International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

An Efficient and Robust Embedded Digital Signature Based Data Sharing Scheme in Cloud Computing

Mr. Vandarani Tarun,
M. tech, P.G Student,
Department of CSE,
S.R.K.R College of Engineering,
Bhimavaram.

Dr. G.V. Padma Raju,
Professor,
Department of CSE,
S.R.K.R College of Engineering,
Bhimavaram.

Dr. G.N.V.G. SIRISHA,
Assistant Professor,
Department of CSE,
S.R.K.R College of Engineering,
Bhimavaram

Abstract

One of the most promising encryption techniques for secure data sharing in the field of Cloud Computing is Cipher text-Policy Attribute-Based Encryption (CP-ABE).This encryption technique has turned to be an important encryption technology to tackle the challenge of secure data sharing. In this encryption technique, data user's private keys and cipher texts are associated with a set of attributes. This technique completely encrypts the data and does not have any control over the individual attributes in the data. So, in order to overcome this problem a concept called attribute with weights was introduced, so that it can have control over the individual elements in the data and could be able to hide sensitive information while sharing data with the users. But the problem of malicious cloud insider still persists. Visualize in the context of an online health records system. Data user can access the health record by satisfying their arbitrary constraints defined by the data owner. Once they get access to the data, the system cannot prohibit or monitor their valid usage of the data. So an Embedded Digital Signature algorithm is proposed. This algorithm can embed the accessing data user's credentials in each health record they access which has a stealth effect of catching and prosecute them in case of an unauthorized data breach. Hence, the resulting scheme becomes more secure.

Keywords-- Cloud Computing, Data sharing, CP-ABE Attribute, Encryption, Embedded Digital Signature;

Introduction

The vast development in technology and internet now a day has made data portability very easy. We can nowadays share almost everything in online like pictures, movies, thoughts, etc.[1] [2]. If anybody need's an emergency help from a doctor or hospital for chronic diseases like cardio, neuron related previous data, are now able to do all these things easily with the help of internet or cloud technology. Because of the increase in the number of internet users, it has become a necessity to protect our data from being misused. An unauthorized user should not be able to access our private data.

Accordingly, how securely and efficiently share user data has become one of the toughest challenges in the scenario of cloud computing [3], [4]. For this reason we have to take care of data by implementing data protection techniques like CP-ABE [5][6]. So first I'm going to give a very quick general

idea of what cipher text-policy attribute-based encryption is. Roughly, it can be viewed as a generalization of identity-based encryption. So as in identity-based encryption, there is a single public key, and there is a master private key that can be used to make more limited private keys.

However, CP-ABE is much more flexible than plain identity-based encryption [7], it allows complex rules specifying which private keys can decrypt which cipher texts. Specifically, the private keys are associated with sets of attributes or labels, when we encrypt, encrypt data and access policy which specifies which keys will be able to decrypt. Along with the concept of CP –ABE , and include the concept of Embedded Digital Signature then there is a atmost possibilty to overcome the problem of misusage of the Data Owner's sensitive information to a very large extent.

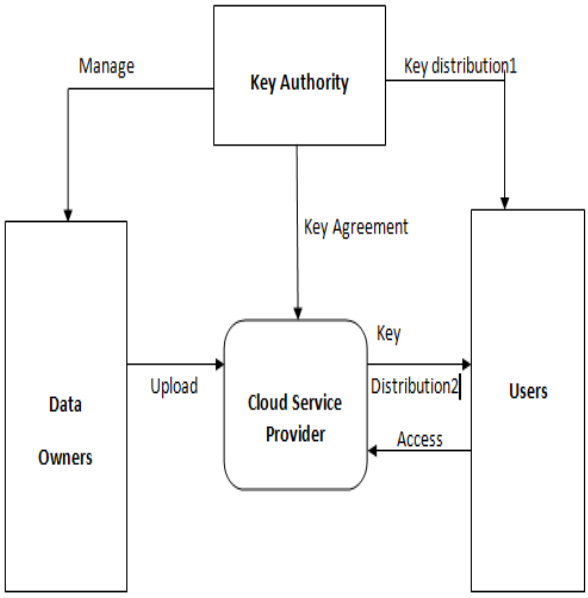

Fig1: System model of CP-WABE-RE scheme in cloud computing

1. Literature Survey

In 2016 Hangman Zhu and Rue Jiang proposed "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", In this paper, whenever Data Owner wants to share data with some end user, he performs some encryption technique and generates a secret key, and sends that secret key to the end user with whom he wants to share data. The end user has to enter the secret key manually. Data Owner grants the permission to End user for accessing his data by providing a secret key to him. But after some time even if Data Owner revokes the permission given to the End user, the secret key is still visible to the End User.

In 2014, Hiding et al introduced "Ciphertext-policy hieratical attribute-based encryption with short cipher texts" wherein the drawback of entering the secret key manually was resolved, but this encryption model completely encrypts the file and it does not have any control over the individual elements of the file. There may arise some situations where Data Owner may wants to show only some particular data and hide some sensitive information from the end user. But using this type of encryption method may not help the Data Owner to hide information from the end user.

In 2016 Shula Wang, Kauai Liang, Joseph K. Liu proposed, "Attribute Based Data Sharing Scheme Revisited in Cloud Computing" wherein we can have control over the attributes you want to share to the end

users by giving weights to the attributes and you can hide those particular attributes from the end user. But this process still has a limitation like the data which is shared by the Data Owner is in the text format and it can be easily manipulated. The owner may share the data over internet and end user can download the data and there may be a chance that the end user can change some important information related to the Data Owner, as the data is in a text format and there may be a chance that the end user can publish the same data again over the internet.

2. Our Contributions

In order to overcome all the limitations seen in the above mentioned base paper, An Embedded Digital Signature based Data sharing scheme in Cloud Computing is proposed. Now whenever the Data Owner shares information with the end user, the data is shared in the form of an image instead of text. As the data is in image format the end user will not be able to make any changes to the original data of the Data Owner. Moreover, it also have a Digital Signature embedded within the data and this Digital Signature varies from one user to another. So with the help of this Digital Signature embedded within the data, we can easily catch the person who has misused or manipulated the data.

The Digital Signature does not come along with the data but it comes within the data that is the reason why we call it embedded. Now days the mobile phones are coming with embedded batteries which means that the battery cannot be removed at any cost. In the same way here, whenever the Data Owner shares the data with the end user, that particular data has Page id embedded in it. Which is nothing but, the Digital signature which cannot be removed and it is coming along with the data. Hence, this technique assures the security and confidentiality to the Data Owner's data and protecting it from malicious user.

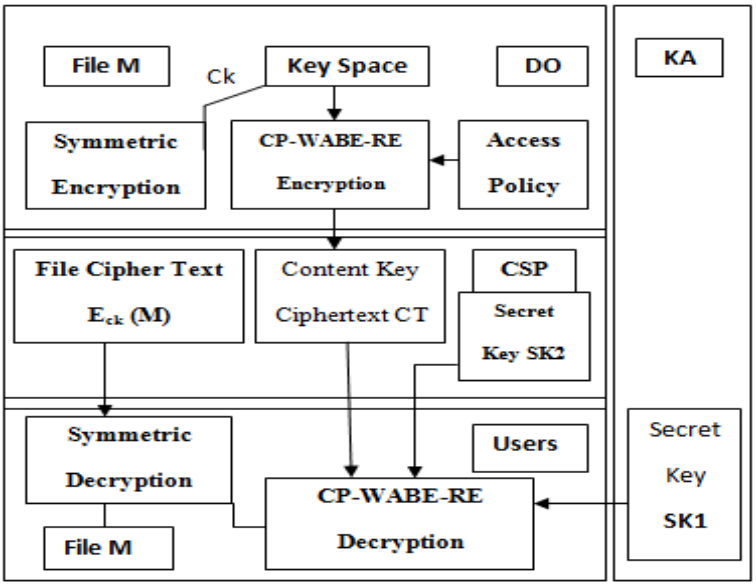

Fig2: System Framework of CP-WABE-RE scheme

In previous systems developed using CP-WABE-RE the cipher text components generated ensured security by overcoming the key escrow problem. The problem of malicious cloud insider still persists. Consider in the context of online medical health records system. An authorized user can access the health record satisfying the access structure defined by the data owner. Once they get access to the data the system cannot prohibit or monitor their valid usage of the data.

An Embeddable Digital Signature algorithm is proposed, that can embed the accessing users credentials in each health record they access which has a secret effect of catching and informing the Data Owner's in case of an unauthorized data breach. Fig 3 shows how a digital ID is embedded in a PDF Document. A digital signature [8] can be used with any kind of message whether it is encrypted or not. Simply the receiver can be sure of the sender's identity and that the message arrived intact. Digital signatures make it difficult for the signer to deny having signed something (non-repudiation) assuming their private key has not been compromised as the digital signature is unique to both the document and the digital signer. In many countries, including the United States, digital signatures have the same legal significance as the more traditional forms of signed documents.

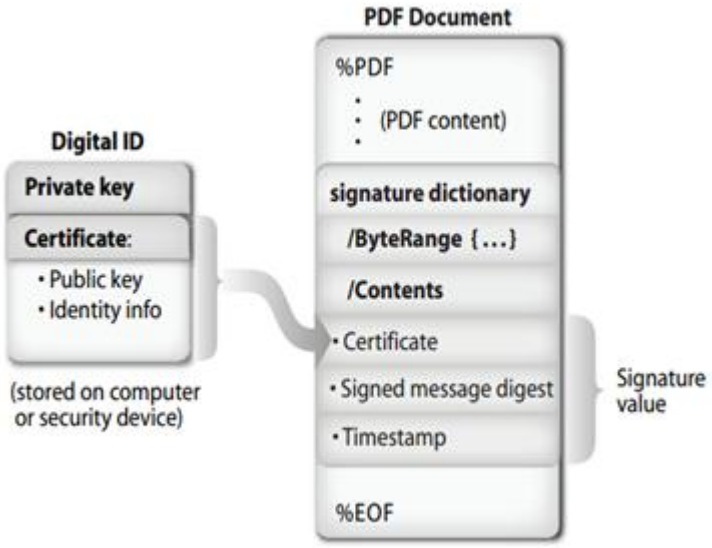

Fig3: Digital ID embedded in a PDF Document.

3. SYSTEM MODEL

As illustrated in Fig. 1 and Fig. 2, the system model and framework of CP-WABE-RE scheme in cloud computing are given, where the system consists of four types of entities: KA, CSP, DO and Users. In addition, we provide the detailed definition of CP-WABE-RE scheme.

Key Authority (KA):

It is a semi-trusted entity in cloud system. Namely, KA is honest-but-curious, which can honestly perform the assigned tasks and return correct results. However, it will collect as many sensitive contents as possible. In cloud system, the entity is responsible for the users' enrollment. Meanwhile, it not only generates most part of system parameter, but also creates most part of secret key for each user.

Cloud Service Provider (CSP):

It is the manager of cloud servers and also a semi-trusted entity which provides many services such as data storage, computation and transmission. To solve the key escrow problem, it generates both parts of system parameter and secret key for each user.

Data Owners (DO):

Data owners of files to be stored in cloud system. Data owners are in charge of defining access structure and executing data encryption operation. Data owners also upload the generated cipher text to CSP.

Users:

Users want to access ciphertext stored in cloud system. Users download the ciphertext and execute the corresponding decryption operation.

4. Algorithm

Representing the CP WABE RE with Embedded DS in four steps:

Step 1: System Initialization

In System Initialization step, Firstly set up KA and CSP which means they can create an understanding between KA and CSP that everything related to storage will be taken care by CSP and information related to keys will be taken care by KA. KA will also make sure to have the control over the individual elements of the data instead of having control over the entire data.

Step2: New File Creation

In this step the encryption modules plays major role. The file which the Data owner wants to share with the end user will be encrypted in this step.

Step 3: New User Authorization

In this step, the key is generated and the encrypted data will be shared among the users. If the user is authorised person then only he can access the data, an unauthorised user cannot access the data.

Step4: Embedded Digital Signature

In this step, a Digital Signature is embedded within the data. which the Data Owner wants to share with the end user. which means that Data owner is sharing the data with an embedded Digital Signature in it, so that it can be able to reduce the misuse of data to some extent and can ensure authentication, confidentiality, Data Integrity, Non repudiation.

5. Comparison

Parameters	Fine-grained access control	Efficiency	Computational Overhead
ABE	Low	Average	High
CP-ABE	Average Realization of complex Access Control	Average Not efficient for modern enterprise environments	Average Computational Overheads
CP-WABE	Best Access control, lighten the access policy	High efficient and security	Very less computation overhead than others

Table: Comparison of Various ABE Techniques Used In Cloud Computing

6. Results

number of weighted attributes	The storage cost of Secret key(KB)
2	5
3	10
5	15
7	20
9	25

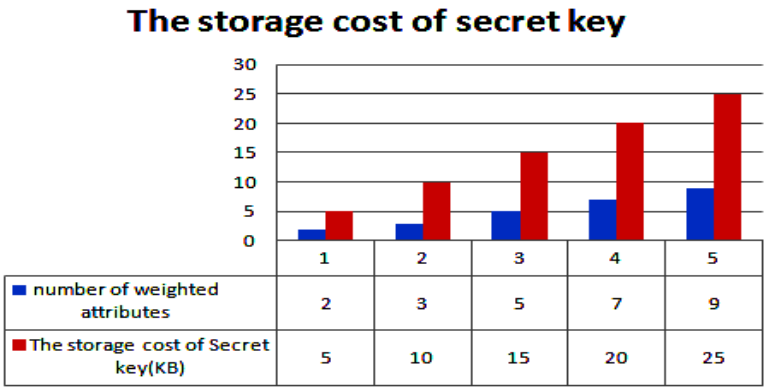

Fig: 1 the storage cost of secret key.

Analysis of Key Escrow:

The storage overhead and computation cost of user secret key are compared as plotted in Fig. 1. The number of weighted attributes used in this simulation is N = {5, 10, 15, 20, 25}. We find that the storage overhead of user secret key. We also observe that all experimental results are gradually increasing and approximately follow a linear relationship with the number of weighted attributes.

Number of weighted attributes	User key generation time(s)
5	0.5
10	0.8
15	1
20	1.4
25	1.7

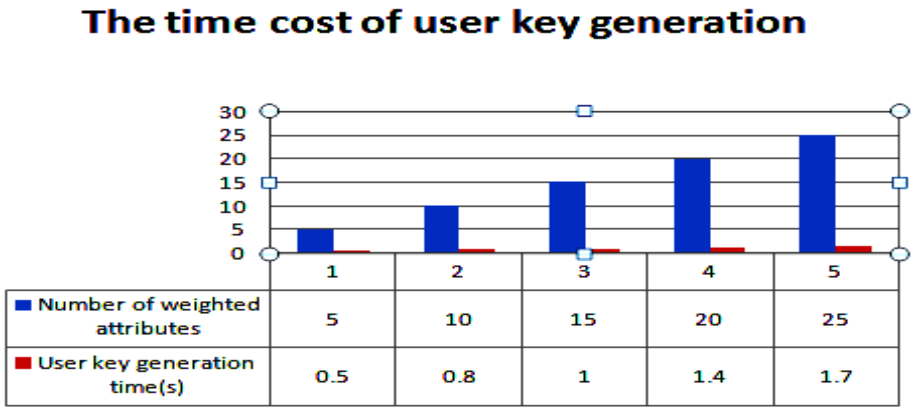

Fig: 2 the time cost of user key generation

Fig. 1 plots the relationship between the storage overhead of ciphertext and the number of weighted attributes in access policy. Fig. 2 shows encryption time of ciphertext versus the number of weighted attributes. When ωi _= $\omega i1$ (here we assume that an attribute can be represented 5 attributes which possess different weights), we find that CP-WABE-RE scheme requires less storage cost and encryption time than the others. We also observe that all results approximately follow a linear relationship with the number of weighted attributes in access tree.

7. Conclusion

In this paper, an Embedded Digital Signature based data sharing scheme along with the concept of Cipher text Policy Attribute Based Encryption Removing Escrow (CP-ABE-RE) is proposed with help of this Data Owner can share data with the end users securely and the shared data is in an image format with a Digital Signature embedded in it which makes it impossible for the end user to manipulate the data. Therefore, security is assured to the data owner's information.

8. References

[1] S.Lai, J.K. Liu, K.-K. R. Coho, and K. Liang, "Secret picture: An efficient tool for mitigating deletion delay on OSN," in Proc. 17th Int. Conf. Inf. Common. Secure., 2015, pp. 467–477.

[2] K. Liang, J. K. Liu, R. Lu, and D. S. Wong, "Privacy concerns for photo sharing in online social networks," IEEE Internet Comput., vol. 19, no. 2, pp. 58–63, Mar./Apr. 2015.

[3]C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. CSU, and J.Zhou, "Security concerns in popular cloud storage services," IEEE Pervasive Comput., vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.

[4] C. Wang, S. S. M. Chow, Q. Wang, K. Ran, and W.Lou,"Privacy preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[5] A. Bale and K. Kuppusamy, "An expressive and provably secure ciphertext-policy attribute-based encryption," Inf. Sci., vol. 276, no. 4, pp. 354–362, Aug. 2014.

[6]H.Dengetal., "Ciphertext-policy hierarchical attribute-based encryption with short cipher texts," Inf. Sci., vol. 275, no. 11, pp. 370–384, Aug. 2014.

[7] A. Sashay and B. Waters, "Fuzzy identity-based encryption," in Proc. 24th Annul. Int. Conf. Theory Appl. Cryptograph. Techno., 2005,pp.457–473

[8]searchsecurity.techtarget.com/definition/digital-signature