A Survey on Access Control Mechanisms using Attribute Based Encryption in Cloud

Mr. S. Vigneshwaran[1] Mr. R. Nirmalan[2]
[1]P.G. Scholar [2]Assistant Professor
[1,2]Sri Vidya College of Engineering & Technology, Virudhunagar

Abstract— Cloud computing is an emerging computing technology that enables users to distantly store their data into a cloud so as to enjoy scalable services when required. And user can outsource their resources to server (also called cloud) using Internet. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. Attribute-based encryption (ABE) can be used for log encryption. This survey is more specific to the different security issues on data access in cloud environment.

Key words: Cloud computing, data storage, security, authentication

I. INTRODUCTION

Cloud computing is shared resource, information, and software are provided to computers and other devices. Cloud computing is a large-scale distributed computing that makes use of existing technologies such as service-orientation, virtualization, and grid computing. It offers a different way to manage IT resources. A webmail is a simple example of cloud computing. The webmail provider maintains the server space and provides access; the webmail user just plugs a web address into a browser and submits user information to access an account.

Cloud computing is the long dreamed vision of computing utility, where cloud customers can remotely store their data into the cloud so as to enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources. Centralized cloud has more and more sensitive information such as e-mails, company finance data, personal health records, government documents and etc.

Though Cloud Computing is in a period of strong growth, but still it has some issues of security and somewhat it is undeveloped. Government Technology Research Alliance (GTRA) research showed that the most common concern about implementing Cloud Computing technology with security.

The real value of cloud computing is that it makes your library related software and data available transparently and everywhere. We are all aware, country like India faced problems like digital device and off course very low internet capacity. So, benefit of new technology can be reached to limited area of educational area.

The cloud verifies the authenticity of the user without knowing the user's identity before storing data. The scheme prevents replay attacks. User revocation are Addressed. Authentication and access control schemes is decentralized and robust.Providing more security for data stored in cloud. Hides the attributes and access policy of a user in the cloud

Consider the following situation: a law student, Alice, wants to send a series of reports about some malpractices by authorities of university Z to all the professors of University Z, Research chairs of universities and students belonging to Law department in all universities in the province. Also she wants to remain anonymous while publishing all evidence of malpractice. She uses cloud to store the information. Access control is important in such case, so that only authorized users can access the information. It is also important to confirm that the information comes from a reliable source. The problems of access control, authentication, and privacy protection should be solved simultaneously.

II. RELATED WORK

ABE is actually a generalization of IBE (identity-based encryption): in an IBE system, cipher texts are associated with only one attribute (the identity). The ABE scheme of Sahai-Waters was proposed as a fuzzy IBE scheme, which allowed for some error tolerance around the chosen identity. In more recent terminology, it would be described as a key-policy (KP) ABE scheme that allows for threshold policies. Key-policy means that the encryptor only gets to label a cipher text with a set of attributes. The authority chooses a policy for each user that determines which cipher texts he can decrypt. A threshold policy system would be one in which the authority specifies an attribute set for the user, and the user is allowed to decrypt whenever the overlap between this set and the set associated with a particular cipher text is above a threshold.

Goyal et al. [2],proposed a KP-ABE scheme which supports any monotonic access formula consisting of AND, OR, or threshold gates. A construction for KP-ABE with non-monotonic access structures (which also include NOT gates, i.e. negative constraints in a key's access formula) was proposed by Ostrovsky, Sahai and Waters. All of these schemes are characterized as key-policy ABE since the access structure is specified in the private key, while the attributes are used to describe the cipher texts. The roles of the cipher texts and keys are reversed in the cipher text-policy ABE (CP-ABE) introduced by Bethencourt, Sahai and Waters, in that the cipher text is encrypted with an access policy chosen by an encryptor but a key is simply created with respect to an attributes set. The security of their scheme is argued in the generic group model.

Recently, sahai,water and goyal et al proposed CP-ABE constructions based on a few different pairing assumptions which work for any access policy that can be expressed in terms of an LSSS matrix. In this paper will look only at the Key Policy Attribute Bsaed Encryption (KP-ABE) setting. A both the simple threshold and the more complicated monotonic access structure case, and will build a construction based on the same assumption. Both non-monotonic access structures and the cipher text policy schemes require much stronger assumptions, and very different techniques.

A. Creation of KDC

Key Distribution Centre (KDC) is an active database which is responsible to distribute secret keys and attributes to all users. To create a different number of KDC's, an administrator have to create with KDC name, KDC ID and KDC password, and then save it in a database. To register user details, the input consist of username and user id.

Sushmita Ruj et all[10], proposed a model to avoid storing multiple encrypted copies of same data in cloud. The main novelty of this model is addition of key distribution centers (KDCs). The DACC algorithm is proposed. They proposed one or more KDCs distribute keys to data owners and users. The decentralized approach is implemented based on Attribute-Based Encryption (ABE). But they not considered the authentication process. User revocation is provided and also utilizes concept of KDC.

John Bettencourt et al [3], proposed a policy which work in several distributed systems, a user should only be able to access data if a user possesses a certain set of attributes. The only method for enforcing such policies is to employ a trusted server to store the data and deal with access control. However, the confidentiality of the data will be compromised, if any server storing the data is compromised. A Ciphertext-Policy Attribute-based Encryption technique allows the encrypted data can be kept confidential even if the storage server is not a trusted one. Moreover, these methods are secure against collusion attacks. Earlier Attribute Based Encryption system uses attributes to describe the encrypted data and built policies into user's keys; while in this system attributes are used to describe a user's attributes, and a party can determine a policy to decrypt the encrypted data.

Thus, above methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). Cipher text-policy attribute-based encryption (CP-ABE) presents a system for realizing complex access control on encrypted data. It improves decryption efficiency and collusion attacks are prevented. One limitation of this CP-ABE system is that it is proved secure under the generic group heuristic.

In paper V.Goyal et Al [2], shows a technique to develop a new cryptosystem for fine-grained sharing of encrypted data called as Key-Policy Attribute-Based Encryption (KP-ABE).Cipher texts are labeled with sets of attributes and private keys are associated with access structures that control the user to decrypt the cipher text easy to decrypt. The Monotone Access Structure is used to resistant the collusion attacks in which an attacker might obtain multiple private keys, as they never hide the set of attributes under which the data is encrypted

B. User Registration

Once KDC created it gives a user id so that to a user, the user will enroll the personal details such as Username, user id, Password and other information to KDC. The KDC will be verifyithe user details and store it in a database if valid.

Shushing Yu et al [9], proposed a revocation mechanism that provides base idea of attribute revocation in CP-ABE. One important issue of attribute revocation is cumbersome for CP-ABE schemes. Attribute based data sharing with attribute revocation scheme to enable base idea of attribute revocation in CP-ABE. It provides authority to revoke any attribute of user at any time. (DBDH) Decisional Bilinear Diffie-Hellmen assumption is used for security implementation. It is applicable to KP-ABE counterpart in which the authority is able to revoke any partial access privilege of users. The centralized approach is used to implement the technique based on ABE algorithms. But the problem is "the scheme not consider the authentication process" and user revocation process.

Matthew Green et al[12], says to eliminate the drawbacks of ABE is that the size of the ciphertext and the time required to decrypt it grows with the complexity of the access formula \in centralized approach and it based on ABE. The authentication process is not considered in this scheme, no user revocation. It only provides adaptive security. Secure against malicious proxy server. It uses Monotone access structure. Secure under the Decisional Parallel BDHE Assumption and the Decisional Bilinear Diffie-Hellman assumption (DBDH) in bilinear groups.

C. Trustee and User Accessibility

Trustee can be someone like federal Government who manages social insurance number. User can login with their credentials and request the token from trustee for the file upload. Trustee is initialized with Tsig, Tver Tsig is the private key with which a message is signed and Tver is the public key used for verification. Trustee Secret Key(TSK) is secret key and Trustee Public Key(TPK) is public key of Trustee (for encryption and decryption).Trustee will create token which contains user id, key and user signature which is signed using signing key Tsig(SHA algorithm).Then the trustee will issue a token to the particular user and then trustee can view the logs. User may be Creator, Writer or Reader.

Kan Yang et al [13] proposed an approach provide effective and secure data access control scheme with efficient decryption. This system use the decentralized approach based on ABE. But it cannot provide privacy preserving authentication. User revocation is provided. The security model is highly efficient and provably secure.

DAC-MACS are a collection of algorithms that combines a set of CP-ABE algorithms. Decrypt and a set of attribute revocation algorithms. DAC-MACS is secure against the collusion attack. Construct a new multi-authority CP-ABE scheme with efficient decryption and also design an efficient attribute revocation method that can achieve both forward security and backward security.

Melissa Chase et al [8], proposed a system to remove the central authority and protects the user's privacy. Attribute based encryption determines decryption ability based on a users attribute .Multi authority ABE scheme monitors different set of attributes and performs a trusted central authority and global identifiers.ABE is a generation of identity based encryption. ABE proposed fuzzy IBE scheme which have some error tolerance .New technology such as key-policy ABE scheme, performs encryptor only gets to label a cipher text with set of attributes. Goyal et al [8] proposed KP-ABE scheme it supports any monotonic access formula consisting of AND, OR gates. Anonymous key issuing protocol allows multiauthority ABE with enhanced user privacy. This key is used to communicate the users and it is used for simple modification to straight forward manner. Global identifier plays the role of anonymous credential secret key. This is unique and secret. Single authority is an unrealistic manner it can monitor every single attribute of all users. Multi authority attribute based encryption is more realistic attribute based access control and it is responsible for different authorities.

Hemanta Maji et al [5], says Attribute-based signatures are just a cryptographic primitive, It provides security and correctness guarantees. ABS is ideally suited for an Attribute-Based Messaging (ABM) system. Attribute-Based Messaging or ABM provides an example of a quilt essential attribute based system which demands new cryptographic primitives for achieving its natural security goals. The goals of an ABM system can be achieved using trusted entities. ABS scheme achieves perfect privacy; unlink ability, and collusion resistant enforceability. ABS goes beyond mesh signatures and provides collusion-resistance. ABS scheme would treat them as a single user; indeed if there is only one user in the system, an ABS scheme degenerates to a mesh signature scheme. ABS allows claims in terms of some arbitrary attributes chosen by the signer.

D. *File Storage*

User submits the token given by trustee to KDC. The token verification algorithm verifies the signature contained in token using the signature verification key T_{ver} in TPK. If it is valid then KDC will provide the public and secret key for encryption/decryption and KDC Secret Key (ASK[i]), KDC Public Key (APK[i]) for signing/verifying to the user. After users received the keys, the files are encrypted with the public keys and set their Access policies (privileges).The user then encrypt the data under access policy X using Attribute Based Encryption. The user can construct a Claim Policy Y to enable the cloud to authenticate the user. The creator will use Timestamp *t* to prevent replay attack. Then Sign the message using Attribute based Signature which is used to enable the cloud for verifying access claim of the user. Finally all these information are encrypted using Asymmetric key approach (Homomorphic Encryption called as Pailier Cryptosystem) and send it to cloud.

Fangming Zhao et al [11], proposed a technique to provide the novel data sharing protocol by combining and exploiting two of the latest attribute based cryptographic techniques: Attribute based Encryption and Attribute based Signature. The data confidentiality is not provided. The cloud client securities are not considered. The centralized approaches are implemented based on ABE and provide authentication, there will be no user revocation. To provide thin clients with both strong data confidentiality and flexible fine grained access control without imposing additional cost on clients.

David F.Ferraolo et al [1] discussed a role based access control that is more central to the secure processing needs of nonmilitary systems then DAC. Role based access control is a non-discretionary access control mechanism which allows and promotes the central administration of an organizational security policy. Security is important for commercial and civilian government organizations. Integrity, availability and Confidentiality are used for software systems, databases and data network security. Integrity is particularly used for transfer, clinical medicine, environmental research, air traffic central trusted computer system evaluation criteria and DAC is an access central mechanism that permits users to allow or disallow other user access to objects.DAC mechanism allows user to grant or revoke access to any of the objects under their control without the intersession of a system administrator. Role based access control policy based access control decisions consists of function which allows the user to perform within an organization .RBAC restricting access to objects based on the sensitivity of the information contained in the objects and formal authorization .RBAC provide a naming, and describe many to many relationships between individual.

E. *File Retrieval*

Using their access policies the users can download their files by the help of KDC's to issue the private keys for the particular users. If the user is valid, cloud decrypts the message using ABE. The input such as chipper text and secret key in decryption algorithm produce the original output.

Cipher Text-RSA allows a party with fine-grained control over identifying information to sign a message. In ABS, a signer who possesses a set of attributes from the authority can sign a message with a predicate that is satisfied by attributes. The signature reveals the fact that a single user with some set of attributes satisfying the predicate has attested to the message. The signature hides the attributes used to satisfy the predicate and any identifying information about the user.

H.Lin,Z.Cao et al [6],proposed a scheme in which Central authority is the danger zone. If any problem occurs in this zone whole system is corrupted. In this paper they used a threshold multiauthority fuzzy identity based encryption scheme without a central authority for first time. Security is performed based on several techniques such as joint random secret sharing protocol, joint zero secret sharing protocol and standard bilinear Diffie-Hellman assumption .Multi authority attribute scheme is used to give the privacy without a central authority. It allows any polynomial number of independent authorities to monitor attributes and distribute keys. Two technologies are mainly used one is every user has global identifier; second one is a fully trusted central authority. The global GID work is to present a collusion attack between different users. Central authority is the second tool used to provide a final secret key to integrate the secret keys from the other attribute authorities. This paper focused on removing the Central authority from multi authority ABE scheme. It is difficult to remove the central authority while preventing the collusion attack and keeping the decryption process of each independent user .We replace the pseudo random function used in chase’s scheme by a polynomial and apply the key distribution technique and joint zero secret sharing technique. The communication is performed in a synchronous manner.

F. *File retrieval and access policy*

Files stored in cloud may be corrupted. To solve this issue, the file recovery technique is used to recover the corrupted file successfully using String Matching Algorithm. It also hides the access policy and the user attributes in cloud.

Hongwei Li et al[7], proposed this paper, based on the identity-based hierarchical model for cloud computing (IBHMCC) and its corresponding encryption and signature schemes, presented a new identity-based authentication protocol for cloud computing and services. To achieve the security in the communication, an encryption and signature schemes are proposed such as an identity-based encryption (IBE) and identity-based signature (IBS) schemes. SSL Authentication Protocol is of low efficiency for Cloud services and users. An identity based authentication for cloud computing, based on the identity-based hierarchical model for cloud computing (IBHMCC).Performance analysis indicate that the authentication protocol is more efficient and lightweight than SAP, especially the more light weight user side.

Melissa Chase et al[4], proposed a scheme which allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. They developed techniques to achieve a multi authority version of the large universe fine grained access control ABE. Multi authority scheme cannot allow changes in a user’s attribute set. It is a similar approach would allow one to choose exactly how many of the attributes given in the cipher text to require from each authority. It proposes each user must go to every authority before he can decrypt any message, for file retrieval and access policy these mechanisms proved to be an efficient one.

III. CONCLUSION

In cloud computing environment, data are stored in decentralized manner for accessing data from the cloud. Here, we surveyed some authenticated access control methodologies with attribute based encryption to provide more security. Each individual has to securely access cloud with any of these access control methods. Attribute Based Encryption mechanism is used to provide authentication for access data from cloud in secure manner.

REFERENCES

[1] D. F. Ferraiolo and D. R. Kuhn, “Role-based access controls,” in 15th National Computer Security Conference, 1992.

[2] Goyal, O. Pandey, A. Sahai, And B. Waters, “Attribute-Based Encryption For Fine-Grained Access Control Of Encrypted Data,” In Acm Conference On Computer And Communications Security, Pp. 89–98, 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in IEEE Symposium on Security and Privacy. , pp. 321–334, 2007.

[4] M. Chase, “Multi-authority attribute based encryption,” in TCC, ser. Lecture Notes in Computer Science, vol. 4392. Springer, pp. 515–534, 2007.

[5] H. K. Maji, M. Prabhakaran, and M. Rosulek, “Attribute-based signatures: Achieving attribute-privacy and collusion-resistance,” IACR Cryptology ePrint Archive, 2008.

[6] H. Lin, Z. Cao, X. Liang and J. Shao, “Secure Threshold Multi-authorityAttribute Based Encryption without a Central Authority,” in INDOCRYPT,ser. Lecture Notes in Computer Science, vol. 5365, Springer, pp. 426–436,2008.

[7] H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-based authentication for cloud computing,” in CloudCom, ser. Lecture Notes in Computer Science, vol.5931. Springer, pp.157–166, 2009.

[8] M. Chase and S. S. M. Chow, “Improving privacy and security in multiauthority attribute-based encryption,” in ACM Conference on Computer and Communications Security, pp. 121–130, 2009.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in ACM ASIACCS, pp. 261–270, 2010.

[10] S. Ruj, A. Nayak, and I. Stojmenovic, “DACC: Distributed access control in clouds,” in IEEE TrustCom, 2011

[11] F. Zhao, T. Nishide, and K. Sakurai, “Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems,” in ISPEC, ser. Lecture Notes in Computer Science, vol. 6672. Springer, pp. 83–97, 2011

[12] Matthew Green, Susan Hohenberger and Brent Waters, “Outsourcing the Decryption of ABE Ciphertexts,” in USENIX Security Symposium, 2011

[13] Kan Yang, Xiaohua Jia and Kui Ren, “DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems”, IACR Cryptology ePrint Archive, 419, 2012.

[14] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak, "Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds," *IEEE Transactions on Parallel and Distributed Systems*, 15 Feb. 2013.