Analysis of Effective Encryption Techniques for Attribute-Based System in Storage Cloud

Priyanka S[1], Nagesha A G[2]

[1]PG Student, Dept. of Computer Science and Engineering, Acharya Institute of Technology, Karnataka, India
[2]Associate Professor, Dept. of Computer Science and Engineering, Acharya Institute of Technology, Karnataka, India

---***---

Abstract - *Cloud computing is one in all most the computing paradigm that enables each user to store the data remotely and also providing on-demand service. The issues in data storage are data security and privacy. The authorized user enforced information access control system that should be provided before users of cloud that possess the freedom for supplying sensitive information to the storage cloud. The data should be protected and encrypted before it is sent. In ABE which enables encoded information through controlled access that uses policies accessed and attributes. ABE was introduced for minimum computational overhead and obtaining controlled access fine-grain. This ABE scheme an attribute are very important that controls user's access and generating public key for encryption of information attributes. In this paper, we are discussing various schemes and an encryption technique mainly includes ABE, KP-ABE, CP-ABE, CP-ASBE, and H-ABE and also provides limitations.*

***Key Words*: Cloud storage, Data Privacy, Cipher Policy, Access Control, ABE.**

1. INTRODUCTION

Cloud computing exist a secure technology. It provides resources to mobile device or user personal computers. Cloud enables to share the software resources and also hardware resources. Cloud storage is mainly used as core technology. It is more popular nowadays. The user obtains effective client service due to integrate resources in the cloud computing. Cloud service provider build a cloud environment, thus provide user services. The two challenges in cloud storage lead to be handled. First is, personal information holds the set of attributes of user information. Nowadays personal information of each user is hazard because user identity has no privacy, so there must be need to protect user information concerned with identity privacy [1]. Second is, data confidentiality focuses on access control and data privacy. It has less focus on privilege control and includes the operation to be controlled whereas other user's uses infer sensitive information.

The primitive cryptographic public key called attribute-based encryption (ABE). ABE enables secure public key sharing with fine grained. In ABE two kinds are proposed: CP-ABE and KP-ABE. The CP-ABE identifies clearly in cipher text and KP-ABE assigned within private key. In effective ABE system, user encoded text and private keys is defined within collection of attribute and access policy. A specified key can be decrypted with specified cipher text, they both matches only if policy and attributes [7]. To protect the data it must be encrypted, before the data is uploaded. The attributes must be protected with security and privacy.

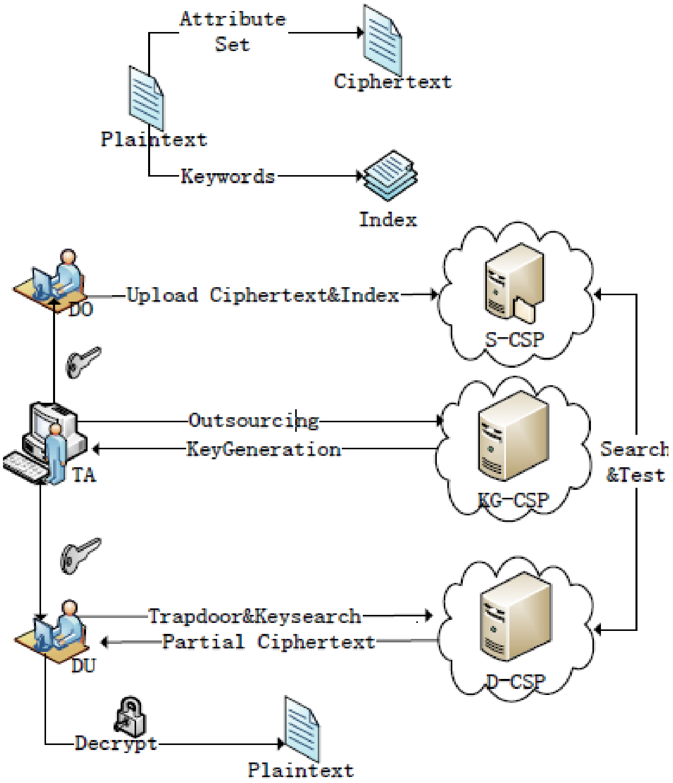

Fig -1: System Architecture

In this architecture the main modules are Data Owner (DO), Data User (DU), Trusted Authority (TA) and Cloud Service Provider (CSP). CSP are allocated for Storage, Key Generation, and Decryption [1]. DO generating indexes for some keywords and upload encoded information with the specific indexes. DU is responsible for choosing keywords to create trapdoor and decoding information. TA initializes system parameters and generates attribute private keys and trapdoor. CSP allocates data storage service for every individual to outsource their file in storage cloud.

1.1 REQUIREMENT

According to these studies, the classification and description of these necessities then we use essential necessities to investigate the theme. The main requirements provide evaluation of performance and evaluation of function for encryption technique [3].

Functional evaluation

1] Data confidentiality: The data-owner provides encryption of each data before uploading each data to the cloud. So, the cloud storage server and unauthorized user cannot understand the secret encryption information.
2] Scalability: When the approved users increase, then cloud storage server will execute with efficiency. Therefore, the performance of the cloud storage server cannot be affected by number of authorized users.
3] Forward secrecy: The attribute that satisfies the access-policy, if any user leaves the attribute that may be prevented from accessing the plain-text. Then the data can be exchanged even after the each user leaves the attribute.
4] Backward secrecy: The attribute that satisfies the access-policy, if user holds any attribute that may be prevented from accessing the plain-text. Then the data can be exchanged even before the each user holds the attribute.
5] Fine-grained access control: Each user severally has access right which can vary for every user. Though the user exists within the same group, then their access might not be a similar.

Performance evaluation

1] Computing cost: The effective public auditing can be achieved by analyzing the users, cloud storage and TA service cost on computing resources.
2] Storage cost: Client uploads the data to cloud storage without local duplicate copy of data, and then analyze the users, cloud storage and TA service cost on resources.

2. LITERATURE SURVEY

In this paper [8], Waters et al, proposed "Fuzzy-Identity Based Encryption" concept that permits error-tolerance within private key and public key which is used for cipher text encryption. Here mainly two applications of F-IBE scheme used are ABE and biometrics. It hides the general public key that was want to encipher the cipher-text is intriguing. It is simplified version of Bilinear Diffie-Hellman Decisional assumption. It motivates few open problems that is creating attributes from different authorities, uses distance metrics within identities.

In IBE scheme, each data adopts random strings in the process of keys so used for encoding and also for decoding. Therefore each decoding key is generalized by key authority and along with an encryption random key [4]. In Hierarchical-IBE represented as ordered structure of single IBE. The idea of H-IBE scheme will facilitate to clarify the security. In a very regular IBE i.e. 1-H-IBE scheme, there's just single private-key-generator (PKG) so circulate non-public key via every individual that holds primitive ID i.e. PID arbitrary strings. The 2-H-IBE (two-level H-IBE) associated with their PID and also includes root PKG, users and domain PKG. Therefore authorized user public key includes with their PID and also with their domains.

3. ENCRYPTION TECHNIQUE

The different existing schemes in cloud computing that provide data confidentiality, access control and security. The authorized users ought to share sensitive information with others supported to the receiver which able to fascinate access policies in the shared system.

A. Attribute-Based Encryption (ABE)

ABE prescribed with management accessed over non-private key cryptography. It mainly provides access control, security, scalability, flexibility. The users and server are within trusted domain only then system success is achieved. Therefore new scheme that is ABE includes KP-ABE that provides controlled accessed fine-grained [5]. It lacks with flexibility and scalability when their authorities at different multiple levels. A collection of attributes are combined with cipher text and users secret key. Therefore cipher text is not encrypted to particular user; it's mainly up to one-to many encryption techniques. It is a principle of IBE so includes attribute as an input to cryptographic native. It not solely offers fine-grained access management however additionally prevents against collusion.

ABE Drawbacks: A disadvantage is only one trusted authority in scheme. It has key escrow problem because it access every encrypted files. It allows privacy potential exposure.

B. Key Policy-ABE (KP-ABE)

In KP-ABE scheme survive non-private key encryption defined as one to many inter-communication. It is extension form of ABE. The keys solely related over an attribute that act as unit combining with information decryption. It mainly reduces the computational overhead that enables the data-owner and cloud server [6]. Each file is encoded adopting symmetric-data encryption key (DEK), then its encrypted again using public key associated with collection of attributes in this scheme.

KP-ABE Drawbacks: The main drawback is data-owner concurrently trusted authority. It's inefficient when multiple data-owner and multiple users is applied with this scheme. When authorized user tend to receive several key against different owners.

C. Cipher Text Policy-ABE (CP-ABE)

CP-ABE is the altered form of ABE. In many distributed systems each user ought to solely be ready to access information if each user possesses an explicit collection of attribute. If the server is not trusted then information is private within the system. While during this system the attributes describe each user credentials, and a celebration encrypting information determines decode or decryption. In CP-ABE policy and attribute are assigned within each individual cipher text and decrypted key. Therefore users' decrypted key is along with collection of attributes and cipher text is along with access tree structure. The cipher text is generated using tree access structure associated by encryption and decryption keys are assigned with collection of attribute. It is efficient and flexible in managing each user attribute.

CP-ABE Drawbacks: Decoded key solely assist each individual attribute as logically well-ordered as single, thus each individual will solely need all available attributes in an exceedingly collection of issued keys that satisfies all policy.

D. Cipher Text Policy-Attribute-Set-Based Encryption (CP-ASBE)

It is modified scheme of CP-ASBE, applied within attribute immediate revocation capabilities, rather than periodical revocation. It associated with each user attributes really into an algorithmic collection which establishes structures and permits every individual to force aggressive constraints. In this strategy user attributes are only supported by decryption keys, so coordinated as one set. Therefore every individual will solely benefit complete potential sequence of an attributes during one set announced and satisfies all policies. Therefore CP-ASBE is proposed, grouping each user attributes really into sets specified those happiness to one set don't have any restrictions on however they'll be combined.

CP-ASBE Drawbacks: The cloud service provider allows each user to combine attributes. The same attributes could also be administrated in step with specific policies that is troublesome to implement in follow.

E. Hierarchical-ABE (H-ABE)

In H-ABE strategy uses ordered keys that are used in H-IBE scheme. Furthermore it is used in DNF that convey the access policy and the identical domain authority. There are mainly five roles proposed that are cloud storage service, root authority, data-owner, data users and domain authority. The part of cloud storage service permits the data owner that will allocate information and store information for each user. A part of data-owner specifies distributing information and enciphering information for each user [9]. Root authority creates domain keys and also system frameworks later circulate them. Domain authority mainly manages itself at different levels, each user in the domain and to assign keys to them. The key authority adopts method of hierarchical form.

H-ABE Drawbacks: The main disadvantage of H-ABE strategy is doesn't take care of numerous rate assignments and also cannot provide aggregate credentials conveniently.

Table -1: Comparisons between multiple types of encryption schemes

METHODS	**ABE**	**KP-ABE**	**CP-ABE**	**H-ABE**
Efficiency	Bad	Bad	Good	Bad
Access control	Good	Good	Good	Good
Security	Good	Bad	Good	Bad
Scalability	Bad	Bad	Bad	Good
Flexibility	Good	Bad	Good	Bad

3. CONCLUSIONS

In this paper, we mainly discussed about encryption techniques: ABE, H-ABE, KP-ABE, CP-ABE, and CP-ASBE then illustrate their limitations. There are many encryption techniques that are classified with monotonic or non-monotonic schemes. An access policy in an every individual private key is within KP-ABE. A policies accessed in an encoded information is within CP-ABE. The ABE schemes have lots of properties: 1) each attribute have secret key, public key and random polynomial. Therefore each user cannot combine attributes to recover the information. 2) The data-owner needs to pre-define these attributes that data-owner uses and does not care about multiple users in system. Therefore, ABE strategies are mostly applicable in the area of proxy re-encryption.

REFERENCES

[1] Jiguo Li, Xiaonan Lin, Yichen Zhang and Jinguang Han, "KSF-OABE: Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage", IEEE Transactions on Services Computing, Volume: PP, Issue: 99, March 2016.

[2] J Li, X Huang, J Li and X Chen, "Securely Outsourcing Attribute-Based Encryption with Check ability", IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201-2210, Oct 2013/Jul 2014, doi:10.1109/TPDS.2013.271.

[3] Chi-Wei Liu, Wei-Fu Hsien, Chou-Chen Yang, and Min-Shiang Hwang, "A Survey of Attribute-based Access Control with User Revocation in Cloud Data Storage", International Journal of Network Security, Vol.18, No.5, PP.900-916, Sept. 2016.

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

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

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

[7] Soni Kumari, Dr. S B Sonkamble, “Survey on cloud security using attribute based encryption”, International Journal of Multidisciplinary Research and Development, Volume 2, Issue 12, Online ISSN: 2349-4182 Print ISSN: 2349-5979, December 2015.

[8] Harshada Deshmukh, Rahul kapse, “Attribute Based Encryption Techniques and its Applications”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 5, May 2016.

[9] A Sahai and B Waters, “Fuzzy Identity-Based Encryption”, Proc. of EUROCRYPT’05, Aarhus, Denmark, 2005.