isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

Protection And Encryption Of Sensitive Data For Banking Using Abe

Seshang Anand[1],Srinivasan Velu[2] ,Ms.K.Deepika[3]

Student, Department of Computer Science and Engineering, Agni College of Technology, India[1, 2].

Assistant Professor, Department of Computer Science and Engineering, Agni College of Technology, India [3].

ABSTRACT

Cloud storage services have become increasingly popular. Because of the importance of privacy, many cloud storage encryption schemes have been proposed to protect data from those who do not have access. All such schemes assumed that cloud storage providers are safe and cannot be hacked; however, in practice, some authorities (i.e., coercers) may force cloud storage providers to reveal user secrets or confidential data on the cloud, thus altogether circumventing storage encryption schemes. In this paper, we present our design for a new cloud storage encryption scheme that enables cloud storage providers to create convincing fake user secrets to protect user privacy. Since coercers cannot tell if obtained secrets are true or not, the cloud storage providers ensure that user privacy is still securely protected.

Keywords—Deniable Encryption, Attribute-Based Encryption, Cloud Storage.

1 INTRODUCTION

Protection and encryption of sensitive data for banking using ABE is for computerizing the working in a Bank. The software takes care of all the methods of an average existing bank and is capable to provide easy and effective storage of information

related to customer that come up to the Bank along with the transaction details of a customer.

The created details will be processed and published as report through online where the details can be safe guarded without establishing the customer details. The customer can access their details anywhere when they needed, they can also make online transaction through this user interface application. Thereby protecting customer details from coercers.

2 EXISTING SYSTEM

The concept of ABE in which data owners can embed how they want to share data in terms of encryption. That is, only those who match the owner's conditions can successfully decrypt stored data. We note here that ABE is encryption for privileges, not for users. This makes ABE a very useful tool for cloud storage services since data sharing is an important feature for such services. Cloud storage users are impractical for data owners to encrypt their data by pair wise keys. Moreover, it is also impractical to encrypt data many times for many people. With ABE, data owners decide only which kind of users can access their encrypted data. Users who satisfy the conditions are able to decrypt the encrypted data. The concept of deniable encryption is nothing but it also like normal encryption schemes, deniable encryption can be divided into a deniable shared key scheme and a public key scheme. Considering the cloud storage scenario, we focus our efforts on the deniable public key encryption scheme. The public key system provides an oblivious key generation function and an oblivious cipher text function. When sending an encrypted bit, the sender will send a set of encrypted data which may be normally encrypted or oblivious.

3 PROPOSED SYSTEM

The implementation of a deniable CP-ABE scheme that can make cloud storage services secure and audit free. In this scenario, cloud storage service providers are just regarded as receivers in other deniable schemes. Unlike most previous deniable encryption schemes, we do not use translucent sets or simulatable public key systems to implement deniability. Deniable Cipher Text Policy Attribute Based Encryption scheme build with two encryption environments at the same time, much like the idea proposed in. our scheme with multiple dimensions while claiming there is only one dimension. This approach removes obvious redundant parts. An existing ABE scheme by replacing prime order groups with Composite order groups. Since the base ABE scheme can encrypt one block each time,

our deniable CPABE is certainly a block wise deniable encryption scheme. The bilinear operation for the Composite order group is slower than the prime order group, there are some techniques that can convert an encryption scheme from Composite order groups to prime order groups for better computational performance. Deniable Cipher Text Policy Attribute Based Encryption provides a consistent environment for our deniable encryption scheme. Consistent environment which means that one encryption environment can be used for multiple encryption times without system updates. The opened receiver proof should look convincing for all cipher texts under this environment3, regardless of whether a cipher text is normally encrypted or deniably encrypted. The deniability of our scheme comes from the secret of the subgroup assignment, which is determined only once in the system setup phase. By the canceling property and the proper subgroup assignment, we can construct the released fake key to decrypt normal cipher texts correctly Deniable Cipher Text Policy Attribute Based Encryption Extends a pairing ABE, which has a deterministic decryption algorithm, from the prime order group to the Composite order group. The decryption algorithm in our scheme is still deterministic; therefore, there is no decryption errors using our scheme.

4 SYSTEM IMPLEMENTATION

4.1 Bank Admin:

In this module bank admin operations are explained. Bank admin creates account for user, view all accounts, view all transaction history, and close accounts. Bank admin plays a major role in this project. Bank admin safeguards the sensitive data of the user by ensuring that the third party is given with the fake login and fake password. By this way the Bank admin protects the bank and the user data.

4.2 Fake account:

Fake account is created simultaneously by bank admin while creating account for user for sending information to the third party. This provides the login for the third party to access for fake environment ensuring that no user secrets are revealed when force bank admin to reveal user secrets or confidential data on the website.

4.3 User:

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

User module is where user operations like transferring money to other account withdraw amount from account and view account details are done with login credentials. User can also be referred to as customers who tend to open an account form which transactions can be carried out by the user. The user's sensitive data such as transactions and details are to be protected as the project.

4.4 Third party:

Third party is the one who force bank admin to reveal user secrets or confidential data on the website. Bank admin gives fake details to third party where they cannot do any transactions in those credentials. The user details are said to be in encrypted form on the fake environment provided by the admin to the third party. This encrypted format ensures that user details cannot be viewed by the third party.

4.5 Attribute Based Encryption:

Attribute Based Encryption, An encryption technique that by the third party login for a particular user as a fake login the user data is encrypted by Attribute Based Encryption. The user details are not visible by third party by this encryption method as a module for this project.

5 ARCHITECTURE DIAGRAM

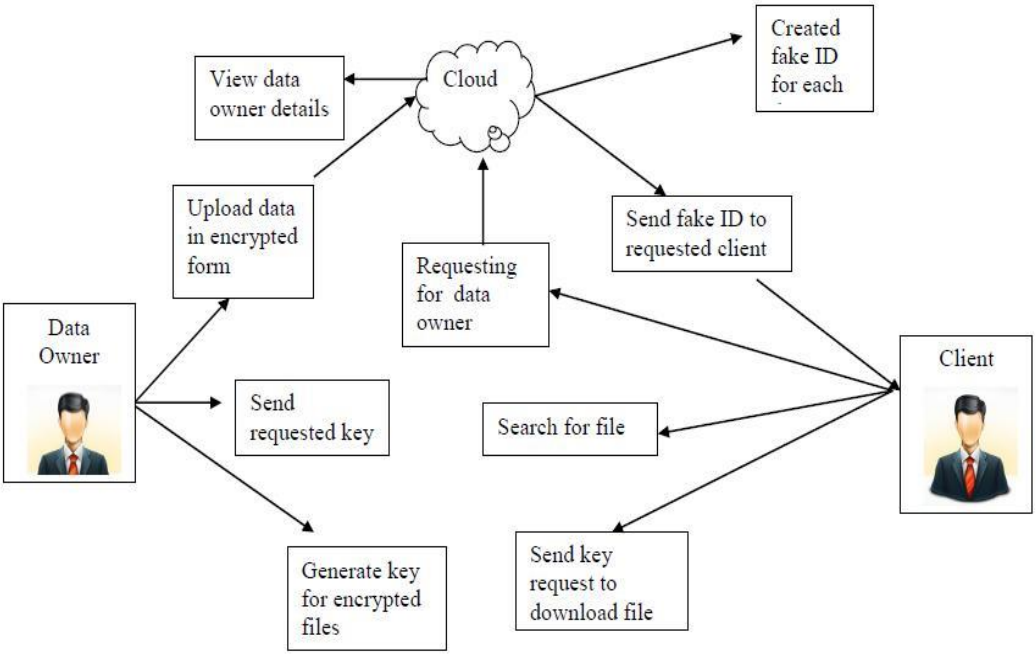

Figure 1: Architecture Diagram.

The purpose of the architecture diagram is to represent the type of software architecture that is used by the system, to describe the various hardware and software components that are used for the system implementation.

6 CONCLUSIONS

By implementing this web based application, In this work, we proposed a deniable CP-ABE scheme to build an audit-free cloud storage service. The deniability feature makes coercion invalid, and the ABE property ensures secure cloud data sharing with a fine-grained access control mechanism. Our proposed scheme provides a possible way to fight against immoral interference with the right of privacy. We hope more schemes can be created to protect cloud user privacy.

7 FUTURE ENHANCEMENTS

The future goal of the project is to provide security to the user details. Secondly to inorder to bring the awareness that there are incidents that happen being stopped by the project among the people to bring the entire medical process to be managed online. The individual customer detail can be viewed throughout the Nations making the transcations online in a secured way which saves time and by this project it is ensured that no third party can access the customer detail thereby securing the data.

8 REFERENCES

[1] Po-Wen Chi and Chin-Laung Lei, ―Audit-Free Cloud Storage via Deniable Attribute-based Encryption,‖ IEEE 2015.

[2] A. Sahai and B. Waters, ―Fuzzy identity-based encryption,‖ in *Eurocrypt*, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ―Attribute-based encryption for fine-grained access control of encrypted data,‖ in *ACM Conference on Computer and Communications Security*, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, ―Ciphertext-policy attribute-based encryption,‖

in *IEEE Symposium on Security and Privacy*, 2007, pp. 321–334.

[5] B. Waters, ―Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,‖ in *Public Key Cryptography*, 2011, pp. 53–70.