I J C T A, 9(32), 2016, pp. 139-144 ISSN: 0974-5572

Deniable Attribute Based Encryption Mechanism for Achieving Better Security of Data Present in the Cloud

D. Shyam Kumar*, G. Vinit Kumar, and A. Subramanyam*****

ABSTRACT

Storing of the data in cloud environment is gaining its importance in recent times because of the advantages and benefits it provides. When the data is maintained in cloud environment means it is handed to the cloud storage service provider. As data is maintained with some second party, privacy for such data is a primary concern of data owner, in order to preserve privacy of such data it is encrypted and stored in cloud environment. All the terms and conditions of cloud service provider makes think data owner that his data is safe and secured, but in reality it is not true some third party members who are interested in data owner's data can get access of it by compromising the cloud service provider or by influencing the cloud owner with whom data is maintained. For protecting privacy of data owner's data in such situations also a deniable attribute based encryption mechanism is proposed where data owner and service provider are to create some fake data which is alike to original data. Since the third party members cannot differentiate original data and fake data privacy of original data is protected.

Keywords: Cloud, Service provider, Data owner, Third party members, Deniable attribute based encryption.

1. INTRODUCTION

Usage of cloud services by many companies and organizations is rapidly increasing because of the flexibility they give to its users. Once data owners store their data in cloud environment they can access it from anyplace and at any time they want and also can give access to who they want. Protecting the data from unauthorised access is very important, so it is encrypted and stored in the cloud. Many encryption techniques have been developed to protect data from unauthorised access among them Attribute based encryption mechanisms has become popular. All these mechanisms were designed keeping in mind that cloud service provider is trusted and that terms and conditions of cloud service provider ensure of preventing unauthorised access data present in the cloud from third party members who are interested in data owner's data.

However in practice it is not true, the third party members can get access to original data by compromising or by influencing the cloud service provider, if this happens all the efforts taken for encrypting the data are wasted. It is very difficult to protect data from outside coercion, so a mechanism using deniable attribute based encryption is developed where users and cloud service provider are needed to create fake user data which resembles original data to prevent access of original data to third party members. When an attempt is made by third party members to access the data in cloud environment by providing wrong credentials they get the fake user data which is alike to original data. As they cannot differentiate original and fake data they get satisfied and do not make any further attempts to access the original data kept in the cloud. Deniability feature of this mechanism is attained by the fact that coercer cannot differentiate original and fake data. This mechanism tries to block all kinds of efforts made by third party members to get access to the data

* PG-Scholar, Department of CSE, AITS-Rajampeta, *Email: shyamkumar1507@gmail.com*

** Associate Professor, Department of CSE, AITS-Rajampeta, *Email: vinitkumar.gunjan@gmail.com*

*** Professor, Head of Department, Department of CSE, AITS-Rajampeta.

situated in the cloud. This method uses ABE characteristics to give better privacy of data maintained in the cloud with well organized access control and deniable encryption. It is similar to that of CP-ABE scheme developed by waters with additional features. Prime order bilinear groups are changed to Composite order bilinear group. Coercers get fake data which is similar to original data because of the sub-group decision problem.

2. DEVELOPMENT OF ABE

Introduction of Attribute Based Encryption (ABE) was first done by Sahai and Waters where data owners are used to set the requirements to decrypt the data kept in cloud and to encrypt data that has to be stored in the cloud. Data consumers who provide exact requirements to decrypt the data can only get original data others get fake data created. Many users wants to use data present in cloud to get their work done by getting authorization so ABE acts as an important mechanism to set privilege for data consumers. There are many users who want to access data stored in the cloud which make pair-wise keys as difficult plus encrypting the data for many times for many users is also difficult. All these difficulties can be removed by ABE, using this data owners can set privilege for accessing the data and those who provide exact requirements can only be allowed to get original data.

Cipher-Text policy Attribute Based Encryption and Key-Policy Attribute Based Encryption are the two types of Attribute Based Encryption mechanisms. Variation in these schemes can be seen in policy checking. The encryption method used in the Key-policy Attribute Based Encryption is laid in the user secret key and attribute sets are laid in cipher-text and encryption mechanism used in the Cipher-text policy Attribute Based Encryption is laid in cipher-text and attribute sets in the user secret key. KP-ABE was first developed by goyal et al. and he also developed a transparent way to connect any formula which is monotonic to the policy for secret key of the user. First Cipher-text Policy Attribute Based Encryption where tree like arrangement is used to show monotonic formula. Waters used Linear Secret Sharing Schemes to construct cipher-text policy and developed first fully expressive cipher-text policy Attribute Based Encryption. Lewko and his other members with some loss in efficiency improved waters method to a completely secured Cp-Abe. Cp-Abe having fixed size of cipher-text was developed by Attrapadung and his co-workers. Cp-Abe for resource constrained users was designed by tysowski.

3. DENIABLE ENCRYPTION MECHANISMS AND LIMITATIONS

Deniable encryption schemes can be divided in to two types same like normal encryption schemes they are

1. Deniable encryption using shared key
2. Deniable encryption using public key

As sharing of data in cloud environment is important all efforts are put into deniable encryption using public key. Translucent sets were used by Canetti et al. to develop deniable encryption schemes; translucent set contains trap-door subset. To find whether an element belongs to subset or not without the trapdoor subset is a hard task, translucent set can be constructed using trapdoor permutation. To develop a deniable public key encryption method with the translucent sets translucent sets can be used as the public key and then trapdoor subset as the private key. One encrypted bit is represented using the translucent set. All the elements in subset are denoted as one and other non subset elements are denoted as zero. If an element of subset is sent sender can encrypt one but can say that element is of universal set and is basic sender deniable scheme. Using intermediary's the sender deniable scheme is modified and made to more powerful receiver deniable scheme or bideniable scheme. Research is going on to find how an efficient translucent set can be designed. Translucent set from samplable encryption was developed by Durmuth et al. ONeill et al. developed a bitranslucent sets with the help of lattice which also can be used for bideniable scheme. Not only bi-

translucent sets but there are other advancements in construction of deniable encryption mechanisms. With help of a simulatable public key method which delivers oblivious key development function and oblivious cipher-text function ONeill et al constructed a deniable encryption mechanism. Sender says that some messages are oblivious even though they are not because he sends a set of encrypted data along with the encrypted bit which might be oblivious or encrypted and if it is applied at receiver side it can be called as bideniable scheme.

Another deniable encryption method where each user has one public-private key pair but actually there are two pairs. The sender encrypts the original message with one key and fake message with other key and sends. Sender can release the key to whoever he wants according to his wish of sharing the original message. This method was developed by Gasti et al. Apart from these deniable encryption schemes a research is going on to know the limitations of the deniable encryption schemes.

4. OUR WORK ON DENIABLE ENCRYPTION

In the developed scheme CP-ABE where policy is embedded in cipher-text and attributes in secret key is used to make cloud storage services more secure and reliable. Sender role in normal deniable encryption scheme is taken by cloud storage service provider. Translucent sets and simulatable keys are not used. The entire data owner's data is encrypted into multidimensional space submitting correct dimensions only can decrypt the encrypted data if wrong dimensions are submitted means encrypted data decrypts to pre-determined fake user data. Information related to the dimensions is maintained secret. Multi-dimensional space is constructed using Composite order bilinear groups and to get similarity between original data and fake data created chameleon hash function is used.

There are many Advantages of proposed scheme over previous schemes:

4.1. Block-wise Deniable ABE

Many of the developed deniable encryption schemes are bitwise schemes so they can process only one bit at a time which makes them inefficient for real-time usage and in cloud storage environment. ONeill et al constructed an encryption scheme which uses simultaneously symmetric and asymmetric encryption which helps deniable encryption schemes when used in cloud environment. Bitwise deniable encryption schemes might be efficient to construct fake user data but in cloud environment where large amount of data comes into play block wise deniable encryption is more efficient.

Our scheme is built by using multiple dimensions but in practice we consider as a single dimension only. Two encryption environments are built in parallel unlike the previous deniable-encryption mechanisms. This mechanism removes redundant parts that are present in the previous schemes. This idea is applied to existing Attribute Based Encryption mechanism and replace prime order group with that of Composite order group. As base Cipher-text Policy Attribute Based Encryption scheme encrypts one block at a time, our deniable Cipher-text Policy Attribute Based Encryption scheme is also a block wise deniable encryption scheme.

4.2. Stability in encryption environment:

Majority of deniable encryption methods developed in starting are independent from their encryption environments which means all encryption environments must not be similar. When any deniable encryptions are done under a similar environment encryptions from second one will be less efficient when the first one is coerced. When a coercer gets a key which is like original key it must work for whole data stored in the cloud environment if it works for some files and does not work for some means coercer will get to know that the key he obtained is a fake one and will try in another way to access the data in the cloud. All previous

encryption schemes do not have proper deniability as it is difficult to have a unique environment for encrypting each file along with fine grained access control mechanism.

Here we construct our deniable encryption mechanism under a consistent environment where numerous encryptions can be done without any system up gradation. The key disclosed in this environment must look convincing to all cipher-texts created in this environment despite how they are encrypted using normal encryption mechanism or deniable encryption mechanism. Deniability feature in our mechanism is attained by sub-group assignment. Using the cancelling feature and by assigning subgroups properly released fake key will be helpful, cipher texts can be decrypted correctly using it.

4.3. Consistency in Decryption

Many decryption errors occur while decrypting the encrypted cipher-texts in many deniable encryption schemes because of design of decryption mechanism. Usage of translucent sets and also the simulatable public key encryption system in deniable encryption mechanisms also introduce decryption problems while decrypting the data.

This mechanism does not use any sets or keys that are vulnerable or of less efficiency so errors due to them are avoided. It also extends pairing Attribute Based Encryption and consistent decryption algorithm is used which avoids many of the decryption errors.

5. DENIABLE ATTRBUTE BASED ENCRYPTION MECHANISM.

Here the deniable attribute based encryption mechanism is constructed from waters ciphertext policy attribute based encryption by enhancing the Composite order bilinear groups to prime order bilinear groups. Some algorithms used in our mechanism are:

INIT: This algorithm takes public properties and the system secret key to setup the functions available in the system.

KEYPRD: This algorithm takes a set of attributes and system secret key and then produces a private secret key.

ENC: This algorithm takes message or data and public properties as input and generates cipher text as output.

DEC: This algorithm takes secret key and ciphertexts and public properties as inputs and decrypts the cipher texts. Output of this algorithm is original message that has been encrypted.

DENSETUP: This algorithm takes system secret key, public properties and secret key and setups the deniability feature for this mechanism.

DENKEYGEN: This algorithm takes system secret key and set of attributes as inputs and generates the key to create fake user data.

DENENC: This algorithm takes public properties, system secret key, and secret key and other data as inputs and submits fake user data created when wrong secret key is provided.

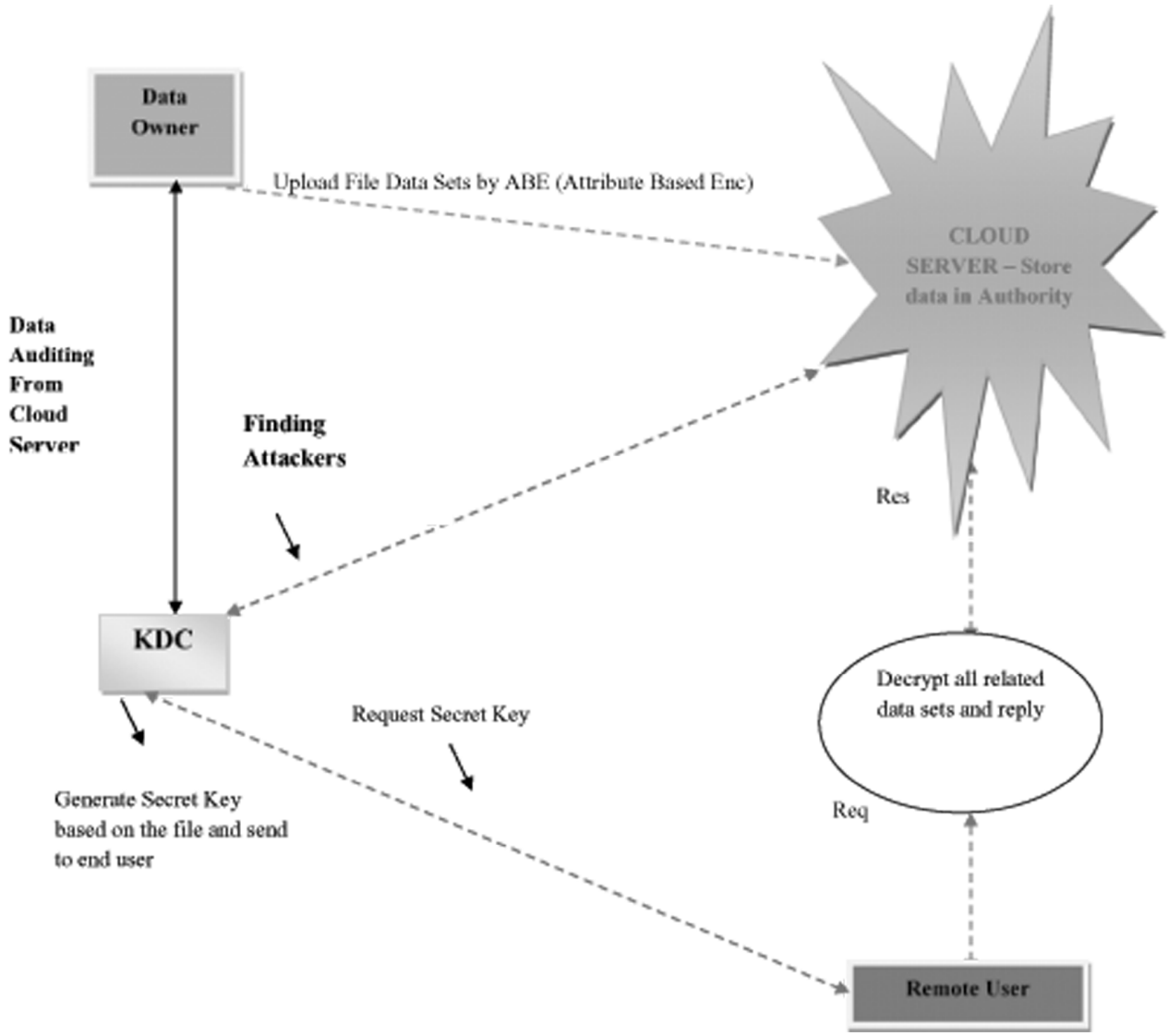
VERIFY: This algorithm verifies the correctness of encrypted data and the decrypted data.

DENOPENENC: This algorithm is to release the fake encryption proof for the fake data created.

DENOPENDEC: This algorithm is to release the fake decryption proof for fake data created.

CLOUD SERVER: Store data in Authority

6. ARCHITECTURE DIAGRAM



ABE—Attribute Based Encryption

Data Sets—Personal Details, Medical Report, Medical Summary

7. IMPLEMENTATION

7.1. Owner of Data

The owner of the data registers himself at service provider and uploads his data after encryption so that unauthorized access can be prevented. He can manipulate his data and can decide who has to access his data by setting certain requirements.

7.2. Cloud

The service provider will allocate space for owner of the data in the cloud so that he can store data after encrypting it and after keeping data in the cloud end users can use the data whenever or at anytime they need it. The end users must be authorized before they access the data, after authorization they can download it and decrypt it with key provided.

7.3. Key Distribution centre

KDC performs authorization by using verification parameters and give a secret key to end user to access the data when user satisfies verification parameters. All the coercers must be identified.

7.4. Data Consumer/End User

Here user get to access the data using secret key which is given when user satisfies the authorization parameters set by the data owner. By using the key he can download the data and decrypt it. End user can also view the list of data owners so that he can use whose data he need. All the privileges to access data owner are set by owner of the data so end users are controlled by owners of the data. In order to access data end user sends request to KDC to generate secret key and KDC will generate the secret key and send to corresponding end user.

7.5. Attacker (Unauthorized User)

Attacker or unauthorized user tries to get access of data without satisfying parameters set by data owner and causes issues for data owner.

8. CONCLUSION

In this work, a deniable CP-ABE mechanism to achieve better security for the data stored in the cloud environment has been proposed. All the unauthorized actions on the data kept in the cloud are avoided by the deniability property of the mechanism and ABE property assures secured sharing of data in the cloud with a well organized access control mechanism. More advanced schemes can be developed for protecting and providing privacy to the data stored in the cloud in near future.

REFERENCES

[1] Fuzzy Identity-based Encryption, by A. Sahai and B. Waters in Eurocrypt, 2005.

[2] Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, in ACM Conference on Computer and Communications Security by V. Goyal, O. Pandey, A. Sahai, and B. Waters, 2006.

[3] Hybrid Attribute and Re-encryption Based Key Management for Secure and Scalable Mobile Applications in Clouds, by P. K. Tysowski and M. A. Hasan, IEEE T. Cloud Computing.

[4] Deniable Encryption, in Crypto, 1997 by R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky.

[5] Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption, in Eurocrypt, 2010 by A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters.

[6] Attribute-Based Encryption Schemes with Constant-Size Ciphertexts, by N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. R‘afols.

[7] Bideniable Publickey Encryption, in *Crypto*, 2011 by A. O’Neill, C. Peikert, and B. Waters.

[8] Deniable cloud storage: sharing files via public-key deniability in *WPES*, 2010 by P. Gasti, G. Ateniese, and M. Blanton.