ISSN 2319 – 2518 www.ijeetc.com
Special Issue, Vol. 1, No. 1, March 2015
National Level Technical Conference P&E- BiDD-2015
© 2015 IJEETC. All Rights Reserved

Research Paper

AN IMPACT OF IMPLEMENTING VARIOUS ATTRIBUTE ENCRYPTION TECHNIQUES IN A PUBLIC CENTRIC CLOUD

Sonia Jenifer Rayen[1]*, Gunaseelan N[1], P Sridharan[1] and Vamsi Krishna S[1]

*Corresponding Author: Sonia Jenifer Rayen, ✉soniya@jeppiaarinstitute.org

The main issue we consider in this paper is providing security to the private data in public centric cloud storage. It is very important to provide security to our own data in a public storage like cloud. Here we address various cryptographic techniques which produce higher order and efficient data security in cloud. Here we survey various architecture that provide some core traditional mechanisms for addressing privacy are no longer flexible, so new approaches need to be developed to address security issue. During this chapter we tend to assess however security, trust and privacy problems occur within the context of cloud computing and discuss ways in which within which they'll be addressed.

Keywords: Centric cloud storage, Cryptographic techniques, IdAM, Attribute Based Encryption (ABE), Key Policy Attribute Based Encryption (KP-ABE)

INTRODUCTION

Public centric cloud storage allows you to store your data online and you can access it from any device like PCs, laptops, tablets, smart phones, etc. You keep au fait of the encoding keys. And solely folks with those keys will access your valuable knowledge. Safeguard Encryption for Cloud Storage protects your data in the cloud. you can Securely share your confidential data with your team members and even share with third-parties without compromising on security. To achieve these good data encryption algorithms should be chosen for the best security and performance.

Mobile readers allow you to view your encrypted files on iOS and Android devices. To avoid destruction and loss of personal data in Cloud, the data in virtual machines need to be backed up by replication on different physical machines in different data centre locations on a regular basis. Protecting data against alteration requires SPs deploying enterprise applications in Cloud and processing personal data to log input or

[1] Jeppiaar Institute of Technology, Chennai, India.

alterations of the data. In order to prevent personal data from being disclosed to unauthorised persons, cloud should implement strong encryption whenever the VM Manager moves or stores data within the cloud. Unauthorised access to personal data must be avoided by implementing an IdAM in the security framework. Finally, the cloud architecture needs to ensure that it is possible for data controllers to meet the obligations laid down in the Data protection directive.

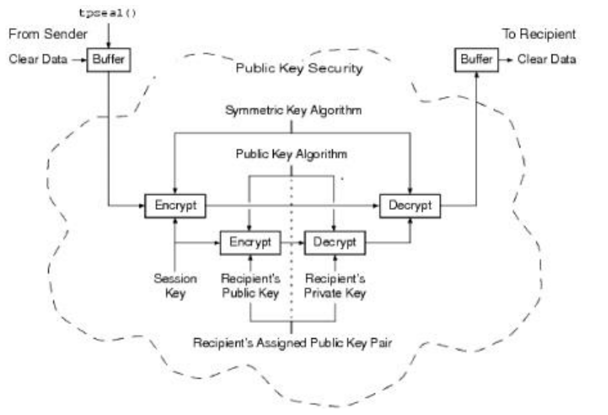
VARIOUS ENCRYPTION SECURITY ARCHITECTURE USED IN CLOUD ENVIRONMENT

Attribute-Based Encryption (ABE)

It is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes. In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. A 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 a identity-based encryption that incorporates attributes as inputs to its cryptographic primitives.

Data's are encrypted using a set of attributes so that multiple users who possess proper can decrypt. Attribute-Based Encryption (ABE) not only offers fine-grained access control but also prevents against collusion. J. Benaloh, has proposed a scheme in which a file can be uploaded without key distribution and it is highly efficient. C. Dong has explored that knowledge the info the information} cryptography theme doesn't need a trusty data server. The server can perform encrypted searches and updates on encrypted data without knowing the plaintext or the keys to decrypt. But in this scheme the server knows the access pattern of the users which allows it to infer some information about the queries.

Figure 1: ABE – Architecture



To improve the quantifiability of the on top of solutions, one-to-many coding strategies like attribute based mostly coding (ABE) are often used. Sahai and Waters initial introduced the attribute based mostly coding (ABE) for enforced access management through public key cryptography. The main aspects ar to produce flexibility, measurability and fine grained access management. In classical model, this system can be achieved only when user and server are in a trusted domain .So, the new access control scheme that is Attribute Based Encryption (ABE) scheme was introduced which consist of key policy attribute based encryption (KP-ABE). As compared with classical model, KP-ABE provided good access control. However it fails with respect to flexibility and scalability when authorities at multiple levels are considered. In ABE theme each the user secret key and also the cipher text ar related to a group of attributes. ABE is enforced for one-to several encoding within which cipher-texts aren't essentially encrypted to 1 explicit user, it's going to be for quite one range of users.Akinyele et al investigated using ABE to generate self-protecting EMRs, which can either be stored on cell phones or cloud servers so that EMR could be accessed when health provider is in offline also.

Drawbacks

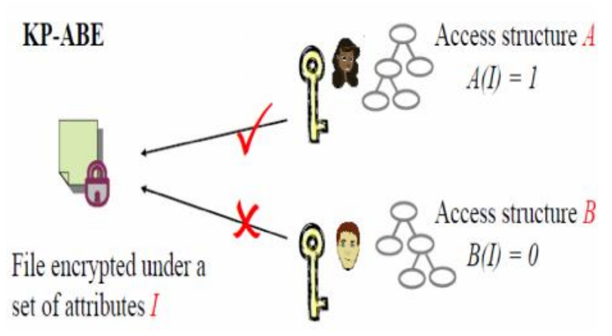
The use of a single Trusted Authority (TA) in the system. Single Trusted Authority (TA) not only creates a load bottleneck, but also have key escrow problem since the TA can access all the encrypted files. This opens the door for potential privacy exposure.

Key Policy Attribute Based Encryption

It is the modified form of the classical model of Attribute based encryption. In this scheme, attribute policies are well associated with keys and data is associated with attributes. Key Policy Attribute Based Encryption scheme is a public key encryption technique that is designed for one-to-many communications. This theme permits a knowledge owner to scale back most of the procedure overhead to cloud servers. the utilization of this coding theme KP-ABE provides fine-grained access management.

The data file that's encrypted is keep with the corresponding attributes and also the encrypted encoding key. as long as the corresponding attributes of a file or message keep within the cloud satisfy the access structure of a user's key, then the user is in a position to decode the encrypted DEK, that is employed to decode the file or message.

Figure 2: Key Policy Based Encryption



Drawbacks of KP-ABE

The main disadvantage in the scheme is that the data owner is also a Trusted Authority (TA) at the same time. If this theme is applied to a PHR system with multiple information house owners and users, it might be inefficient as a result of then every user would receive several keys from multiple house owners, albeit the keys contain constant set of attributes.

Expressive Key Policy Attribute Based Encryption

In the key policy Attribute based encryption, the primitive enables senders to encrypt messages with a set of attributes and private keys are associated with access tree structure that specifies which all the cipher texts the key holder is allowed to decrypt. In most ABE systems, the cipher text size grows linearly with the number of cipher text attributes and the only known exceptions only support restricted forms of threshold access policies. This communicatory key-policy attribute based mostly coding (KP-ABE) schemes giving non-monotonic access and with constant cipher text size. The personal keys have quadratic size within the variety of attributes. They scale back the amount of pairing analysis size to a continuing, that seems to be a singular feature among communicative KP-ABE schemes. this is often a lot of economical than KP-ABE.

Cipher Text Policy Attribute Based Encryption

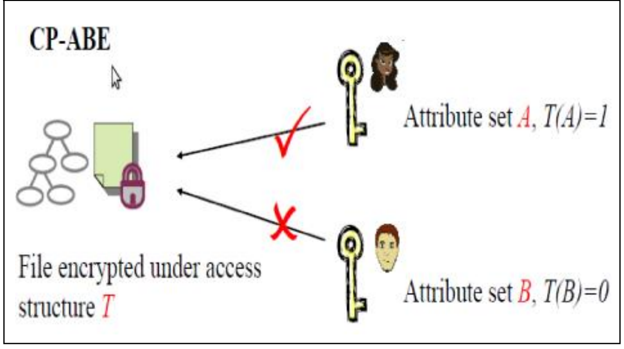
In many distributed systems a user should solely be able to access information if a user possess an exact set of credentials or attributes. To store the information and mediate access management a trusty server is that the solely technique for imposing such policies The confidentiality of the information are compromised, if any server storing the information is compromised. The storage server is un trusted if the data can be confidential by this technique. Previous Attribute-Based Encryption systems used to the outsourced data can be described and built policies into user's keys.

While in this system attributes are used to describe a users credentials, and a party encrypting data determines a policy for decrypt. In cipher text-policy attribute-based encryption (CP-ABE), depends how attributes and policy are associated with cipher texts and users decryption keys. In a CP-ABE scheme, a cipher text is associated with a monotonic tree access structure and a user's decryption key is associated with set of attributes. In this scheme the cipher text is encrypted with a tree access policy chosen by an encryptor, while the decryption key is generated with respect to a set of attributes. As long because the set of attributes should satisfy the tree access policy and it will be related to a coding key with a given cipher text, the key will be accustomed rewrite the cipher text. However, basic CP-ABE schemes are far from enough to support access control in modern enterprise environments, require considerable flexibility and efficiency in specifying policies and managing user attributes.

Cipher text Policy Attribute Based Encryption

This theme, the encryptor will fix the policy, United Nations agency will rewrite the encrypted message. The policy is fashioned with the assistance of attributes. In CP-ABE, access policy is distributed at the side of the ciphertext. we tend to propose a technique during which the access policy needn't be sent at the side of the cipher text, by that we tend to area unit ready to preserve the privacy of the encryptor. The planned construction is demonstrably secure below call linear Diffe-Hellman assumption. Cipher text Policy Attribute Set based mostly encoding (CP-ASBE)—a replacement kind of CP-ABE. It organizes user attributes into a algorithmic set based mostly structure and permits users to impose dynamic constraints on however those attributes could also be combined to satisfy a policy. in a very CP-ABE theme, coding keys solely support user attributes that area unit organized logically as one set, thus users will solely use all potential combos of attributes in a very single set issued in their keys to satisfy policies. to unravel this drawback, cipher text-policy

Figure 3: CP-ABE – Architecture



attribute-set based mostly encoding is introduced.

Thus, by grouping user attributes into sets such that those belonging to a single set have no restrictions on how they can be combined, CP-ASBE can support compound attributes without sacrificing the flexibility to easily specify policies involving the underlying singleton While restricting users to use attributes from a single set during decryption can be thought of as a regular CP-ABE scheme, the challenge in constructing a CP-ASBE scheme is in selectively allowing users to combine attributes from multiple sets within a given key while still preventing collusion.

Drawbacks

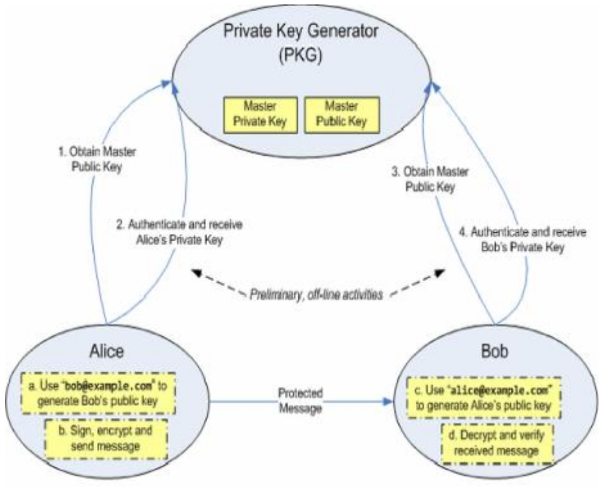
Constructing a CP-ASBE theme is in by selection permitting users to mix attributes from multiple the cloud suppliers. However, HABE uses divisional traditional kind policy and assumes all attributes in one conjunctive clause square measure administrated by a similar domain master by multiple domain masters. A similar attribute is also administrated per specific policies, that is tough to implement in apply.

Identity Based Encryption (IBE) and Hierarchical Identity Based Encryption (HIBE)

Hierarchical Identity Based Encryption (HIBE) is the hierarchical form of a single IBE [3]. The concept of HIBE scheme can help to explain the definition of security. In a regular IBE (1-HIBE) theme, there's only 1 personal key generator (PKG) that distributes personal keys to every users, having public keys square measure their primitive ID (PID) discretionary strings. A two-level HIBE (2-HIBE) theme consists of a root PKG, domain PKGs and users, all of that ar related to PID's.A users public key consists of their PID and their domains. In a 2-HIBE, users retrieve their private key from their domain PKG.

The personal key PK is cipher by Domain PKGs of any user in their domain, their domain secret key-SK will be provided and antecedent requested from the basis PKG. Similarly, is for range of sub-domains. There conjointly includes a sure third party or root certificate authority that enables a hierarchy of certificate authorities: Root certificate authority problems certificates for alternative authorities or users in their various domains. the first system doesn't give such structure. However, a hierarchy of PKG is reduces the employment on root server and permits key assignment at many levels.

Figure 4: ID-Based Encryption – Architecture


Private Key Generator (PKG)
Master Private Key
Master Public Key
1. Obtain Master Public Key
2. Authenticate and receive Alice's Private Key
3. Obtain Master Public Key
4. Authenticate and receive Bob's Private Key
Preliminary, off-line activities
Alice
a. Use "bob@example.com" to generate Bob's public key
b. Sign, encrypt and send message
Protected Message
Bob
c. Use "alice@example.com" to generate Alice's public key
d. Decrypt and verify received message

Drawbacks

The main disadvantage of this system is key management overhead. Letting each user obtain keys from every owner PHR wants to read would limit the accessibility.

Distributed Attribute - Based Encryption

In DABE, there'll be AN impulsive variety of parties to take care of attributes and their corresponding secret keys. There square measure 3 differing kinds of entities in an exceedingly DABE theme one. (1) The master is liable for the distribution of secret user keys. However, master isn't concerned within the creation of secret attribute keys. (2) Attribute authorities square measure accountable to verify whether or not a user is eligible of a particular attribute; during this case they distribute a secret attribute key to the user. AN attribute authority generates a public attribute key for every attribute it maintains; this public key are obtainable to all or any the users. Eligible users receive a customized secret attribute key over AN documented and trustworthy channel. (3) Users will cipher and rewrite messages. To cipher a message, user ought to formulate the access policy in separative traditional kind (DNF).To rewrite a cipher text, a user wants a minimum of access to some set of attributes that satisfies the access policy. The most advantage of the answer is every user will acquire secret keys from any set of the Trustworthy Authorities (TAs) within the system.

Table 1: Comparison of Techniques

Fetures	ABE	KP-ABE	IBE	HABE	DABE
Access control	High	High	Low	High	Low
Scalability	High	Low	Low	High	Low
Efficiency	Low	Low	Low	Low	High
Flexibility	High	Low	Low	Low	Low
Security	Low	Low	High	Low	High

Drawbacks of DABE

It requires a data owner to transmit an updated cipher text component to every non-revoked user. While sharing the information the communication overhead of key revocation is still high.

CONCLUSION

By scrutiny numerous situations of cryptographical techniques employed in cloud it's necessary to conclude a best and economical approach to supply security for our knowledge. totally different attributes primarily based secret writing (ABE) schemes which will be employed in cloud systems for versatile, climbable and fine grained access management. Addressing the protection and privacy considerations of cloud- primarily based PHR system by integration advanced cryptographical techniques, like ABE, into PHR system. By exploitation acceptable cryptographical techniques, patients will shield their valuable tending data against part trustworthy cloud server. in the meantime patients gain full management access over their PHR files, by process fine-grained, attribute-based access privileges to chose knowledge users. The attribute-based secret writing model is increased to support operations.

The dynamic policy management model supported by this method. With security and privacy the non-public Health Records ar maintained. In future, to supply high security and privacy for Private Health Record (PHR), the prevailing Multi authority attribute {based|based mostly|primarily primarily based} secret writing can be any increased to proactive Multi authority attribute based secret writing.

REFERENCES

1. Boneh D and Franklin M (2001). "Identity-Based Encryption from the Weil Pairing", Proc. of CRYPTO'01, Santa Barbara, California, USA.

2. Dong C, Russello G and Dulay N (2010), "Shared and Searchable Encrypted Data for Untrusted Servers", *J. Computer Security*, Vol. 19, pp. 367-397.

3. Goyal V, Pandey O, Sahai A and Waters B (2006), "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", Proc. 13th ACM Conf. Computer and Comm. Security (CCS'06), pp. 89-98.

4. ID-Based Cryptography for Secure Cloud Data Storage.

5. Jahid S, Mittal P and Borisov N (2011), "Easier: Encryption-Based Acess Control in Social Networks with Efficient Revocation", Proc. ACM Synp. Information, Computer and Comm. Security, March.

6. Ostrovsky R, Sahai A and Waters B (2006), "Attribute-Based Encryption with Non-Monotonic Access Structures", Proc. of CCS'06, New York.

7. Privacy, Security and Trust in Cloud Computing.

8. Ruj S, Nayak A and Stejmenovic I (2011), "Distributed Access Control in Clouds", Proc. IEEE 10th Intl. Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology, pp. 568-588.