ISSN : 2231-0711

An Impact of Implementing Various Cryptographic Techniques Efficiently in a Public Centric Cloud

Thamil kumaran V.C[1] , Chithra Mol C.R[2] , & Sai Prasath[3]

[1]Asst Professor , Computer Science & Engineering Department ,
Annai Mathammal sheela engineering college, India
E-Mail :vcthamilkumaran@gmail.com

[2]UG Scholar ,Computer Science & Engg Department ,
Annai Mathammal sheela engineering college, India, Member – CSI , IEEE
E-Mail :chithramolrpmc@gmail.com

[3]PG Scholar ,Computer Science & Engg Department ,
Annai Mathammal sheela engineering college, India,
E-Mail : sai.sampath82@gmail.com

***Abstract*- 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. In this chapter we assess how security, trust and privacy issues occur in the context of cloud computing and discuss ways in which they may be addressed.**

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 stay in control of the encryption keys. And only people with those keys can access your valuable data. 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 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:

a) Attribute based encryption (ABE)
b) Expressive attribute based encryption (EABE)
c) Cipher text policy attribute based encryption
d) Expressive key policy attribute based encryption
e) Cipher text policy attribute set based encryption
f) Hierarchical attribute based encryption
g) Distributed attribute based encryption

A. 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.

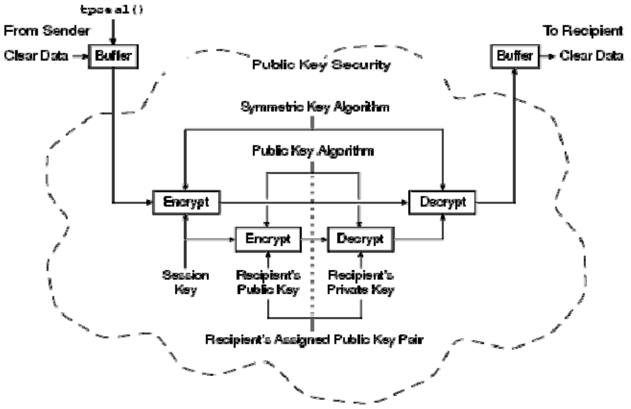

Fig 1: ABE – Architecture

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 the data encryption scheme does not require a trusted 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. To realize fine grained access control, the usual public key encryption based schemes and either incur high key management overhead, or require encrypting multiple copies of a file using different users keys. To improve the scalability of the above solutions, one-to-many encryption methods such as attribute based encryption (ABE) can be used. Sahai and Waters first introduced the attribute based encryption (ABE) for enforced access control through public key cryptography. The thought for these models is to provide security and access control. The main aspects are to provide flexibility, scalability and fine grained access control. 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 scheme both the user secret key and the cipher text are associated with a set of attributes. ABE is implemented for one-to many encryption in which cipher-texts are not necessarily encrypted to one particular user, it may be for more than one number 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.

B. 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. The keys are well associated with the policy that is to be satisfied by the attributes that are associating the data can decrypt the data. Key Policy Attribute Based Encryption scheme is a public key encryption technique that is designed for one-to-many communications. This scheme enables a data owner to reduce most of the computational overhead to cloud servers. The use of this encryption scheme KP-ABE provides fine-grained access control. Each file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key corresponding to a set of attributes in KPABE, which is generated corresponding to an access structure. The data file that is encrypted is stored with the corresponding attributes and the encrypted Data Encryption key. Only if the corresponding attributes of a file or message stored in the cloud satisfy the access structure of a user's key, then the user is able to decrypt the encrypted DEK, which is used to decrypt the file or message.

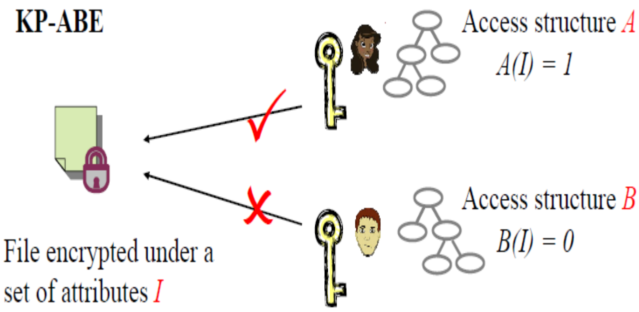

Fig 2: KP-ABE – Architecture

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 scheme is applied to a PHR system with multiple data owners and users, it would be inefficient because then each user would receive many keys from multiple owners, even if the keys contain the same set of attributes.

C. 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 expressive key-policy attribute based encryption (KP-ABE) schemes allowing for non-monotonic access and with constant cipher text size. The private keys have quadratic size in the number of attributes. They reduce the number of pairing evaluation size to a constant, which appears to be a unique feature among expressive KP-ABE schemes. This is more efficient than KP-ABE.

D. Cipher Text Policy Attribute Based Encryption:

In several distributed systems a user should only be able to access data if a user possess a certain set of credentials or attributes. To store the data and mediate access control a trusted server is the only method for enforcing such policies The confidentiality of the data will be compromised, if any server storing the data 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 users' 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 as the set of attributes should satisfy the tree access policy and it can be associated with a decryption key with a given cipher text, the key can be used to decrypt 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.

E. Cipher text Policy Attribute based Encryption:

This scheme, the encryptor can fix the policy, who can decrypt the encrypted message. The policy can be formed with the help of attributes. In CP-ABE, access policy is sent along with the ciphertext. We propose a method in which the access policy need not be sent along with the cipher text, by which we are able to preserve the privacy of the encryptor. The proposed construction is provably secure under Decision Bilinear Diffe-Hellman assumption. Cipher text Policy Attribute Set Based Encryption (CP-ASBE)- a new form of CP-ABE. It organizes user attributes into a recursive set based structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. In a CP-ABE scheme, decryption keys only support user attributes that are organized logically 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, cipher text-policy attribute-set based encryption is introduced.

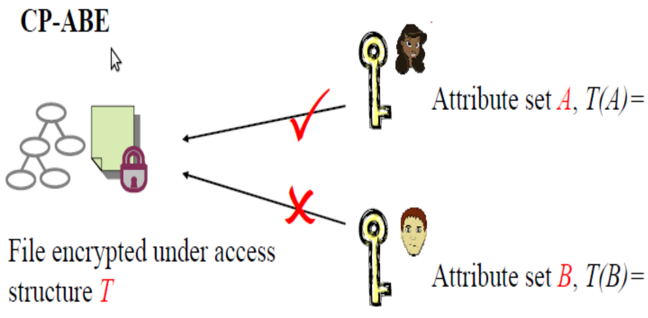
CP-ABE
Attribute set *A*, *T*(*A*)=
File encrypted under access structure *T*
Attribute set *B*, *T*(*B*)=

Fig 3: CP-ABE – Architecture

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 scheme is in selectively allowing users to combine attributes from multiple the cloud providers. However, HABE uses disjunctive normal form policy and assumes all attributes in one conjunctive clause are administrated by the same domain master by multiple domain masters. The same attribute may be administrated according to specific policies, which is difficult to implement in practice.

F. 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) scheme, there is only one private key generator (PKG) that distributes private keys to each users, having public keys are their primitive ID (PID) arbitrary strings. A two-level HIBE (2-HIBE) scheme consists of a root PKG, domain PKGs and users, all of which are associated with 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.

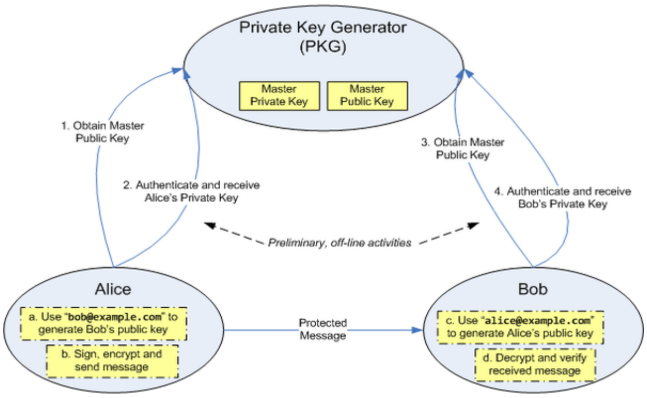
Private Key Generator (PKG)
Master Private Key
Master Public Key
1. Obtain Master Public Key
2. Authenticate and receive Alice's Private Key
3. Obtain Master Public Key
4. Authenticate and receive Bob's Private Key
Preliminary, off-line activities
Alice
a. Use "bob@example.com" to generate Bob's public 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

Fig 4: ID-Based Encryption – Architecture

The private key PK is compute by Domain PKGs of any user in their domain, their domain secret key-SK can be provided and previously requested from the root PKG. Similarly, is for number of sub-domains. There also includes a trusted third party or root certificate authority that allows a hierarchy of certificate authorities: Root certificate authority issues certificates for other authorities or users in their respective domains. The original system does not allow for such structure. However, a hierarchy of PKG is reduces the workload on root server and allows key assignment at several levels.

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.

G. Distributed Attribute - Based Encryption:

In DABE, there will be an arbitrary number of parties to maintain attributes and their corresponding secret keys. There are three different types of entities in a DABE scheme 1. The master is responsible for the distribution of secret user keys. However, master is not involved in the creation of secret attribute keys. 2. Attribute authorities are responsible to verify whether a user is eligible of a specific attribute; in this case they distribute a secret attribute key to the user. An attribute authority generates a public attribute key for each attribute it maintains; this public key will be available to all the users. Eligible users receive a personalized secret attribute key over an authenticated and trusted channel. 3. Users can encrypt and decrypt messages. To encrypt a message, user should formulate the access policy in Disjunctive Normal Form (DNF).To decrypt a cipher text, a user needs at least access to some set of attributes which satisfies the access policy. The main advantage of the solution is each user can obtain secret keys from any subset of the Trusted Authorities (TAs) in the system.

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.

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

CONCLUSION:

By comparing various scenarios of cryptographic techniques used in cloud it is necessary to conclude a best and efficient approach to provide security for our data. Different attributes based encryption (ABE) schemes that can be used in cloud systems for flexible, scalable and fine grained access control. Addressing the security and privacy concerns of cloud- based PHR system by integrating advanced cryptographic techniques, such as ABE, into PHR system. By using appropriate cryptographic techniques, patients can protect their valuable healthcare information against partially trustworthy cloud server. Meanwhile patients gain full control access over their PHR files, by defining fine-grained, attribute-based access privileges to selected data users. The attribute-based encryption model is enhanced to support operations. The dynamic policy management model supported by this technique. With security and privacy the personal Health Records are maintained. In future, to provide high security and privacy for Personal Health Record (PHR), the existing Multi authority attribute based encryption could be further enhanced to proactive Multi authority attribute based encryption.

REFERENCE:

[1] ID-Based Cryptography for Secure Cloud Data Storage

[2] Privacy, Security and Trust in Cloud Computing

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

[4] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security, vol. 19, pp. 367-397, 2010.

[5] S.Jahid,P.Mittal,N.Borisov,"Easier: Encryption- Based Acess Control in Social Networks with Efficient Revocation ," Proc. ACMSynp. Information ,computer and Comm.Security, Mar.2011

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

[7] R.Ostrovsky, A. Sahai, and B. Waters. "Attribute-based encryption with non-monotonic access structures". Proc. of CCS'06, New York, NY, 2007.

[8] S.Ruj,A.Nayak, and I.Stejmenovic,'Distributed Access Control in Clouds,"Proc.IEEE10th Intl Conf.Theory and Applications of Cryptographic Techniques: Advances in Cryptology,pp. 568-588,2011.

AUTHORS:

Rajadurai J, student research scholar of Sathyabama university pursuing M.E (Computer science & Engineering) have done many research in the field of cryptography and cloud storage proposed this article with my faculty guidance.

Thamil kumaran V C Assistant Professor of Annai Mathammal Sheela Engineering College doing research under the area of cloud computing and conducted many workshop and conferences in the area of the same.

C.R Chithra Mol final year student of Annai Mathammal Sheela Engineering college have made many research in Cloud computing Area under the guidance of Research Scholors. Have visited Many Industries to collect data regarding Security in cloud. Proposed many presentation about cloud & its security computing. Member of Computer society of India, IEEE.