Attribute based Encryption in Cloud Computing – A Review

B. Firdaus Begam, PhD
Assistant Professor
Karpagam Academy of Higher Education,
Coimbatore

M. Sasikala, PhD
Assistant Professor
PSGR Krishnammal College for Women,
Coimbatore

ABSTRACT
Emerge of cloud computing technology over the world has caused a revolution in internet. The virtual usage of platform, infrastructure and software over cloud has provided an environment where the user can store and run the application from anywhere. This has led to think about security over data stored over cloud. In this paper, Attribute Based Keyword Search over encrypted data in cloud are discussed which provides security over searching of data based on keyword.

Keywords
Cryptography, Cloud Computing, Attribute Based Keyword Search.

1. INTRODUCTION
Cloud computing deals with both hardware and software data center to satisfy user requirement [1]. According to National Institute of Standards and Technology (NIST) cloud computing has the capability to enable ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [2].

Ian Foster defined cloud computing as, "a large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet" [3].

A cloud is a pool of virtualized computer resources. It can host various workloads under different platforms, helps to monitor real-time need of resources and other related workloads. Cloud is empowered by virtualization, by running hypervisor over application it is running. One main and important feature used by cloud to maximize it computing power for performing various task is virtualization. Cloud stands strong when compared to grid computing as it leverages virtualization.

Cloud computing provides customers a virtual computing infrastructure where they can store data and run applications. However, cloud computing also presents some unique security challenges as cloud operators are expected to manipulate client data without being fully trusted. From facilitating remote access to data, to the digitalization of the education system, cloud technology has touched our lives in more ways than we realize. Today, almost every application we use is powered by cloud computing. If you want to take business online (because that is where people are), you need to get your hands on this revolutionary technology as soon as possible.[4].

2. ATTRIBUTE BASED ENCRYPTION (ABE)
The cloud has moved to next generation computing with critical applications and real time applications. The main aspects are to provide flexibility, scalability and fine-grained access control. This can be achieved only when user and server are in a trusted domain in classical model.

Encryption in ABE is easy and secure and inexpensive compared to another encryption. The ABE is secure because the encrypted data contains the attributes rather than the data. The attribute-based encryption makes the application to be secure. the performance of the ABE is high compared to other encryption methods. Thus, attribute-based encryption is the solution to all cloud applications in future.

In ABE, encryption is performed as one-many approach that means the encryption is not done for only one user but for a greater number of users. So, this method was not more expressive to define a control system. So, changes made in policies are enforced in encryption techniques to maintain the authentication and security of the data [5][6]. This results in two different streams of algorithm based on key policies and cipher text policies as,

i. Key policy based ABKS (KP-ABKS) and
ii. Cipher text policy based ABKS (CP-ABKS)
iii. Identity based Cryptography

2.1 Key Policy Attribute Based Encryption (KP-ABE)
In KP-ABE approach, attribute policies are associated with keys and data is associated with attributes. Public key encryption technique follows one-many communications. Data attributes are represented as access tree structures to the user, with leaf nodes are based on attributes and act as threshold gate for access of information/data. The secret key is generated based on tree structure. Cipher text is associated with set of attributes and for decryption the key is associated with monotonic access tree structure [7].

2.2 Cipher Text Policy Attribute Based Encryption
In this approach the data and attributes are used in generation of keys. The keys are generated based on attributes associated with data which can be used for encryption and decryption. CP-ABE performs in the reverse of KP-ABE, where each user key is associated with set of attributes and the cipher text is based on access tree structure [8].

In attributed based approaches the authority is responsible for generation of Master Key (MK), Public Key (PK) and User

secret keys using Setup and Key Generation algorithm for encryption of data. The authorized users are responsible for decrypting data based on access structures [5].

2.3 Identity-Based Cryptography

Identity-Based cryptography mechanism is used for securing cloud data using attribute-based approach. The main idea consists in using Identity Based Cryptography to provide a per data pair of keys. This potentially offers a more lightweight key management approach. Each client acts as a PKG and generates their Identity-Based Cryptography Public Elements (IBC-PE). These IBC-PE are used to compute ID-based keys which are used to encrypt the data before it is stored and shared in the cloud. For every different data, the client computes the corresponding private and public keys based on the IBC-PE and a local secret key SK.[9]

3. KEY POLICY - ATTRIBUTE BASED TEMPORARY KEYWORD SEARCH (KP-ABTKS)

In Key-Policy Attribute Based Temporary Keyword Search (KP-ABTKS) schemes, the data owner generates a searchable cipher text related to a keyword and the time of encrypting according to an arbitrary time interval and generates a search token for intended keyword to find the cipher text. Then, he/she sends the generated token to the cloud to run the search operation. By receiving the token, the cloud looks for the documents contain the intended keyword. The search result on a cipher text is positive, if

(i) data user's attributes satisfy the access control policy,
(ii) time interval of the search token encompasses the time of encrypting, and
(iii) searches token and the cipher text are related to the same keyword. [10-12]

3.1 Architecture

Key-Policy Attribute-Based Temporary Keyword Search (KP-ABTKS) consists of four entities:[10]

- ✓ Data Owner
- ✓ Data User
- ✓ Cloud Server
- ✓ Trusted Third Party (TTP).

1) ***Data owner:*** Encryption of the document using arbitrary access control policy is done by data owner and outsourced to cloud.

2) ***Data user***: Entity or user looking for document which is holding the keyword and encrypted in determined time interval.

3) ***Cloud Server (CS):*** CS entity store huge amount of data which are encrypted and accepts the keyword token to search the encrypted documents for the user. If the document matches it is shared with the user.

4) ***Trusted Third Party (TTP):*** Entity generates secret key based on the attributes set and sends credentials of the user through authenticated channel as shown in Fig. 1.

4. SECURITY ANALYSIS

Security analysis performed on two threat models, namely an honest but curious cloud provider and a malicious user that intends to get extra-information from outsourced data.

i) ***Privacy*** - Privacy is a critical concern with regards to cloud storage since clients' data reside among distributed public servers.[13][14].

ii) ***Data Confidentiality*** — when dealing with cloud storage environments, confidentiality implies that client's data have to be kept secret from both cloud provider and other users [14].

iii) ***Deduplication Concern*** - this approach leads to encrypt the same content several times, and then, to decrease the storage abilities of the cloud provider. Proof of Ownership Frameworks (PoW) enables the cloud server to check a client data possession, based on a static and short worth (for instance, hash esteem) [15].

iv) ***Data Sharing:*** Sharing of customer data with trusted parties [16]

v) ***Reliability:*** User data can be backed up reliable [16].

vi) ***Efficient Retrieval:*** Time taken for retrieving data from public cloud storage service models are comparable [14][16].

5. CONCLUSION

Cloud computing is the next generation environment which is causing and will cause huge change in IT field. The main hurdle and issue in growing path of cloud computing is handling privacy and security of data. This field has open wide field of research in data security and privacy protection, resulted in number of algorithms. In this chapter the security and privacy issues over cloud computing and various cryptographic techniques are discussed. Attribute based encryption and decryption schema and its types KP-ABE, CP-ABE and Identity Based approaches were discussed.

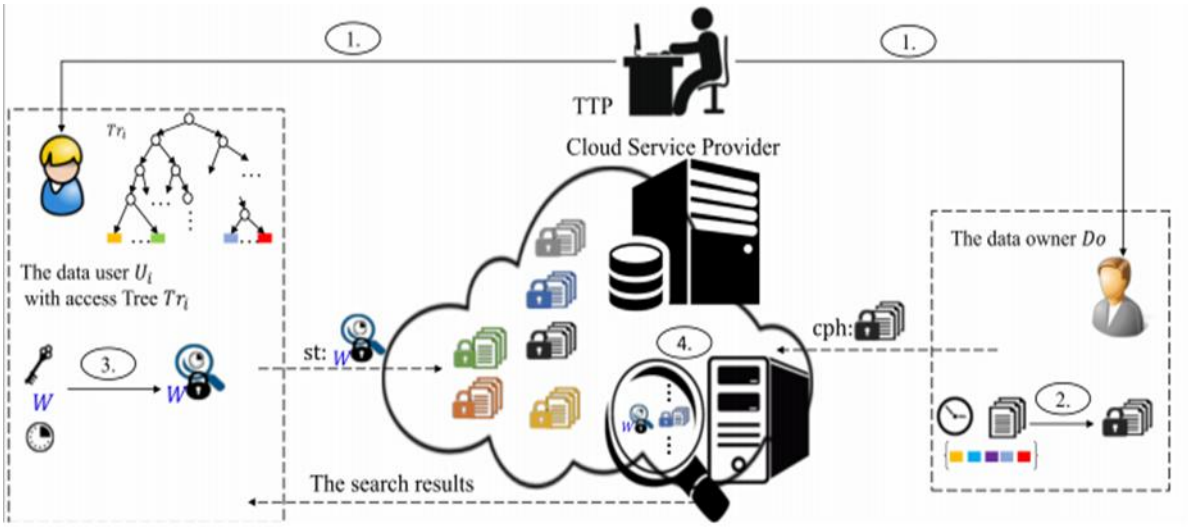

Fig 1: KP-ABTKS Architecture [10]

6. REFERENCES

[1] N. Leavitt. 2009. Is cloud computing really ready for prime time?, Computer, 42(1), 15–25.

[2] P. Mell and T. Grance. 2009. The NIST definition of cloud computing, National Institute of Standards and Technology, 53(6).

[3] Ian Foster, Yong Zhao, Ioan Raicu, Shiyong Lu. 2008. Cloud Computing and Grid Computing 360-Degree Compared. Grid Computing Environments Workshop.

[4] Furht, B., 2010. Cloud computing fundamentals. In Handbook of cloud computing, Springer, Boston, MA, 3-19.

[5] Anup R. Nimje , V. T. Gaikwad, H. N. Datir. 2013. Attribute-Based Encryption Techniques in Cloud Computing Security: An Overview, International Journal of Computer Trends and Technology – 4(3).

[6] N. Chaudhari, M. Saini, A. Kumar and G. Priya, 2016. A Review on Attribute Based Encryption. 8th International Conference on Computational Intelligence and Communication Networks (CICN). Tehri,380-385.

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

[8] J. Bethencourt, A. Sahai and B. Waters, 2007. Ciphertext-policy attribute-based encryption, IEEE Symp. Security and Privacy.

Anand, Darpan & Khemchandani, Vineeta & Sharma, Rajendra, 2013. Identity-Based Cryptography Techniques and Applications (A Review). Proceedings - 5th International Conference on Computational Intelligence and Communication Networks, CICN. 343-348.

[9] Mohammad Hassan Ameri, Mahshid Delavar, Javad Mohajeri, Mahmoud Salmasizadeh, 2018, A Key-Policy Attribute-Based Temporary Keyword Search scheme for Secure Cloud Storage. IEEE Transactions on Cloud Computing. 660 – 671.

[10] Hui Yin, Yinqiao Xiong, et.al., 2019. A Key-Policy Searchable Attribute-Based Encryption Scheme for Efficient Keyword Search and Fine-Grained Access Control over Encrypted Data. Electronics. 8(3).

[11] Kai Zhang , Ximeng Liu, et.al., 2020. A Secure Enhanced Key-Policy Attribute-Based Temporary Keyword Search Scheme in the Cloud. IEEE Access. 8.

[12] C. Zhong, J. Zhang, Y. Xia, and H. Yu. 2010. Construction of a trusted SaaS platform. SOSE 2010. 244-251.

[13] B. R. Kandukuri, P. V. Ramakrishna, and A. Rakshit, 2009. Cloud security issues. SCC 2009. 517-520.

[14] Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. 2010. Security issues for cloud computing. International Journal of Information Security and Privacy (IJISP). 4(2). 36-48.

[15] Kamara, Seny & Lauter, Kristin. 2010. Cryptographic Cloud Storage. Financial Cryptography and Data Security. 136-149.