A Comparative Study of Different Attribute Based Encryption Models for Cloud Data Security

S Kranthi Kumar
Assistant Professor
Department of CSE
VNRVJIET
Hyderabad,India

Dr. P V Siva Kumar
Associate Professor
Department of CSE
VNRVJIET
Hyderabad, India

M Venkata Krishna Rao
Assistant Professor
Department of CSE
VNRVJIET
Hyderabad,India

Abstract :*With the rapid development of the distributedcomputing and internet architectures, there is an exponential demand for data processing and sharing resources in the cloud environment. The third-party provider needs to implement trusted access control and confidentiality for the cloud customers. Also, it is highly recommendable for the large scale applications to support one to many communications to reduce the data encryption and decryption mode. Ensuring the security and access of the cloud data is a major issue, as users often store their sensitive data with the third party authorities, but these TPA may be interested. The access control mechanism ensures that trusted clients are able to access data and unauthorized clients are not able to access data from the remote cloud server. Most of the client's data stored in the remote cloud server are highly sensitive and need to secure against third party authorities and unauthorized users. In this paper, traditionally, Attribute based encryption and decryption such as CP-ABE, KP-ABE,HPABE, Homomorphic ABE approaches are studied with different security parameters. Also, an analysis of the different attribute based encryption techniques along with limitations and security challenges are discussed.*

Keywords— *ABE, Cloud security, Encryption andDecryption Algorithm*

I.INTRODUCTION

To protect the data and privacy from disclosure, a number of schemes have been proposed for data access control in cloud computing. Before applying an access control scheme in a practical system, it is indispensable to evaluate its performance in various aspects, such as efficiency and flexibility. The cloud service providers adopted various methodologies to provide a more secure and trust worthy environment for their customers. They prefer to encrypt customer's sensitive data before uploading it to cloud. The prime goal of attribute-based encryption model is to provide security and access control. They identified users' attributes as the main component and used in both secret key as well as in cipher text. When the attributes of secret key and cipher text are identical as threshold *d*, decryption occurs. Another significant feature of ABE is collision resistance. The only flaw of this scheme is users' public keys are required by the data owner in encryption. This drawback forbids the implementation of this model in real environment due to involvement of monotonic attributes. The traditional cryptosystem framework based on public key infrastructure (PKI) can achieve data security, confidentiality and non-repudiation along with limitations. In order to encrypt data, the third party provider needs to obtain the authorized user's public keys and then communicate the cipher data to the individual authorized user, which increases the bandwidth and processing overhead[1-4].

Third party cloud servers are vulnerable to different type of message integrity attacks[1-4].

Sahai and waters proposed a fuzzy Identity based encryption scheme in which a descriptive attributes set are considered as identity for encryption and decryption process. For the privacy or secret key k_{AS} corresponds to the attribute set S. We can decrypt the data using $k_{AS'}$ corresponds to the attribute set s' and satisfies the condition $|S \cap S'| < d$,where d is the minimum number of attributes. With the immense growth of cloud services, data servers are needed to be trusted as well as safe enough in order to store much confidential sensitive information. Numbers of algorithms involving various access control schemes are developed to achieve data

security in cloud. But with the rapid growth of technology, now-a-days data are stored in distributed cloud servers. Distributed cloud servers are data servers responsible for storing data in different servers which is by default exposed to other data owners.

Some frequently used symmetric cryptographic algorithms are AES, DES, IDEA, TDES, Blowfish and RC6. RSA and ECC can be categorized under asymmetric cryptographic algorithms. Symmetric cryptographic algorithms generally consider a common key both for the process of encryption and decryption. But, the asymmetric cryptographic algorithm uses separate keys for encryption and decryption. Here, a public key is considered for encryption and a private key is used for decryption. The initial or first tier of security is formed by implementing digital signature scheme[5]. Cloud computing environment in mostly insecure, as it is used worldwide. All the data are needed to be encrypted prior to uploading it on cloud. Several classical public key encryption approaches can be implemented to enhance security, but it also gives rise to some issues which are mentioned below

1. For the encryption process to be executed, data owners require user's public key.
2. The storage overhead is increased, as for a single plain text there exist many public keys.
3. In order to resolve the above issues, Sahai and Waters introduced a new technique and named it as attribute-based encryption (ABE) technique in the year 2005. At first they developed the basic algorithm of attribute based encryption which is modified and extended by various different models in the subsequent period of time [5]. In the above approach, users' identity is considered as attributes and set of attributes are used together to encrypt and decrypt data.

Attribute based encryption (ABE)

The main objective of the ABE is to provide better security and access control mechanism. ABE can be stated as a special type of public key encryption method which is responsible for encryption and decryption according to the attribute values. In the above approach, both the secret key and cipher text depends on attributes. The cipher text is decrypted by decryption algorithm, when attributes of user keys matches attributes of cipher text. If the number of matching is equivalent with the minimum threshold d, the decryption algorithm is executed successfully.

Key Policy Attribute Based Encryption(KP-ABE)

The traditional attribute based encryption technique is modified and extended in order to overcome the above issues. Every individual user is associated with an access tree structure. Threshold gates represent the nodes of access trees, whereas attribute values are assigned to leaf nodes. User's secret key has the responsibility of representing access tree structure. Cipher text includes set of attributes and the secret keys are merged with monotonic access structures in order to choose the particular cipher text which is meant for that user to decrypt[6-7].

Chaos based hash functions have gained a lot of attraction by the researchers in the field of cloud computing and mobile computing. Due to the limited computing power, chaotic orbits will become non-periodic. Most of the traditional chaos based hash functions are processed in sequential model, which restricts their execution speed and performance on the mobile computing. In [8] a parallel keyed hash function using the chaos-based algorithm is proposed. The limitations in the parallel chaos model were presented in [9]. Various experimental results have been performedon arbitrary messages and finally concluded that the parallel chaotic hash function is not secured against the statistical attacks.

To overcome this problem, complex chaotic-based hashing techniques are developed which are non-linear, random and dynamic in nature. It can be represented by either discrete or continuous systems. Henon mapping and logistic mapping can be categorized under discrete, whereas Lorenz and Rossler system comes under continuous. This system is highly responsive to initial conditions. Lyapunov exponents are one of the important components of chaotic system which decides whether the given system is chaotic or not. Our proposed scheme involves various logical functions and is developed according to the complex temporal behavior and provides high sensitivity to the initial constraints of the high-dimensional chaotic maps. The main objective of a chaotic-hashing system is the convergence property in the complex chaotic systems. The features responsible for this convergence are:- a) Both are deterministic. b) Both are complex and not predictable. c) In chaotic system, a small change in the initial conditions can affect and reflect a huge change in the output.

I. Related Work

Symmetric Key Encryption (SKE): Symmetric Key Encryption is a special cryptographic approach which applies a shared secret key for both the process of encryption and decryption. The key which is used for encryption is also considered for the process of decryption. Therefore, both the sender and receiver must have the same shared secret key. The sharing of secret key can become a major disadvantage of encryption scheme. If an unauthorized user gets access to this key, then the cloud data can be compromised[78-81].

Public Key Encryption (PKE): In the process of Public Key Encryption, two different keys are used for encryption and decryption process. Among two of these keys, one key is public and the other one is private. The public key is distributed publicly and the private key is only available to the receiver. All messages are encrypted with receiver's public key and the process of decryption is carried out by the private key.

The conventional attribute based encryption approach is modified and extended in the subsequent time. Two other techniques are developed such as, Cipher-text Policy Attribute Based Encryption (CP-ABE) and the Key Policy Attribute Based Encryption (KP-ABE). CP-ABE and KP-ABE are two extended versions of traditional ABE scheme.

Also, summarized key management models with different cloud properties are shown in Table1.

Model	Security	Scalability	Cryptographic Method
Key management at customer side	Yes	Yes	Symmetric
Key management at cloud server side	No	Yes	Asymmetric
Key management at both sides(cloud and client)	Yes	Yes	Symmetric
Key management in distributed central server	No	no	Asymmetric

Basic Steps in ABE scheme in the Cloud Environment:

Bilinear Maps:

Let G be a cyclic group of prime order p generated by group element g. Let G_p be the group of prime order p.

Let a map m: $G \times G \rightarrow G_P$ is said to be bilinear maps if it satisfies the following conditions:

1. $m(e1^x, e\ 2^y) = m(e1, e\ 2)^{xy}$

   for all e1,e2∈G and x,y∈G_p

   and $x,y \in Z_p$
2. m is efficiently computable.
3. Non- Degenerate
   a. $m(g,g) \neq 1$

Most of the ABE schemes have four steps as shown in Fig 1:

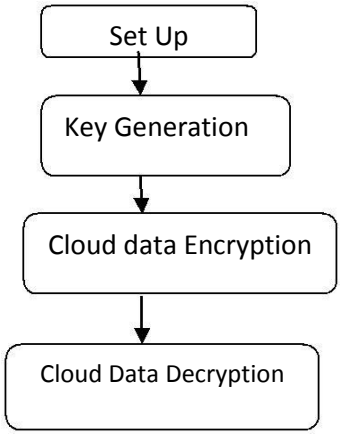

Fig 1: Cloud based ABE Scheme

Setup: This phase setup public key parameters of theuser using the mathematical group theory functions. **Key Generation:** This phase generates private key assecret key , depending on the set of user's attribute and policies.

Cloud Data Encryption: Each cloud user encrypts thedata using his public key along with the credentials.
Cloud Data Decryption: This phase enables a receiverwith the matching attributes and polices to decrypt the cloud data.
A basic requirements of attribute based access control mechanisms in a cloud computing environment are as follows:

- The implemented approach should be distributed in nature which prevents single point failure.
- This system should be secure against collision.
- The system should enable user efficient revocation.
- It should support forward and backward security.
- Forward security describes that a new user cannot decrypt any cipher text which was previously deployed.
- Backward security means that a revoked user cannot decrypt any cipher text that will be deployed in the cloud.

Attribute-Based Encryption for Non-Monotonic Access Structures:

All the formerly described models support monotonic access structures and there is no representation of negative constraints in key's access. Thus, Ostrovsky presented an attribute-based encryption with non-monotonic access structure in the year 2007. Non-monotonic access structure can induce negative constraint which was not possible in case of monotonic access structure[10]. There are four algorithms which describe this model, those are

- Setup (d): The numbers of attributes contained by cipher texts are specified by parameter d.
- Encryption (M,Y,PK): Encryption algorithm uses message M, set of attributes Y and a random value S. The algorithm procures cipher text E as output.
- Key Generation (~A,MK,PK): If and only if the attributes of cipher text satisfy the access structure ~A, key generation algorithm generates a key D.
- Decryption (CT,D): Cipher text and the generated key are taken as input to the decryption algorithm which produces the plain text M.

The issue arises in this approach is that, it increases the data overhead extensively by adding negative attributes which are unable to relate with encrypted data. The said issue makes this model inefficient and complex.

Hierarchical Attribute-Based Encryption Model

Wang proposed Hierarchical Attribute-BasedEncryption model. As the model represents a hierarchical structure of key generation, it contains a root master (RM) which communicates with multiple domain masters (DMs). Further DMs communicate with numbers of enterprise users. HABE model is defined by the following algorithms

- Setup (K)→(params,MK0):For input, the algorithm chooses a large security parameter K. It results with output parameters params and root master key MK0.
- CreateDM(params,MKi, PKi+1) → (MKi+1): It checks if RM or DM generates master keys for the DMs directly by involving params and its master key.
- CreateUser(params,MKi, PKu, PKa) → (SKi,u, SKi,u,a): Eligibility criteria of U is verified for a. If it is eligible, user identity secret key and user attribute secret key are produced for U by considering params and master key. Else, results "NULL".
- Encrypt(params; f ;A; {PKa|a E A})→(CT):The encryption algorithm accepts file f, DNF access policy A, public keys for attributes as input and results cipher text CT.
- Decrypt(params, CT, SKi,u,{SKi,u,a|aECCj}→(f): The decryption algorithm accepts j-th conjuctive clause CCj, params, cipher text, user secret key and attribute keys as input to produce the original message. These model can be implemented in cloud enterprise environment and proxy re-encryption. This can't be implemented practically because all attributes in a conjunctive clause is controlled by a common domain authority and same attribute is controlled by multiple domain authorities.

[6] introduced a new mechanism of parallelizing CP-ABE approach . The main objective of this approach is to parallelize and enhance the traditional CP-ABE. They studied a pre-existing approach of CP-ABE to

encounter performance bottleneck. The authors tried to parallelize key generation algorithm and encryption/decryption algorithm through a multithreading scheme. They altered the traditional CBC mode with CTR mode in AES cryptographic algorithm. This enables the system to enhance its performance significantly. The researchers evaluated and validated their proposed scheme with the traditional CP-ABE and found huge difference in terms of performance. Further work may be done in future for hardware acceleration and implementation of this model in real world scenario.

[7] proposed a extended ABE scheme with file hierarchy concept [7]. They considered the conventional CP-ABE scheme at first, and then they modified it for an efficient inclusion of file hierarchy concept. The data files used for sharing information mostly have multi-level hierarchy. The original CP-AABE scheme is unable to handle this multi-level hierarchy. All the layers access structures are merged together to form an unit of combined access structure. After that the hierarchical files are encrypted with the combined newly formed access structure. Through this, both cipher text and its attributes are shared. Thus, it will reduce the storage space and encryption time. This model provides more security than that of the previous one. The authors simulated their research work and found that, the approach shows significant performance in terms of encryption and decryption. The only drawback of this approach is that:- while considering heavy volume of files, the performance decreases. This flaw can be studied and resolved in future works.

[8] introduced an extended ABE with a new key policy. The mentioned key policy is a decentralised approach applicable for privacy protection. Decentralised approach adds an advantage over centralised authority scheme. Here secret keys are provided to every individual authority and authorities are allowed to use these keys on users irrespective of the knowledge of GID. This is an advantage in security point of view, that is: if some authorities are compromised, they are not able to get users' attributes from their GID. The authorities are independent of each other like the other schemes. GID has the ability to combine secret keys of various authorities and prevents collision attacks. They experimented and found that, computation and communication costs do not require re-initialisation.

[9] researched and identified one of the important flaw of ABE, that is:- With increase of complexity, pairing of decryption also increases and it results very high overhead. Some approaches have been proposed with ABE containing outsourced decryption to reduce the decryption overheads. In a cloud server a key is used for transformation of ABE cipher text to normal cipher text which encounters very less overhead in the process of conversion to plain text. The authors worked on verifiable outsourced decryption, where verifiability ensures whether the transformation is done correctly or not. They validated their work in an outsourcing environment and noticed remarkable reduction of computation overhead.

[10] developed a new approach and named it as Privacy Preserving Constant CP-ABE. It is responsible to decrease the cipher text to constant size and mentioned numbers of attributes. It emphasizes on privacy preservation by a hidden policy construction scheme. The authors also introduced and Privacy Preserving Attribute-Based Broadcast Encryption model. This enhances the properties of the traditional Broadcast Encryption. By comparing with the conventional approach, the proposed model achieves more flexibility as the broadcast message is encrypted by a hidden access policy with or without explicit receivers[11-12]. This approach decreases storage and communication overhead significantly. As this only satisfy conjunctive access policy, further future work can be done to satisfy disjunctive access policy. There is also no need to include wildcard attributes in order to support a hidden access policy.

Conclusion

Cipher policy based encryption schemes consume high computation overhead for each user in the encryption and decryption process. If the number of attributes or policies increases, then the size of the access tree structure increases in the encryption and decryption process. Traditional cipher policy based models are independent of hash integration in the encryption and decryption process. Data confidentiality and inefficient data access methods are the major issues which block the cloud users to store their high dimensional data. With more and more cloud based applications are being available and stored on various cloud servers, a novel multi-user based privacy protection mechanism need to design and develop to improve the privacy protection on high dimensional data. In the future work, an optimized Cipher policy based attribute encryption and decryption model will be

designed and devloped to overcome the traditional limitations of the traiditional attributed based encryption schemes for large data.

References

[1] S. Zhu, Y. Han and Y. Wei, "Controlling Outsourcing Data in Cloud Computing with Attribute-Based Encryption", "International Conference on Intelligent Networking and Collaborative Systems", pp. 257-261, 2015.

[2] G. S. Tamizharasi, B. Balamurugan and R. Manjula, "Attribute Based Encryption with Fine-grained Access Provision in Cloud Computing ", "Proceedings of the International Conference on Informatics and Analytics. ACM", 2016.

[3] B. Chandrasekaran and R. Balakrishnan, "Attribute Based Encryption Using Quadratic Residue for the Big Data in Cloud Environment", "Proceedings of the International Conference on Informatics and Analytics. ACM", 2016.

[4] A. Kaci and T. Bouabana-Tebibel, "Access Control Reinforcement over Searchable Encryption ", "IEEE IRI 2014, August 13-15, 2014, San Francisco, California, USA", pp.130-137, 2014.

[5] J. Li, Y. Shi and Y. Zhang, "Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage", "International Journal Of Communication Systems International Joirnal of Communication System,2015.

[6] L. Li, X. Chen and H. Jiang, "P-CP-ABE: Parallelizing Ciphertext-Policy Attribute-Based Encryption for Clouds ", "17th IEEE/ACIS International Conference on. IEEE", pp.1-6, 2016.

[7] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen and W. Xie, "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing", "IEEE Transactions on Information Forensics and Security 11.6", pp.1265-1277, 2016.

[8] L. Warren and H. Chi, "Securing EHRs via CPMA Attribute-Based Encryption on Cloud Systems ", "Proceedings of the 2014 ACM Southeast Regional Conference. ACM", 2014.

[9] F. Xhafa, J. Li, G. Zhao, J. Li, X. Chen and D. S. Wong, "Designing cloud-based electronic health record system with attribute-based encryption", "Multimedia Tools and Applications 74.10 (2015)", pp. 3441-3458, 2014.

[10] H. Yan, X. Li and J. Du, "Secure Personal Health Record System with Attribute-Based Encryption in Cloud Computing", "Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing", pp.329-332, 2014.

[11] Y. Zhang, D. Zheng, Q. Li, J. Li and H. Li, "Online/offline unbounded multi-authority attribute-based encryption for data sharing in mobile cloud computing", "Security and Communication Networks 9.16 ", pp. 3688-3702, 2016.

[12] L. Zhenpeng, Z. Xianchao and Z. Shouhua, "Multi authority attribute based encryption with attribute revocation", "IEEE 17th International Conference on Computational Science and Engineering", pp. 1872-1876, 2014.