EasyChair Preprint

№ 5744

A Comparative Study on Cipher Text Policy Attribute Based Encryption Schemes

Badal Pradhan, Bhagwan Singh, Abhishek Bhoria and Ashutosh Kumar Singh

June 7, 2021

A Comparative Study on Cipher Text Policy Attribute Based Encryption Schemes

Badal Pradhan
Dept. of Computer Applications
National Institute of Technology
Kurukshetra, India
bdprdhn36@gmail.com

Bhagwan Singh
Dept. of Computer Applications
National Institute of Technology
Kurukshetra, India
ibhagwanji0123@gmail.com

Abhishek Bhoria
Dept. of Computer Applications
National Institute of Technology
Kurukshetra, India
abhishek6198@gmail.com

Dr. Ashutosh Kumar Singh
Dept. of Computer Applications
National Institute of Technology
Kurukshetra, India
ashutosh@nitkkr.ac.in

Abstract

Cloud Computing is one of the demanding services in the current times. It should be said that it has become a necessity of small to large scale business to have a dedicated cloud computing service. The security, privacy and other features must be kept intact in all conditions. This high demand has made cloud computing being utilized in several ways such as in Fog ,VANETs, Mobile cloud computing and many others. All these are based on a common encryption scheme known as CP-ABE(Ciphertext Policy Attribute Based Encryption Scheme) it is an enhanced form of ABE which allows owner to set the attribute of user within the encryption. As a result even after sharing the data stays secure and this is one of the reasons which compelled many to use this as a base for their targeted encryption scheme. This is quite flexible to be utilized in a vehicle, mobile and in fog systems which are based off of cloud computing. In this review paper our contribution lies within the range of qualitative analysis of ABEs and CP-ABEs. The comparison will be shown in tabular form on the basis on the criteria of an ideal encryption scheme. This could be helpful for selection of a suitable scheme for a specific type of tasks in cloud computing.

Keywords—cloud computing, CPABE, ABE, VANETs, Fog , security, privacy, access control ,encryption ,decryption

I. INTRODUCTION

The requirement of keeping the flow of data continuous and available on demand to the user gave rise to the Cloud Services, [2] The most appropriate technology for such is cloud computing. Since its nature makes it scalable and flexible for implementation of above requirements. It allows users to share data with authorized users but with its quality nature there lies its weakness as well. Cloud computing is quite insecure without any proper infrastructure because once a user shares their data they loses any control over it . Any unauthorized user may probably decipher it and collect the information for themselves. This makes the system based on such insecure techniques to be more susceptible to attacks from hackers.[1] In 2005 an encryption scheme was introduced by Sahai and Waters known as ABE (Attribute Based Encryption Scheme), The objective was to eloquent execution of cloud computing with fine security and access control. In this scheme the cipher text and key depend upon a certain set of attributes to identify the authorized user and correctly decrypting the data. A year later another scheme was

brought into existence, it was known as KP-ABE (Key Policy Attribute Based Encryption) this embedded access policy within the user's attribute to provide a better control to the user. It also had a flaw in the system which didn't allow the users to select who can decrypt the data, the user was allowed to just set the attribute that can describe the data. It was better than ABE but still lacking in a way that compromises the entire aspect of access control. In 2007 So, a scheme was put in action that allowed users to attach a tag to each attribute this was ABE with a non monotonic access structure the contribution of Ostrovsky. In the same year another scheme named CP-ABE (Ciphertext Policy Attribute Based Encryption) Bethencourt et al. this scheme allowed the user to set attributes which describes user's credentials and the users encrypting the data establishes, who can decrypt. This solved the problem of KP-ABE but still had some weaknesses of it's own . The review will be focusing on how the scheme CP- ABE is being modified in-order to cover those gaps and also investigate on this scheme's selection over other schemes in the first place.

The Most Defining Features of an Encryption Scheme

A. Security

[]The ideal security must have protection against all types of currently being used attacks. The most recent example would be Ransomware attacks that locks away a user's data and demands payment to be unlocked. So the information of the user must be kept safe in every situations. For that few measures are as follow

- Top Tier firewall protection.
- Improved Intrusion Detection System.
- Applications and Database equipped with dedicated firewall protection.
- Storage of Encrypted Data in Cloud Infrastructure.

- Installment of Top level Physical Security to Datacenters.

B. Privacy

It is most simple yet essential feature in Cloud Computing which corelates with both the security and access control. The 'privacy' still is a standalone features that need attention. The best privacy would be

- Avoidance of Data loss from Client's Database
- Making system Data Leakage proof
- Allowing the complete control to disclosing the data to the user.

C. Access Control

The access control determines the user's access to the data set by the data owner. The high profile data accessed by an unauthorized user can cause serious problem for the client. So the data must be protected form unauthorized users and you need more than just username and password authentication.

- Emergency Lockdown Features
- Ease of Establishing and maintain access control group.
- Instant configuration of current access rights.
- Ability of Integration with currently popular softwares.

II. QUALIFYING ASPECTS TO BE AN IDEAL ATTRIBUTE BASED ENCRYPTION SCHEME

[7]-[13]A standard system was necessary for a suitable scheme to be selected for Cloud Computing which gave us the list of aspects which we will be used to evaluate the quality of the Encryption Schemes.

A. User Accountability

This is a case of an improper conduct committed by an authorized user ,when they share their private key with an unauthorized user. Here the misconduct must be dealt with and handling of such issues should be included within the system.

B. User Revocation

The revoking of the rights of an user who has exited the system. This plays a major role in ensuring the security of other users who shares the same space.

- Identifying the currently inactive user.
- revoking the rights of users according to owner.
- Maintaining an honest cloud service.

C. Scalability

This is one of those key features which was used to promote the Cloud Computing services at its dawn. This describes the flexibility of the system to provide the owner the type of service that they require as they demanded in the first place. The change in the services and resources utilized for owner according to their demands almost instantly. This aspect still makes the cloud computing services all the more desirable to customers.

D. Data Confidentiality

This aspect only allows the authorized user to access the data since it has been encrypted to keep the data hidden from access made by the unauthorized user. The encryption of data ensures the safety of stored data from any unauthorized actions. This is one of the strict rules that the cloud service must follow themselves too.

E. Collusion Resistant

The resistance towards an attack that is executed by having multiple attributes to combine and form a key that can decrypt a ciphertext associated with the targeted user. This is an attack which can be carried out by a group of unauthorized users or a malicious attacker in possession of multiple attributes that were acquired through hacking a user or by their assistance.

F. Fine Grained Access Control

This also considered one of the defining aspects of the cloud computing services. The ability to maintain the access rights to the data , assigning a new access control for a new user and basically having complete control of the data's revelation and also to whom it may be shown.

III. LITERATURE SURVEY

The Literature survey contains all the information regarding the Encryption schemes such as ABE it's different types. It will also include all the different CP- ABE schemes that were reviewed. This will contain all the crucial information on the schemes their advantages and disadvantages based on the above shown aspects.

A. ABE (Attribute Based Encryption Schemes)

[8]The primary goal while constructing this scheme was to provide better security and access control. Since naturally cloud computing in its naked form is completely unsafe to establish a service. The entities within the system are Sender(Data Owner), Receiver(Data user) and authority generates key for data both the entity to use for the encryption and decryption.

An access policy will be created according to the data which will act as the condition required to decrypt it. The implementation of Receiver's attribute within the encryption allows only the authorized user with that specified attributes to the decrypt the ciphertext.

Disadvantages:-

- Lack of a practical attribute access to be applied in real situations.
- It is heavily dependent upon key generation.
- It is very taxing while dealing with large number of authorized users since requirement for encryption are their public keys.

B. KP-ABE (Key Policy Attribute Based Encryption Scheme)

[9]This scheme is a type of ABE ,All the ciphertexts are

created with access policy instead of user's attributes. It is completely reverse form the another type of ABE, In this scheme decryption is performed through user's attributes. An access structure is assigned to every private keys which only allows specific ciphertext to be decrypted by a particular key.

The process starts from generation of public parameters PK and master key MK , then selection of a random value from set of attributes provides us with our ciphertext hence completion of encryption. A key is generated which authorize encryption only and only if the attribute of the user matches the access policy.

Disadvantages:-

- This scheme very loosely allows the exertion of control over ciphertext decryption. Since the data owner must stay reliant on the work of key allocator.
- The tree structure does not allow the multiple parties to perform co-operatively.

C. CP-ABE (Ciphertext Policy Attribute Based Encryption Schemes)

[6]This is another modified version of ABE, this includes the creation of an access policy with user's attributes for encryption and only allows a user decrypt if their attributes satisfies the condition of the access policy. It is exact opposite of KP-ABE in terms of selection of parameters for encryption and decryption. It starts with generation of public parameters PK and master key MK from the setup algorithm. A ciphertext CT is produced employing an access policy to encrypt the message taking the public parameters PK as an input. Key generation takes the MK master key and a set of attributes S that describes the key and provide with the secret key SK.

Disadvantages:-

- It has low resistance to collusion attacks.
- The scheme is very rigid and does not perform well with exceptions or customization.

The types of CP-ABEs while building this reports are:

a. MA-CP-ABE (Multi Authority Ciphertext Attribute Based Encryption Scheme)

[1]This scheme deals with the implementation of CP-ABE on large vehicular data. It is intended towards a completely practical oriented environment based on combining the Multi Authority factor to the original CP-ABE. They have claimed that there are some gaps in access control with the previous schemes used in vehicular cloud computing.

They have proposed a solution by implementing the improved access control integrated through multi authority and also with VANETs.

b. HP-CP-ABE (Hidden Policy Ciphertext Attribute Based Encryption Scheme)

[2]This scheme was proposed to specifically target the issues while handling big data within the cloud computing services. It's implementation probably about transmitting and receiving the big data produced by an Artificial Intelligence or possibly any of deep learning applications.

It utilizes concept of hidden policy combined with the CP-ABE to overcome the issues that they have claimed to have found is about data leakage and causing more computational costs. They have proposed a complete hidden policy which functions exactly identical to it's name by implementing a mask technique on each and every attributes to hide them.

c. *CP-ABHE* (*Ciphertext-Policy Attribute-Based Hierarchical document collection Encryption scheme*)

[7]This scheme was introduced with hierarchical concept which has it's downsides and yet it was successful in implementing enhancements. This scheme was claimed to be fulfilling in all manners and sufficient enough to meet all current enterprises' requirements.

It's concept is associated with hierarchical tree based access structure which is incorporated within the ciphertext. The issues that they have claimed to have encountered were low efficiency especially dealing with large files. They have claimed that this proposal scheme have decreased the size of ciphertext with it's security intact with efficiency drastically increased.

d. MCC with CPABE (Mobile Cloud Computing with CP-ABE)

[12]The scheme was invented while developing a new access structure along side which is called Secure and Lightweight fine grained data sharing scheme (SLFG-DSS)for a cloud computing environment.

It has a concept which involves generation of a secret key that transforms while returning from the server. It is has been claimed that ABE schemes on it's own are not appropriate for MCC since the are expensive including their employed strategy.

They proposed that outsourcing the heavy data which was computed using the limited mobile resources to be stored in a remote server. Now the security and privacy untouched because of the transforming key, this also resulted in minimizing the risk of key exposure.

e. KEP-CP-ABE (Key Exchanging Policy with CP-ABE)

[3]This scheme focuses on the sole purpose of making the fog computing more secure with the help of ABE schemes.
This consist of the concept of applying the CP-ABE to establish an efficient key exchange protocol. Since fog is a version of cloud computing that works as smart grid structure supporting even the IOTs which makes it essential for daily life.

Since the information that are being transmitted continuously must have a better security. They have claimed to have applied this scheme and produced positive results where they made these data transactions more secure without causing any efficiency decay.

D. MABE (Multi- Authority Attribute Based Encryption Schemes)

[13]There are numerous attribute authorities are present within this scheme for generation and handling of the secret key. The decryption requires the user to possess set
of each and every authority present within the system. The similar way of input of security parameters and generation of the public key PK and Master Key MK as an output. This lead to running of an algorithm the provide is the secret key by computing owner's secret key, authority value d_k , user's GID , set of attributes in authority domain A_c^k . Then central key is generated using user's GID and Master Secret Key. An algorithm run for encryption which takes set of attributes from each and every authority, hence result in ciphertext. Another algorithm run for decryption in a complete opposite manner.

Disadvantage:-

The one and only demerits appears in the base MABE is that each authority's set of attributes must be disjoint.

E. HABE (Hierarchical Attribute Based Encryption Scheme)

[11]It is derived from the HIBE and contains very similar properties. It includes hierarchy of domain authorities and various attributes are provided to the user. All the Secret Key SK assigned to the users will be a leaf of the SK of root domain authority. The attribute is excluded from abiding by this hierarchy rule. This overall structure does follow the hierarchical format where the leaf domain authority does not have clearance to decrypt the ciphertext related to its root and entities above them.

The process involves the public key PK and master key MK and selection of cryptographic hash functions H1 & H2. Then the key generation is where the level of authority is established and could produce the secret key for future sessions. The user's attributes are implemented within the secret keys of that respective users. A random algorithm employed the access structure within the ciphertext C and the decryption requires the user's key to satisfy the access structure τ.

Disadvantages:-

- The main parent authority is capable of decrypting all ciphertext. It is one of the major concerns because if it get compromised entire scheme will be compromised.
- The implementation of this scheme is difficult given it's complex structure which also results in high computational overhead.

IV. COMPARISON

The comparison is done between the original ABEs and its types using the aspects of an ideal encryption schemes and performance. Here the Table 1. [6][8]-[10] shows the schemes capability to support the qualifying features.

Criteria	ABE	KP-ABE	CP-ABE	MABE	HABE
User Accountability	No	Yes	Yes	Yes	No
User Revocation	No	Yes	Yes	Yes	Yes
Scalability	No	No	No	Yes	No
Data confidentiality	Yes	Yes	Yes	Yes	Yes
Fine grained Access control	No	Yes	Yes	Yes	Yes
Collusion Resistance	Yes	Yes	Yes	Yes	Yes
Computational Overhead	Hih	High	Avg	Higher	Higher
Secured access control	Low	Low	Avg	Avg	High
efficiency	Avg	Avg	Avg	Flexible	Better

Table 1: The comparison based on the ideal aspects and performance

Table 2. shows overview of various CP-ABE's Algorithm

Scheme	Setup	Encryption	Key Generation	Decryption
MA-CP-ABE [1]	(1^k) (PK,MK)	(M,P,AS) (CT)	(S,AA) (SK)	(TK,GSK) (M)
HP-CP-ABE [2]	(1^π) (PK,MK)	(PK,M, AS) (CT)	(PK,MK, S) (SK)	(CT,SK) (M)
CP-ABHE [7]	(G_0,g,e,α, β) (PK, MSK)	(PK,cK, S_T) (CT)	(MSK,S) (SK)	(CT_T,SK) (M)
MCC-CP-ABE [12]	(K,u) (params, MSK)	(params, MSK) (CT)	(params,S K_s,T_k)(CT, TK,param) (CT')	(params,CT') (M)
KEP with CP-ABE [3]	(K) (MKS,PK)	(PK,AS) (CT)	(MK,PK, S) (SK)	(SK,PK,CT) (M)

CONCLUSION

The selection of the CP-ABE for further research and development of an original scheme for specified purpose or service is justified according to Table1. It does has its shortcomings such as the poorly present collusion resistance and absence of scalability but it still produce consistent performance. This is also further proved by the Table 2. that these factors calls for the requirement to enhance it's core features as well as overcoming other weaknesses. If such enhancement are successful then it will be a balanced base to be adopted and customized to build any type of cloud computing service.

REFERENCES

[1] *Wei Luo and Wenping Ma*, "Efficient and Secure Access Control Scheme in the Standard Model for Vehicular Cloud Computing" *IEEE-40420 Volume 6* ,2018.

[2] *Sucharita Khuntia and P. Syam Kumar*," New Hidden Policy CP-ABE for Big Data Access Control with Privacy-preserving Policy in Cloud Computing", *IEEE- 43488 9th ICCCNT* 2018.

[3] *Arwa Alrawais,Abdul Rahman Althohaily Chunqiang Hu,Xiaoshuag Xing And Xiuzhen Cheng*,"An Attribute-Based Encryption Scheme to Secure Fog Communications",IEEE- 9138 ,Volume -5,May 2017

[4] *Pan Jun sun* "Privacy Protection and Data Security in Cloud Computing:Survey, Challenges, and Solutions " volume 7 2019 IEEE 147449.

[5] *Mehdi Sokhaka, F.Richard Yua, Muhammad Khurram Khanb , Yang Xiang c, Rajkumar Buyya d,*" Attribute-based data access control in mobile cloud computing:Taxonomy and open issues", (2017) 273-287.

[6] *J. Bethencourt, A. Sahai, and B.Waters,*``Ciphertext-policy attribute- basedencryption," in *Proc. IEEE Symp. Secur . Privacy (SP),* Berkeley, CA, USA,May 2007, pp. 321_334.

[7] J. Fu and N. Wang, ''A practical attribute-based document collection hierarchical encryption n scheme in cloud computing,' IEEE Access, vol. 7, pp. 36218–36232, 2019.

[8] Vinothkumar, A., Anand, M., & Ravi, S. (2006). ATTRIBUTE BASED ENCRYPTION (ABE) ALGORITHM FOR SEARCHING AND SECURING ENCRYPTED DATA.

[9] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM Conference on Computer and Communications Security - CCS '06.

[10] Chase, M., & Chow, S. S. (2009, November). Improving privacy and security in multi-authority attribute-based encryption. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 121-130).

[11] Asim, M., Ignatenko, T., & Petkovic, M. (2019). *U.S. Patent No. 10,211,984*. Washington, DC: U.S. Patent and Trademark Office.

[12] Li, H., Lan, C., Fu, X., Wang, C., Li, F., & Guo, H. (2020). A Secure and Lightweight Fine-Grained Data Sharing Scheme for Mobile Cloud Computing. *Sensors*, *20*(17), 4720.

[13] Chase, M. (2007, February). Multi-authority attribute based encryption. In Theory of cryptography conference (pp. 515-534). Springer, Berlin, Heidelberg.