International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

A Literature Review On Audit Free Cloud Storing Through Deniable Attribute-Based Encryption

Kunchala Ashok#1& K.V Srenivas Rao #2
1PG Scholar, Dept of CSE, Prakasam Engineering College, Singarayakonda, Prakasam(Dt), AP, India.
2Associative Professor, Dept of CSE, Prakasam Engineering College, Singarayakonda, Prakasam(Dt), AP, India.

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 provider ensure that user privacy is still securely protected.

Keywords– Cloud computing, Deniable Encryption, Attribute Based Encryption, Data security and Privacy.

1. INTRODUCTION

Cloud storage is a form of data storage where the digital data is stored in logical pools, the physical storage span multiple servers (and often locations), and the physical environment is typically owned and handled by a hosting organization. These cloud storage providers are answerable for keeping the data available and accessible, and the physical environment protected and running. Different organizations buy or lease storage capacity from the providers to store customer application data. Cloud storage services may be accessed through a co-located cloud computer service, a web Service application programming interface (API)[4] or by applications that utilize the API, such as cloud desktop storage, a gateway or Web- based content management systems. In the cloud storage environment customers can store their data on the cloud and access their data from anywhere at any time by connecting to a network. Because of user privacy, the data stored on the cloud is normally encrypted and safe guarded from access by other users. Considering the collaborative property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage. Attribute-based encryption is a kind of public-key encryption in which the secret key of a user and the ciphertext are reliant upon attributes. In such a structure, the decryption of a ciphertext is achievable only if the set of attributes of the user key equals the attributes of the ciphertext.[5]. A central security feature of Attribute-Based Encryption is collusion-resistance: An challenger that grasps multiple keys be supposed to only be capable to access data if at least one individual key grants access. The aim choosing this attribute-based encryption is that as more responsive, data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One disadvantage of encrypting data is that it can be selectively

shared only at a coarse-grained level (i.e., giving another party your private key). To overcome this disadvantage we used a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In this cryptosystem, ciphertext are labeled with sets of attributes and private keys are associated with access structures that control which ciphertext by this the user can easily able to decrypt the data which was encrypted. The applicability of this construction is to share the audit-log information and broadcast encryption and also supports delegation of private keys which includes the Hierarchical Identity-Based Encryption. These Encryption schemes assuring that cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked.

2. RELATED WORK:

The concept of ABE(Attribute-Based Encryption) in which data owners can insert how they want to distribute data in terms of encryption. That is, only those who match the owner's conditions can successfully decrypt stored data. We can say here that ABE is encryption for privileges, not for users. This makes ABE a very helpful tool for cloud storage services since data sharing is a significant feature for such services. Cloud storage users are not practical for data owners to encrypt their data by pair wise keys. Furthermore, it is also impractical to encrypt data many times for many people. With ABE, data owners make a decision only which kind of users can access their encrypted data. Users who convince the conditions are able to decrypt the encrypted data. The scheme of deniable encryption is nothing but it also similar to common encryption schemes, deniable encryption can be separated into a deniable shared key scheme and a public key scheme. Allowing the cloud storage scenario, we focus our efforts on the deniable public key encryption scheme. The simulatable public key system provides an unaware key generation function and an oblivious cipher text function. When transferring an encrypted bit, the sender will send a set of encrypted data which may be usually encrypted or insensible. Therefore, the dispatcher can claim some sent messages are oblivious while actually they are not. The scheme can be applied to the receiver side such that the scheme is a bi-deniable scheme. While performing this scheme there are some disadvantages may arise. Those are Computational overhead. I.e. Encryption parameters should be totally different for each encryption operation. So each coercion will reduce flexibility. We can also face Decrypted data with missing of contents at such blocks. Entities of the cloud environment may stop communications between users and cloud storage providers and then require storage providers to release user secrets by using power or other means. In this situation, encrypted data are assumed to be known and storage providers are requested to discharge user secrets here another disadvantage is Data redundancy is Occur at each block of data. The non interactive and fully receiver deniable schemes cannot be achieved simultaneously. It is also impossible to encrypt unbounded messages, using one short key in non committing schemes.

The future performance scheme with Cipher Text Policy Attribute Based encryption presents a cloud storage provider which means to make fake user secrets. Specified such fake user secrets, outside coercers can only obtained fake data from a user's stored cipher text. The coercers think the received secrets are real, they will be content and more prominently cloud storage providers will not have revealed any real secrets. So, user privacy is still confined in cloud computing environment[7].

In order to overcome all these disadvantages Cipher text policy attribute-based encryption

(CP-ABE) scheme is being implemented. The implementation of a deniable CP-ABE scheme that can make cloud storage services secure and audit free. In these circumstances, cloud storage service providers will just watch as receivers in other deniable schemes. Unlike most previous deniable encryption schemes, we do not use transparent sets or simulatable public key systems to apply deniability. Deniable Cipher Text Policy Attribute Based Encryption scheme make with two encryption environments at the same time, much like the idea planned in this scheme with many sizes while claiming there is only one size. This approach removes clear redundant parts. The base ABE scheme can encrypt one block each time; our deniable CPABE is definitely a block wise deniable encryption scheme. The bilinear operation for the Composite order group is slower than the prime order group, there are some methods that can change an encryption scheme from Composite order groups to prime order groups for improved computational performance. Deniable Cipher Text Policy Attribute Based Encryption offers a reliable environment for our deniable encryption scheme[8]. This scheme extends a pairing ABE, which has a deterministic decryption algorithm.

3. LITERATURE SURVEY:

#A unified scheme for resource protection in automated trust negotiation

AUTHORS: Ting Yu , Winslett, M.

Automated trust negotiation is an approach to establishing trust between strangers through iterative disclosure of digital credentials. In automated trust negotiation, access control policies play a key role in protecting resources from unauthorized access. Unlike in traditional trust management systems, the access control policy for a resource is usually unknown to the party requesting access to the resource, when trust negotiation starts. The negotiating parties can rely on policy disclosures to learn each other's access control requirements. However a policy itself may also contain sensitive information. Disclosing policies' contents unconditionally may leak valuable business information or jeopardize individuals' privacy. This paper proposing UniPro, a unified scheme to model protection of resources, including policies, in trust negotiation. UniPro improves on previous work by modeling policies as first-class resources, protecting them in the same way as other resources, providing fine-grained control over policy disclosure, and clearly distinguishing between policy disclosure and policy satisfaction, which gives users more flexibility in expressing their authorization requirements. It also show that UniPro can be used with practical negotiation strategies without jeopardizing autonomy in the choice of strategy, and present criteria under which negotiations using UniPro are guaranteed to succeed in establishing trust.

#Ciphertext-Policy Attribute Base Decryption AUTHORS: John Bethencourt, Amit Sahai, Brent Waters In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. This paper presenting a system for realizing complex access control on encrypted data that call Ciphertext-Policy Attribute-Based Encryption. By using this techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, this methods are secure against collusion attacks. Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in this system attributes are used to describe a user's credentials, and a party encrypting data

determines a policy for who can decrypt. Thus, this methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition,it provide an implementation of our system and give performance measurements.

4.EXISTING SYSTEM :

There are numerous ABE schemes that have been proposed. Most of the proposed schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked; however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using government power or other means. In this case, encrypted data are assumed to be known and storage providers are requested to release user secrets.

Sahai and Waters first introduced the concept of ABE in which data owners can embed how they want to share data in terms of encryption.

There are two types of ABE, CP-ABE and Key-Policy ABE (KP-ABE).Goyal et al. proposed the first KPABE. They constructed an expressive way to relate any monotonic formula as the policy for user secret keys. Bethen court et al. proposed the first CP-ABE. This scheme used a tree access structure to express any monotonic formula over attributes as the policy in the ciphertext.

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.

Use translucent sets table public key systems to implement deniability.

Most deniable public key schemes are bitwise, which means these schemes can only process one bit a time; therefore, bitwise deniable encryption schemes are inefficient for real use, especially in the cloud storage service case. Most of the previous deniable encryption schemes are inter-encryption independent. That is, the encryption parameters should be totally different for each encryption operation. If two deniable encryptions are performed in the same environment, the latter encryption will lose deniability after the first encryption is coerced, because each coercion will reduce flexibility. Most deniable encryption schemes have decryption error problems. These errors come from the designed decryption mechanisms.

5.PROPOSED SYSTEM :

In this work, It is describing a deniable ABE scheme for cloud storage services. By make use of ABE characteristics for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing. This scheme is based on Waters ciphertext policy-attribute based encryption (CP-ABE) scheme. This enhance the Waters scheme from prime order bilinear groups to composite order bilinear groups. By the subgroup decision problem assumption, this scheme enables users to be able to provide fake secrets that seem legitimate to outside coercers.

In this work, constructing a deniable CP-

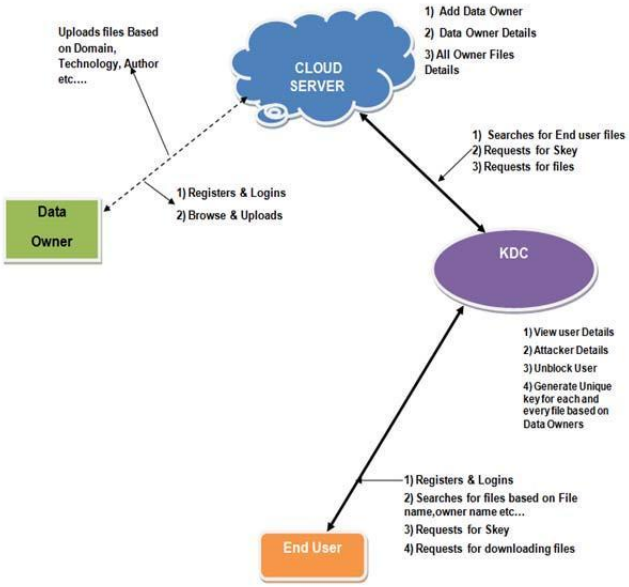
ABE scheme that can make cloud storage services secure and audit free. In this scenario, cloud storage service providers are just regarded as receivers in other deniable schemes.

Unlike most previous deniable encryption schemes, it is not useing translucent sets table public key systems to implement deniability. Instead, this adopt the idea proposed with some improvements. This construct deniable encryption scheme through a multidimensional space. All data are encrypted into the multidimensional space.

Only with the correct composition of dimensions is the original data obtainable. With false composition, cipher texts will be decrypted to predetermined fake data. The information defining the dimensions is kept secret. This make use of composite order bilinear groups to construct the multidimensional space. This also use chameleon hash functions to make both true and fake messages convincing.

In this work, there is a consistent environment for deniable encryption scheme. By consistent environment, 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 environment, regardless of whether a cipher text is normally encrypted or deniably encrypted. The deniability of this 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, can construct the released fake key to decrypt normal cipher texts correctly.

6.SYSTEM ARCHITECTURE :



- **Data Owner**

  In this module, the cloud server adds data owner by Registering with their details like owner name, password, email, organization and address, The Data owner Logins by user name and password. The data owner browses and uploads their data in the cloud server by providing details Domain (Cloud computing, Data mining, networking, sensor networking, adhoc networking), Technology (Java, Dot net, SAP, PHP, NS2), Author name and publication. For the security purpose the Data owner encrypts data as well as encrypted keyword-index stores to the cloud Server.

Cloud Server

The cloud server is responsible for data storage and files authorization and file search for an end user. The encrypted data file contents will be stored with their tags such as file name, domain, Technology, Author, Publication, secret key, digital sign, date and time and

owner name. The data owner is also responsible for adding data owner and to view the data owner files. The owner can conduct keyword search operations on behalf of the data users, the keyword search based on keywords (Author, Technology, Domain, publishers) will be sent to the Trust authority. If all are true then it will send to the corresponding user or he will be captured as attacker. The cloud server can also act as attacker to modify the data which will be auditing by the audit cloud.

Data Integrity

Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.

KDC

The KDC allows clients and cloud applications to simultaneously data user services from and route data to cloud. Module issues credentials to the data users. The credentials are sent over authenticated private channels. It is responsible of searching, requesting the file to cloud server, generating secret key for each and every files based on data owner and provides to the Data user.

Data Consumer (Data User/End User)

In this module, the user is responsible of searching the files in cloud server by providing attributes like Technology, author name, publisher, Domain(cloud computing, network security,). The data consumer can request the secret key to cloud server via KDC and then the Data Consumer can access the data file with the encrypted key, so if User access the file by wrong Key then the user will consider as malicious users and blocked the User.

7.CONCLUSION:

A deniable CP-ABE scheme is an audit-free cloud storage service. The deniability feature makes force invalid, and the Attribute Based Encryption

belongings guarantee secure cloud data sharing with a fine-grained access control method. This scheme presents a likely way to struggle next to dissipated intervention with the right of privacy. Not only the above can this scheme be formed to guard cloud user privacy with high computational performance.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Eurocrypt, 2005, pp. 457–473.

[2] 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.

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

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

[5] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in Crypto, 2012, pp. 199–217.

[6] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in Public Key Cryptography, 2013, pp. 162–179.

[7] K. Liang, L. Fang, D. S. Wong, and W. Susilo, "A ciphertext policy attribute-based proxy re-encryption with chosen-ciphertext security," IACR Cryptology ePrint Archive, vol. 2013, p. 236, 2013.