International Journal of Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.05,Issue.17
July-2016,
Pages:3449-3451

www.ijsetr.com

Audit Free Cloud Storage via Deniable Attribute Base Encryption for Protecting User Privacy

SRIDHAR REDDY[1], P. SATHISH REDDY[2], PABBU SRAVANTHI[3]

[1]Assist Prof, Dept of CSE, Kasireddy Narayan Reddy College of Engineering & Research, Hayathnagar, RR(Dt), TS, India.
[2]Assoc Prof&HOD, Dept of CSE, Kasireddy Narayan Reddy College of Engineering & Research, Hayathnagar, RR(Dt), TS, India.
[3]PG Scholar, Dept of CSE, Kasireddy Narayan Reddy College of Engineering & Research, Hayathnagar, RR(Dt), TS, 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.

I. INTRODUCTION

Hiding platform and implementation details unlimited virtualized resources provided to the users as a service is a cloud computing. Presently cloud service provided to the users offered high available storage and massively parallel computing of resources at relatively low costs. But the question is about the cloud users with different privileges store data on cloud is a most challenge issue in managing cloud data storage system. Most important problem for cloud environment is privileges.

II. PROBLEM STATEMENT

The problem is to determine, public auditing for such shared data while preserving identity privacy remains to be an open challenge. unique problem introduced during the process of public auditing for shared data in the cloud is how to preserve identity privacy from the TPA(Third Party Auditor).

III. LITERATURE SURVEY

A. 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. Thenegotiating 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.

B. Ciphertext-Policy Attribute Base Decryption

AUTHORS: John Bethencourt, AmitSahai, 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.

C. Fuzzy Identity Based Encryption

AUTHORS: AmitSahai , Brent R. Waters

This introduce a new type of Identity Based Encryption (IBE) scheme that it call Fuzzy Identity Based Encryption. A Fuzzy IBE scheme allows for a private key for an identity id to decrypt a ciphertext encrypted with another identity id # if and only if the identities id and id # are close to each other as measured by some metric (e.g. Hamming distance). A Fuzzy IBE scheme can be applied to enable encryption using biometric measurements as identities. The error-tolerance of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently contain some amount of noise during each measurement.

IV. RELATED WORK

Secure auditing and deduplication is big problem in cloud environment.

- **Audit:** This technique can securely monitoring server space allocation.
- **Deduplication:** This technique is dealing with how to maintain back up data and remove unwanted file on server.

V. 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.

VI. 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.

VII. SYSTEMARCHITECTURE

A. 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 as shown in Fig.1. 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.

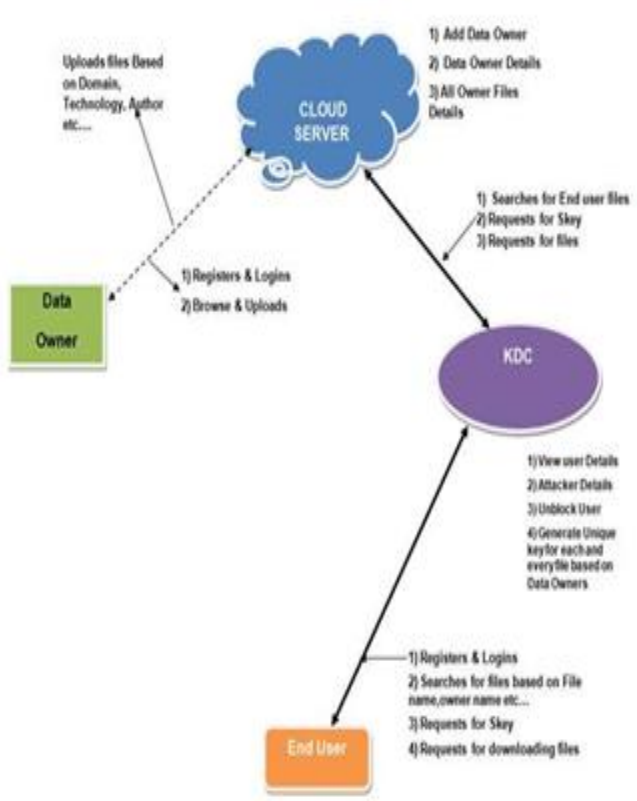

Fig.1. System architecture.

B. 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.

C. 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.

D. 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.

E. 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.

VIII. CONCLUSION

It can be conclude this paper deals with how to securely audit public data and how to put security public data when share data. How to provide security base on attribute schema.

IX. 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,"inACM 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.