Securing Cloud Data Access using Attribute Based Encryption (Abe) Scheme

Ms. G.Hari Priya[1] Ms. M.Kowsalya Devi[2] Ms. M.Kowsalya Devi[3] Mr.R.Sivaramakrishnan[4]
[1,2,3]UG Scholar [4]Assistant Professor
[1,2,3,4]Department of Computer Science and Engineering
[1,2,3,4]KPR Institute of Engineering and Technology-Arasur Coimbatore

Abstract— Cloud computing provides flexible, low cost usage of computing resources but there may be a chance of data gets outsourced to some other cloud servers and various privacy concerns emerge from it. For protecting the data's that are stored in cloud servers, we are using ABE scheme (ATTRIBUTE BASED ENCRYPTION SCHEME). Whereas in existing schemes, less importance is given for privilege control and identity privacy. In this paper, data privacy and user identity can be addressed in anony control scheme. Anony control is secured under Decisional Bilinear Diffie Hellman Assumption. To achieve more efficiency we go for user revocation mechanism.

Key words: Cloud Computing, Integrity, Security

I. INTRODUCTION

A. *Cloud Computing:*

Cloud computing is an on-demand computing which provides shared resources and data to computers in a network. It solves problems in any computer in a network. Cloud computing can be applied to super-computing or high performance computing power which is used by military and research facilities to perform tens of trillions of calculations per second.

1) *Advantage:*

- It reduces software costs.
- Instant software updates without needing to pay for or download increase the data reliability.
- Multiple users can collaborate easily on documents and projects.
- It is device independence and lower cost.

B. *Private Cloud:*

In private cloud, infrastructure is operated for a single organization. It is managed internally or by a third party. It takes the advantage of providing more control of resources and steering clear of multi-tenancy.

C. *Public Cloud:*

A public cloud is a cloud computing deployment scheme that is used by general public. The general public is defined as either individual user or corporations. The public cloud infrastructure is used by a cloud services organization.

D. *Hybrid Cloud:*

A hybrid cloud uses a private cloud foundation with strategic integration and also used for public cloud services. Most of the companies manage with data centres, private cloud and public clouds there by creating hybrid clouds.

II. DATA SECURITY ISSUES

There are two main issues exist with security and privacy aspects of cloud computing. They are,

- Loss of control over data
- Dependence on the cloud computing provider

These two issues can lead to a number of legal and security related to infrastructure, access control, integrity control as well as cloud computing provider at risk. The typical issues due to loss of control over data are:

1) To analyse user data cloud computing providers are able to perform data mining techniques.
2) Data protection and privacy legislation is not same in many countries.
3) It depends on a reliable and secure telecommunication network that assures the operation of the terminal users.

The typical issues due to dependence on the cloud computing provider are:

1) Cloud computing is a service similar to traditional services and utilities. They tend to be offered by large providers.
2) Cloud computing services do not include any interaction between customers and cloud computing provider.

III. IDENTITY BASED ENCRYPTION (IBE)

The IBE concept proposes any string can be used as an individual public key, including e-mail address. Here the important aspect is to maintain the access that matches with the profile. Maintenance of the identity is required to conduct operation in cloud deployment and authenticate the real users. This is requiring for both internal and external purposes. The problem arise is to secure the data. We have to maintain a secure protocol over a network.

A. *Fuzzy IBE:*

The type of IBE is called as fuzzy IBE. This fuzzy IBE scheme allows for a private key. It can be applied to enable encryption using biometric input as identities. It is used for a type of application called as ATTRIBUTE BASED ENCRYPTION.

IV. CIPHER TEXT ATTRIBUTE BASED ENCRYPTION:

In cipher text ABE scheme, the encryption can fix the policy, which can decrypt the encrypted message. Here four fundamental algorithms are Setup, Key generation, Encrypt, Decrypt

A. *Access Control:*

It is a security technique that can be used to regulate who or what can view or use resources in a computing environment.

B. Types*:*

- Physical- it limits access to campuses, building, rooms, physical IT asset.
- Logical – it access limits of connections to computer networks, system files and data.

– Access Control Systems performs authorisation, identification, authentication, access approval and accountability of entities through login credentials including password, personal identification number.

V. MODELS FOR CONTROLLING ACCESS:

1) MANDATORY ACCESS CONTROL- the authorisation of a subject‘s access to an object depends upon labels which indicate the subject’s clearance and classification or sensitivity of the object. E.g.: military classifieds document as unclassified, confidential, secret and top secret.
2) DISCRETIONARY ACCESS CONTROL- with dac, the subject has authority, within certain limitations to specify what objects are accessible. E.g. a tabular listing that would show the subject’s or users who have access to the subject.
3) NON-DISCRETIONARY ACCESS CONTROL- a central authority determines which subjects can have access to certain objects based on the organisational security policy. It may be role based or task based. E.g.: used in organization with frequent personal changes because the access control are based on individual role or title within the organization. Therefore access controls need not to be changed whenever a new person assumes that role.

A. *Identity Based Protection:*

Maintenance of the identity is required to conduct smooth operation in the cloud deployment and authenticate the real users. The biggest problem is to secure the confidential data. In order to do this, one has to maintain a secure protocol over the networks and activate the firewalls to ensure the security of the confidential information and sensitive information that is not important for business should be destroyed.

B. *Semi Anonymity:*

Here the information is partial i.e. partial disclosure. E.g. voting system. In this system the politician’s are known but the voters are not known i.e. political people doesn’t know who is voting for them. It is also achieved in some of social media apps. It is used in biometric technology.

VI. DECISIONAL DIFFIE-HELLMAN ASSUMPTION (DDH):

Initially computational decisional diffie-hellman assumption was used to solve hard problems by using discrete logarithms. Solving problems using CDH is very hard and also considered as weaker assumption. To overcome this DDH assumption was introduced to support security purposes and also used in various protocols such as cryptographic protocols. Here mathematical operations were fast to compute but the operations cannot be reversed. Based on discrete logarithms DDH assumption is stated as, consider a cyclic group of order G having a, b which belongs to z. Therefore g^ a, b is a random element in G. Also g^a, g^b, g^ab where a and b are random and independent are known as DDH triples. Also g^a, g^b, g^c where a, b and c are random and independent are known as DDH tuples. The problem of detecting DDH tuples is easy for small fraction of inputs then it is easy for large fraction of inputs otherwise it is not easy for large inputs.

A. *Advantage:*

Shared key is not transmitted over the channel. It is light weight two-pass protocol having only a public key transport from participant A to B and vice versa.

VII. RELATED WORK:

A. *Cipher Text Policy Attribute Based Encryption (CP-ABE):*

Cipher text is used to convert message to plain text. The CP-ABE is under cryptographic assumption in standard model. Here any encryption is allowed to access the control over the attributes of the system. Based on three constructions first system is proved to be selectively secure under parallel bilinear diffie-hellman exponent assumption (PBDHE). It is the generalization of bilinear diffie hellman exponent (BDHE) assumption. The next two constructions provide performance to achieve security. Public key encryption is done for transmitting and storing the information but it is not done for large set of attributes. Encryption algorithm is done in terms of specifying the access with any access formula. Access control is done based on linear secret sharing scheme (LSSS). Previously it could support only limited access control. Hence we go for efficient way of controlling the access.

B. *Fuzzy Identity Based Encryption:*

A new type of identity based encryption is called as Fuzzy Identity Based Encryption. In fuzzy identity based encryption scheme a user having secret key for identity ω can decrypt the encrypted cipher text ώ if and only if ω and ώ are matched. IBE schemes are both error tolerant and secure against collision attacks. Identity based encryption is used in biometric entities and also for attribute based encryption where to encrypt a document a user must have certain set of attributes. Any user can decrypt a document if and only if they have same set of attributes. When identity based encryption is used in biometrics a user will always have a public key. One important thing is it must provide security against collision attacks.

C. *Attribute Based Encryption For Fine-Grained Access Control Of Encrypted Data:*

There is a more need for personal data’s of users which get stored on the internet by third parties e.g. Email id are stored on the web portals such as Google, yahoo. Those data’s must be encrypted. For encrypting the data’s in a fine grained manner that are stored on these sites, a cryptosystem scheme called as Key-Policy Attribute Based Encryption is used. In this scheme, encrypted texts are attached with set of attributes and secret key of a user’s are associated with access structure which specifies the control to the users to decrypt the encrypted text. Randomized algorithm is used in four stages such as setup, encryption, key generate, decryption. Drawback of encrypted data’s are used with the existing scheme was sharing private keys in a selective manner i.e., giving private keys to others. The solution provided in this paper is delegation of private keys which includes Hierarchical Identity Based Encryption (IBE).

D. *Attribute Based Data Sharing With Attribute Revocation:*

Cipher text-Policy Attribute Based Encryption (CP-ABE) can access the shared data. Each user can be associated with set of attributes and retrieved data can be encrypted. If the user wants to decrypt a cipher text only his attributes satisfy with the cipher text access structure. The public key and cipher text sizes in CP-ABE are same to the number of attributes, independent to the number of users. Here PPT algorithm is used to generate distribution of outcomes and it includes randomness of the algorithm as a random variable. The main problem is attribute revocation. To overcome this on-line proxy servers are used. Authority to revoke user's attribute is enabled. It can be achieve by uniquely combining the proxy re-encryption technique with CP-ABE and enables the authority to assign, perform task to proxy servers.

E. Multi-Authority Attribute Based Encryption:

In multi authority ABE scheme, each user is identified by a set of attributes and by using the functions of those attributes, it is possible to decrypt the encrypted texts. Each of the n authorities is able to monitor attributes and distribute the secret keys based on the user's request they can encrypt the message using the key. The message can be decrypted by the one who is having the key of the given attributes from each authority. In this scheme, user's secret keys are generated randomly so they could not be combined. Here the problem was collusion because the secret keys are spitted for each user in a separate manner by two techniques. First technique is, it is necessary for each user to have Global Identifier (GID) which describes two properties first, no user can state another user's identity and secondly, it is possible for all the authorities to verify the user's identity. The second technique is, Central Authority that is, users can get their corresponding secret keys by sending their own Global Identifier to the central authorities. To randomize the secret key function used in this scheme was pseudorandom function (PRF).Randomized algorithm is used in five stages namely, setup, attribute key generation, central key generation, encryption, and decryption. The solution provided is additive secret sharing for the problems occurred in multi authority attribute based encryption.

VIII. Encryption and Decryption:

Encryption is the process of encoding the messages i.e. the message can be encrypted by converting from plain text into cipher text [1]. The user whose private key matches with the public key can encrypt the message. For encryption, public key, master key, privilege tree is the main function to produce cipher text and verification set, so that the user can execute specific operation on cipher text. The attributes can satisfy with the corresponding privilege tree. Encryption keys are created with algorithms to ensure that each key is unique.

For encrypting a file, first a user has to request a public key from the attribute authorities. Public key and master key are already generated (PK, MK). Based on user attributes public key is given to the user to encrypt and upload a file.

$$\text{Setup} \longrightarrow (\text{PK, MK})$$

$$\text{Key generator :(PK, MK, } A^{U}) \longrightarrow \text{SK}_{u}$$

$$\text{Encrypt (PK, M, \{Tp\} p } \epsilon \text{ \{0,....., r-1\})} \longrightarrow \text{(CT, VR)}$$

For the encrypted file a set of privilege access is allocated which performs operations such as read, write, modify, update. The message is converted to cipher text (CT) and is verified using verification set (VR).

Decryption is the process of converting encrypted data back into its original form. Decryption requires a secret key. It is the reverse process of encryption. For decryption, public key, secret key, cipher text is the main function to produce message. If the user wants to read the message, before the cloud servers can verify it, then only the user can decrypt the file.

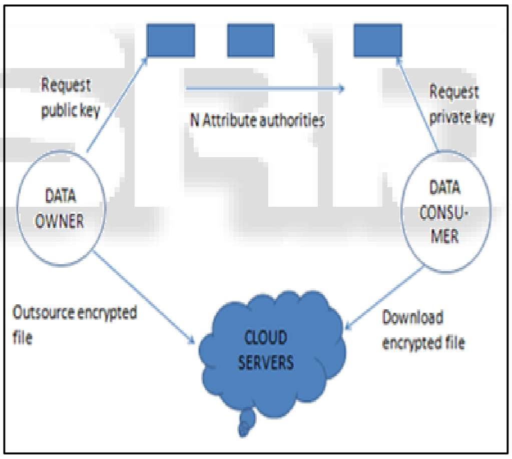
$$\text{Decrypt (PK, SK}_{u}\text{,CT)} \longrightarrow \text{M}$$

A. Attribute Based Encryption:

Less effort is paid for Identity based encryption scheme for user privacy hence we go for Attribute based encryption scheme. In this scheme based on user's attributes, the issuer issues private keys so that the key is not known to other user and the issuer [2]. In this ABE scheme, we propose AnonyControl and AnonyControl-F mechanism which allows cloud servers to control user's access privileges without knowing their identity information.

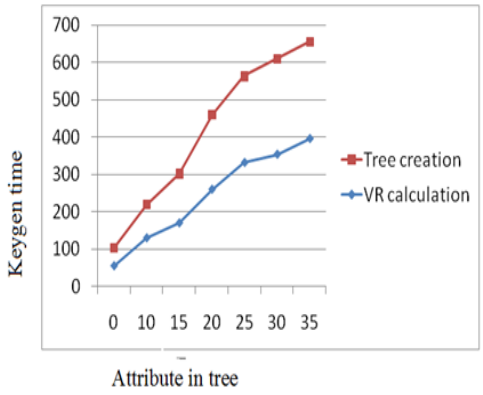
In this paper a public key is generated to the data owner to upload a file. Using the private key the data of the file are encrypted. The encrypted message can be downloaded by the user using his own private key. The file can be decrypted only if the user public key matches with the public key of the data owner [4].

B. Architecture:



C. Advantages:

The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. Both AnonyControl and AnonyControl-F provides detailed analysis on security and performance.



IX. CONCLUSION

In this paper we use an efficient mechanism known as user revocation. In this user revocation mechanism, when a user gets out of cloud network his identity is erased and data's are updated. The particular user cannot use his public key to upload a file. Also here a third party auditor is involved to check whether the file is encrypted and check the type of file. This user revocation mechanism is one of the challenges for future applications.

REFERENCES

[1] A.Sahai and B.Waters, "Fuzzy Identity-Based Encryption" in advances in cryptology. Berlin, Germany: Springer-Verlag, 2005, pp, 457-473.
[2] V.Goyal, O.Pandey, A.Sahai, and B.Waters, "Attribute-Based Encryption for fine grained access control of encrypted data", in Proc. 13Th CCS, 2006, pp.89-98.
[3] J.Bethencourt, A.Sahai, and B.Waters, "Cipher text-policy attribute-based encryption", in Proc, IEEE SP, May 2007, pp 321-334.
[4] M.Chase, "Multi-authority attribute based encryption", in Theory of Cryptography. Berlin, Germany: Springer-Verlag, 2007, pp.515-534.
[5] S.Yu, C.Wang, K.Ren and W.Lou,"Attribute – based data sharing with attribute revocation", in Proc.5th ASIACCS, 2010, PP.261-270.
[6] Cipher text policy Attribute Based Encryption Toolkit. Available: http//acsc.csl.sri.com/cp abe/, accessed 2014.