. This message will allow an access to any user who will have required number of attributes, so that it will have same kind of keys to decrypt the message. In future this scheme can be enhanced for more than one owner with their own key generation to provide more security in terms of keys as well as messages.

References

[1] Muhammad Yasir Shabir, Asif Iqbal, Zahid Mahmood and Ataullah Ghafoor, Analysis of Classical Encryption Techniques in Cloud Computing, IEEE Tsinghua Science & Technology, Vol.21, February 2016.

[2] A.Sahai and B.Waters, Fuzzy identity based encryption, in Proc. Advances in Cryptology – Eurocrypt, 2005, pp.457-473.

[3] Adi Shamir. Identity-based cryptosystems and signature schemes, in Proc. of CRYPTO 84 on Advances in cryptology, pages 47–53. Springer- Verlag New York, Inc., 1985.

[4] V.Goyal, O.Pandey, A.Sahai and B.Waters, Attribute based encryption for fine grained access control of encrypted data, in proc. ACM conf. computer and communications, 2006.

[5] J.Bethencourt, A.Sahai, and B.Waters, Ciphertext policy attribute based encryption, in proc. IEEE symposium security and privacy, 2007.

[6] K.Meena,S.Vinodhini, T.Pallavi & R.Vasugi," Surveillance Based Gcm Home Security System Using Object Motion Detection",International Innovative Research Journal of Engineering and Technology,pp.44-47,2016.

[7] S.Rifki, Y.Park, and S.Moon, A fully secure ciphertext policy attribute based encryption with a tree-based access structure, Journal of Information Science and Engineering, Vo.31,pp.247-265,2015.

[8] 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 communication security, 2010.

[9] K.Yang, X.Jia, K.Ren and B.Zhang, Dac-Macs: Effective data access control for multiauthority cloud storage systems, in Proc. Of IEEE Infocom, 2013.

[10] Shulan Wang, Junwei Zhou, Joseph K.Liu, Jianping Yu, Jianyong Chen and Weixin Xie, An efficient file hierarchy attribute based encryption scheme in cloud computing, IEEE Transactions on information forensics and security, Vol. 11, No.6, June 2016.

[11] Ximeng Liu, Jiafeng Ma, Jinbo Xiong, Qi Li, Jun Ma, Ciphertext – policy weighted attribute based encryption for fine grained access control, International conference on Intelligent networking and collaborative systems, 2013.

[12] Jyoti Yogesh Deshmukh, Arati M. Dixit, Message Privacy with Load Balancing using Attribute based Encryption, International Journal of Computer Applications (0975 – 8887) Volume 103 – No.10, October 2014.

[13] G.K.Sandhia, G.K.Bhaskar, secure data sharing using attribute based encryption in cloud computing, Journal of Chemical & Pharmaceutical Sciences, Vol.9, December 2016.