ISSN: 0976-3104
SPECIAL ISSUE: (Emerging Technologies in Networking and Security (ETNS)
Divya et al

THE IIOAB JOURNAL

ARTICLE OPEN ACCESS

A REVIEW ON ATTRIBUTE BASED ACCESS CONTROL SCHEME IN CLOUD ENVIRONMENT

S. Divya*, B.Ananthi, V. Shanmugavalli
Dept of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Namakkal, T.N, INDIA

ABSTRACT

***Aim**: Data security is main concern in cloud computing for protecting the confidentiality of the stored data. Nowadays Computer Science technologies have pulled more and more people to store and share their sensitive data on third party servers. To share the personal data on third party servers, it is essential to obtain an efficient encryption system. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic algorithm, where the encryptor can decide the access structure that will be used to protect the sensitive data. Here the survey is made in order to re-examine the attribute-based data sharing proposals. In future an improved Decisional Bilinear Diffie Hellman key exchange protocol has been proposed in CP-ABE scheme. It can guarantee that either key authority or cloud service provider can compromise the entire secret key of a user separately. It also enables dynamic modification of access policies and supports efficient on-demand user/attribute revocation. **Conclusion:** To overcome the drawbacks of ABE scheme in future the attributes can be constructed with weight which also reduces the complexity of access policy, so that the storage cost of cipher text and time cost in encryption can be saved.*

Published on: 2nd -December-2016

KEY WORDS

Cloud Security, Secure data sharing, ABE, KP-ABE, CP-ABE, HABE, and Removing Escrow.

***Corresponding author: Email:** divyasnkl@gmail.com; **Tel.:** +91 9486029378

INTRODUCTION

Cloud computing is a promising a computing paradigm which recently has drawn from both the academic and industry. By combining a set of a different techniques from research areas such as Service Oriented Architecture (SOA) and virtualization, cloud computing has become a widely adopted paradigm for delivering services over the internet. Cloud computing provides services according to three primary service models: Infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). The five characteristics of cloud computing are: on demand service, self service, location independent, rapid elasticity and measured scale service

Data Security

With the rapid growth of sensitive information on cloud, security is getting more important than even before. Most of the organization and institute utilized of this characteristics of the cloud computing and take benefit to gain profit. Hence, industries are shifting their businesses towards cloud computing. Cloud computing uses increased day by day, however, Data security is main concern in cloud computing. For protecting the confidentiality of the stored data, the data must be encrypted before uploading to the cloud by using some cryptographic algorithms. A data owner [13] [15] (DO) is usually willing to store large amounts of data in cloud for saving the cost on local data management. Without any data protection mechanism, cloud service provider (CSP), however, can fully gain access to all data of the user. This brings a potential security risk to the user, since CSP may compromise the data for commercial benefits.

Accordingly, how to securely and efficiently share user data is one of the toughest challenges in the scenario of cloud computing [15],[12],[1].

Attribute based Encryption

Public-Key encryption is a powerful mechanism for protecting the confidentiality of stored and transmitted information. Traditionally, encryption is viewed as a method for a user to share data to a targeted user or device. In 2008, Sahai and Waters [11] introduced fuzzy identity based encryption (IBE), which is the seminal work of attribute based encryption (ABE). Recently, much consideration has been attracted by a new public key primitive called Attribute-Based Encryption (ABE) [4]. ABE has significant advantage over the traditional PKC primitives as

it achieves flexible many-to-many encryption instead of many-to-one. ABE is envisioned as an important tool for addressing the problem of secure and fine-grained data sharing and access control.

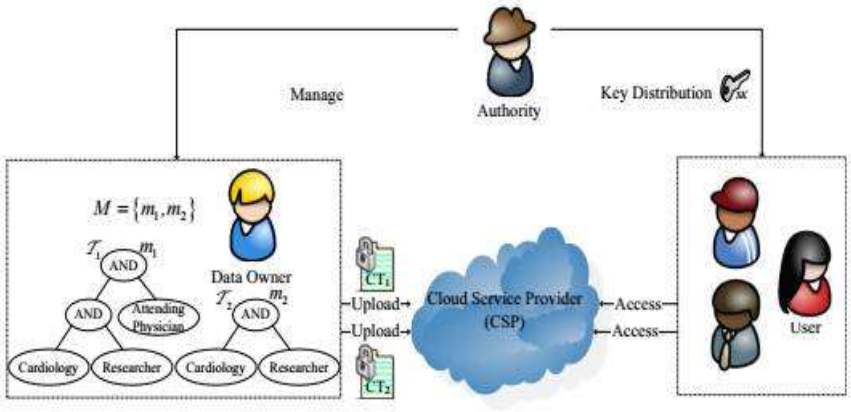

Fig: 1. An example of secure data sharing in cloud computing

In an ABE system, a user is identified by a set of attributes. For example, one can encrypt a recruitment related document to all recruitment committee members in the Computer Science Department. In this case the document would be encrypted to the attribute subset {''Faculty'', ''CS Dept.'', ''Recruitment Committee''}, and only users with all of these three attributes in the University can hold the corresponding private keys and thus decrypt the document, while others cannot. There are two variants of ABE: Key-Policy based ABE (KP-ABE) [12] and Ciphertext-Policy based ABE (CP-ABE) [13].

In KP-ABE, the ciphertext is associated with a set of attributes and the secret key is associated with the access policy. The encryptor defines the set of descriptive attributes necessary to decrypt the ciphertext. The trusted authority, who generates user's secret key, defines the combination of attributes for which the secret key can be used. In CP-ABE, the idea is reversed: now the ciphertext is associated with the access policy and the encrypting party determines the policy under which the data can be decrypted, while the secret key is associated with a set of attributes. DO (Data Owner) is allowed to define access structure over the universe of attributes. A user can decrypt a given ciphertext only if his/her attribute set matches the access structure over the ciphertext. A CP-ABE system can used into a cloud application may cause some open problems. Firstly, all users' secret keys need to be issued by a fully trusted key authority (KA). This brings a security risk that is known as key escrow problem. By knowing the secret key of a system user, the KA can decrypt the entire user's ciphertexts, which stands in total against to the will of the user. Secondly, the expressiveness of attribute set is another concern. As far as we know, most of the existing CP-ABE schemes [1], [4], [19], [12], [15].

LITERATURE SURVEY

Since all the data is transferred using Internet, data security is of major concern in the cloud. They shift their data from server to service based technology brought a significant change in computing technology. However these developments have created new security vulnerability. There are several security mechanisms are available. Sahai and Waters [12] proposed fuzzy Identity-Based Encryption (IBE) in 2008, which was the prototype of ABE. Latterly, a variant of ABE named KP-ABE,CP-ABE [11], [12], [16], was proposed. The following literature reviews attempts to demonstrate the different ABE schemes to provide a data security.

In [1] authors K. Liang, J. K. Liu, D. S. Wong, and W. Susilo in this paper "Cipher text policy Attribute based Encryption with anonymous access policy" described a scheme for constructing a Ciphertext Policy Attribute based Encryption with hidden access policy and provide security under the Decisional Diffie-Hellman assumption. In this scheme access policy can be expressed using AND, OR Boolean operators, so that it is possible to express the access policy effectively. The access policy can be represented in an n-ary tree, the leaf nodes represents the attribute present in the access policy, interior nodes represents the AND, OR operators. Each attribute in the leaf node can take multiple values. The value assigned for the leaf node by the secret sharing method will be distributed to these multiple values. The disadvantage of this scheme is key escrow problem.

In [2] authors S. Roy, M. Chuah in this paper "Secure Data Retrieval Based on Ciphertext Policy Attribute-Based Encryption (CP-ABE) System for the DTNs" proposed an access control scheme which is based on the Ciphertext Policy Attributed-Based Encryption (CP-ABE) approach. That provides a flexible fine-grained access control such that the encrypted contents can only be accessed by authorized users. The advantage of this scheme is that the incorporation of dynamic attributes value may change over time, and can be revocated its feature. This methodology makes use of groups with efficiently computable bilinear maps, and it is the key to our security proof, which gives a generic bilinear group model. The demerits of using this scheme are high computational overhead.

In [3] authors Tsz Hon Yuen, Joseph K. Liu_, Man Ho Au, Xinyi Huang, Willy Susilo, and Jianying Zhou in this paper "k-times Attribute-Based Anonymous Access Control for Cloud computing" explained a new notion called k-times attribute-based anonymous access control. This provides a k-times limit for anonymous access control. That is, the server may limit a particular set of users to access the system for maximum k-times within a period or an event. Further the additional access will be denied. It provides an option for service provider to make it linkable or unlinkable. Yet even if it is unlinkable, the service provider knows whether the user has exceeded the k-times access limit. The security of this system is instantiated by using q- Decisional Bilinear Diffie-Hellman Inversion (DBDHI).The disadvantages of the paper is the user revocation is not possible. The advantage of this paper is limit access control.

In [4] authors Chun-I Fan, Vincent Shi-Ming Huang, and He-Ming Ruan in this paper "Arbitrary-State Attribute-Based Encryption with Dynamic Membership" proposed an ABE scheme that aims at dynamic membership management with arbitrary states, not only the binary states for every attribute. That also keeps high flexibility of the constraints on attributes and makes users to dynamically join, leave, and update their attributes. It is not necessary for those users who do not change their attribute statuses to renew their private keys when some user updates the values of her/his attributes. It consists of six algorithms which are Setup, Enrollment, Leaving, Updating, Encryption, and Decryption. The disadvantage of this scheme is it takes more time to process a retrieval of documents.

In [5] authors Fuchun Guo, Yi Mu, Willy Susilo, Duncan S. Wong, and Vijay Varadharajan in this paper "CP-ABE With Constant-Size Keys for Lightweight Devices" proposed a novel CP-ABE scheme with constant-size decryption keys independent of the number of attributes. Normally CP-ABE schemes suffer from the issue of having long decryption keys, in which the size is linear to and dependent on the number of attributes. This drawback was prevented by the use of lightweight devices in practice as storage of the decryption keys of the CP-ABE for users. The size of the device is 672 bits. The authority generates decryption keys of users and stores them in an RFID tag, which is embedded within a user's ID card.

Since the key size is constant and small, the user can extract the key from his/her ID card for a security purpose. The advantages of this CP-ABE scheme allow all applications with key storage in lightweight devices. The main disadvantage of this scheme is when the key size is exceeded more than 672 bits, the cost of the device will get increased.

In [6] authors A. Balu, K. Kuppusamy in this paper "An expressive and provably secure Ciphertext-Policy Attribute-Based Encryption" proposed a new type of Ciphertext-Policy Attribute-Based Encryption based on linear integer secret sharing scheme. That scheme is very expressive and provably secure under the Decisional Bilinear Diffie–Hellman assumption. So the encryptor can specify the access policy in terms of LISS matrix M, over the attributes in the system. LISS focus on the advantages of secret sharing over integers opposed to secret sharing over finite groups or fields in LSSS. In LISS, the cost of the secret sharing is less.

In [7] authors Aparna C Bhadran, and Maria Joy in this paper "Enhanced Large Universe Ciphertext Policy Attribute Based Encryption" proposed the traceability and blocking properties to the large universe based on CP-ABE scheme. Traceability property traces the malicious user who tries to access the encrypted data without proper decryption key and pin code. Blocking property blocks the illegal user who has been traced as a malicious user. Large universe property supports a flexible number of attributes to the system. The decryption key and pin code which are needed to decrypt the data are sent to the receiver via email. When the receiver gives the invalid pin code that receiver will be blocked temporarily. Admin can activate the blocked user if wanted for one time. But if the user again gives invalid pin code the corresponding user is permanently blocked. MiM attack is possible in this scheme. This is the main disadvantage of this scheme.

In [8] authors Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen, and Weixin Xie in this paper "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud computing" proposed an efficient file hierarchy attribute-based encryption scheme. The shared data files generally have the characteristic of multilevel hierarchy, particularly in the area of healthcare and the military. The layered access structures are integrated into a single access structure, and then the hierarchical files are encrypted with the integrated access structure. The ciphertext components related to attributes could be shared by the files. Therefore, both ciphertext storage and time cost of encryption are saved. The demerits of this scheme is when more files are stored in hierarchal way there occurs a high computational overhead.

In [9] authors Zhihua Xia , Liangao Zhang , and Dandan Liu in this paper "Attribute-Based Access Control Scheme with Efficient Revocation in Cloud Computing" introduced the access controller and designs an escrow-free key generation protocol between the attribute authority and the access controller to generate user's secret keys in order to remove the key escrow problem. An efficient attribute revocation mechanism is presented using the version key. They adapt Hur's secure key generation protocol to construct our escrow-free key generation protocol. This scheme consists of five phases: system initialization, key generation, data encryption, data access, and attribute revocation. The advantage of this scheme is the security has been proven by the random oracle model and the user revocation mechanisms.

In [10] authors Chaudhari Swapnil and Mandre in this paper "Secure Data Retrieval based on Attribute-based Encryption in Cloud" described the Hierarchical attribute base encryption scheme implementation on cloudsim tool. In this the Rijndael algorithm are used to encrypt the data. To perform encryption the string value of attribute and data file are converted into a bytes. Rijndael algorithm performs encryption on byte arrays. The issue addressed by Hierarchical CP-ABE scheme is time require for encryption and decryption overhead and reduce the generation of complex key. The advantages of this proposed work provides easy and simple to and understandable key structure. The disadvantage of this scheme is, it takes more time to convert a string value to bytes for large files.

COMPARATIVE ANALYSIS OF DIFFERENT ABE SCHEMES

This section presents the comparison of different Attribute Based Encryption schemes such as HABE, FP-ABE and CP-ABE. This also gives the advantage and disadvantage of different techniques based on the algorithm.

Table: I. Comparison of different ABE schemes

Papers	Techniques	Algorithm	Advantage	Disadvantage
[1]	CP-ABE	Decisional Diffie Hellman(DDH)	Access policy can be expressed using AND, OR Boolean operators	Key escrow problem
[2]	CP-ABE	Decisional Diffie Hellman(DDH)	The incorporation of dynamic attributes whose value may change over time, and the revocation feature.	High Computational overhead
[3]	CP-ABE	Decisional Bilinear Diffie-Hellman Inversion (DBDHI)	It provides a k-times limit for anonymous access control	User revocation is not possible
[4]	CP-ABE	Decisional Bilinear Diffie-Hellman (DBDH)	It makes users are able to dynamically join, leave, and update their attributes	Occurs a collision
[5]	CP-ABE	Decisional Diffie Hellman(DDH)	It allows all applications with key storage in lightweight devices.	It takes a more cost

THE IIOAB JOURNAL
ISSN: 0976-3104

[6]	CP-ABE	Decisional Bilinear Diffie-Hellman (DBDH)	Secret sharing over integers opposed to secret sharing over finite groups	High computational overhead
[7]	CP-ABE	Not Mentioned	Traceability and Blocking property	Man in the middle attack is possible
[8]	FH-ABE	Decisional Bilinear Diffie-Hellman (DBDH)	Ciphertext storage and time cost of encryption are saved.	Average Computational overhead
[9]	CP-ABE	Hur's secure key generation protocol	Efficient revocation mechanism are presented	Key escrow problem
[10]	HABE	Rijndael algorithm	Which provides easy and simple to and understandable key structure	It's getting more time to convert a string value to bytes for large files

From the above survived we got some information on the performance achieved by the different ABE schemes.**[Figure- 2]** shows the storage cost of ciphertext with fixed attribute N=50. **[Figure- 3]** displays measurements of key generation time, encryption time, and decryption time on a range of different attribute size.

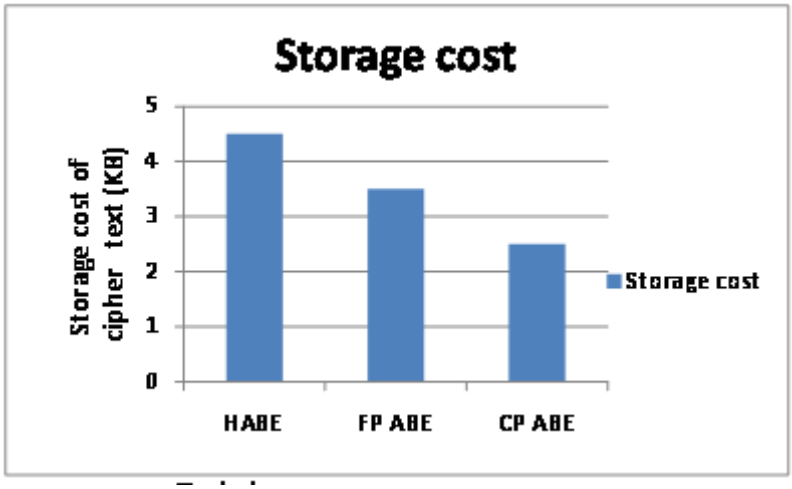

Fig: 2. The storage cost ciphertext to different techniques

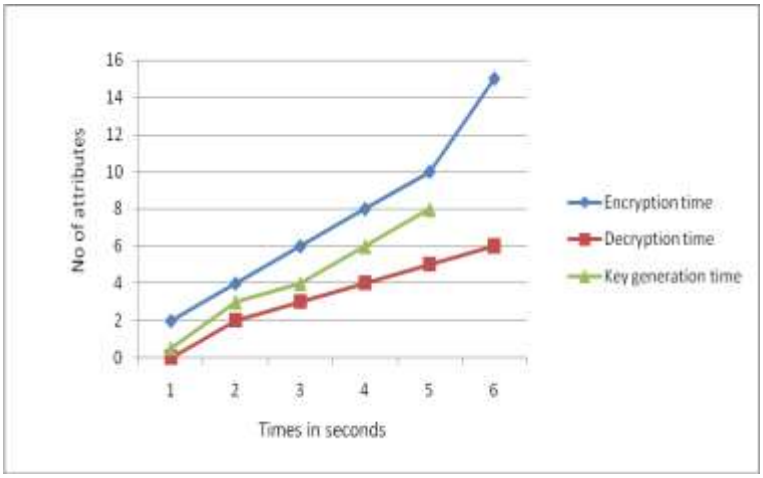

Fig: 3. The Encryption, Decryption, and Key generation time for existing CP-ABE method

POSSIBLE SOLUTION

Several security issues such as scalability in key management, flexible access and efficient user revocation that has been the most important challenges toward achieving fine-grained data access control. From the above comparison the storage cost of CP-ABE is 60%. And the encryption, decryption and key generation time is 70%. So for improving the efficiency of the above CP-ABE scheme we propose a ciphertext-policy weighted ABE scheme with removing escrow (CP-WABE) by using improved Decisional Bilinear Diffie Hellman key exchange protocol. By using this protocol the storage cost of ciphertext and time cost in encryption can be saved. It also enables dynamic modification of access policies and supports efficient on-demand user/attribute revocation.

CONCLUSION

Hence the survey is made up on a various attribute based access control schemes such as ABE, CP-ABE, HABE and KPABE. Where the ABE scheme provides more security but does not provide more resistance and key escrow problem. To overcome the drawbacks of ABE scheme in future the attributes can be constructed with weight which also reduces the complexity of access policy, so that the storage cost of cipher text and time cost in encryption can be saved. In order to improve the efficiency of encryption we can use an improved Decisional Bilinear Key Exchange protocol. It also enables dynamic modification of access policies and supports efficient on-demand user/attribute revocation.

CONFLICT OF INTEREST

The authors declare no conflict of interests.

ACKNOWLEDGEMENT

None

FINANCIAL DISCLOSURE

None

REFERENCES

[1] A Balu, K.Kuppusamy.[2010] Ciphertext policy Attribute based Encryption with anonymous access policy, International Journal of peer-to-peer networks (IJP2P) 1(1)October.

[2] S Roy, M Chuah. “Secure Data Retrieval Based on Ciphertext Policy Attribute-Based Encryption (CP-ABE) System for the DTNs” Lehigh University Bethlehem, PA, USA – 18015.

[3] Tsz Hon Yuen, Joseph K. Liu_, Man Ho Au, Xinyi Huang, Willy Susilo, Jianying Zhou. "k-times Attribute-Based Anonymous Access Control for Cloud Computing" IEEE Transactions on Computers.

[4] Chun-I Fan, , Vincent Shi-Ming Huang, and He-Ming Ruan.[2014] Arbitrary-State Attribute-Based Encryption with Dynamic Membership" IEEE Transactions on computers, 63(8).

[5] Fuchun Guo, Yi Mu, Willy Susilo, Duncan S. Wong, and Vijay Varadharajan," CP-ABE With Constant-Size Keys for Lightweight Devices" IEEE Transactions on information forensics and security, 9(5)May 2014.

[6] A. Balu , K. Kuppusamy. [2014]"An expressive and provably secure Ciphertext-Policy Attribute-Based Encryption" Information Sciences 276:354–362.

[7] Aparna C Bhadran, Maria Joy.[2016] Enhanced Large Universe Ciphertext Policy Attribute Based Encryption" International Journal of Advanced Research in Computer Science and Software Engineering, 6(1),ISSN: 2277 128X.

[8] Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen, Weixin Xie. [2015]An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing" IEEE Transactions on Information Forensics and Security 1556-6013

[9] Zhihua Xia, Liangao Zhang, Dandan Liu.[2016] Attribute-Based Access Control Scheme with Efficient Revocation in Cloud Computing China Communications

[10] Chaudhari Swapnil, [2016]Mandre Secure Data Retrieval based on Attribute-based Encryption in Cloud" International Journal of Computer Applications (0975 – 8887) 134 (13)

[11] A Sahai and B. Waters.[2009] Fuzzy identity-based encryption" Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 457–473.

[12] V Goyal, O Pandey, A Sahai, B Waters.[2008] Attribute-based encryption for fine-grained access control of encrypted data" Proceedings of the 13th ACM conference on Computer and communications security, pages 89–98.

[13] J Hur.[2013] Improving security and efficiency in attribute-based data sharing, IEEE *Transactions on Knowledge and Data Engineering*, 25(10): 2271-2282

[14] J. Bethencourt, A. Sahai, B. Waters, Ciphertext policy attribute based encryption" IEEE Symposium on Security and privacy, 2007, pp. 321–334.

[15] K. Liang, JK Liu, DS Wong, W Susilo. [2014]An efficient cloud based revocable identity-based proxy re-encryption scheme for public clouds data sharing. Proceedings of the 19th European Symposium on Research in Computer Security, pages 257–272.

[16] K Yang, X Jia, K Ren et al., "Dac-macs: Effective data access control for multi-authority cloud storage systems, pp. 2895-2903.