International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.1., 2016
(Jan-Feb)

REVIEW ARTICLE

ISSN: 2321-7758

CLOUD STORAGE IN ASSESSMENT FREE USING DENIABLE ENCRYPTION-A SURVEY

SHREEKANTH SALOTAGI[1], PRADEEP MUTTIGI[2]

[1]Department of Computer Science and Engineering,
Secab Institute of Engineering & Technology, Vijayapur, Karnataka, India
Nauraspur, Bagalkot road ,vijayapur, Karnataka, India,
[2]Department of Computer Science and Engineering,
Secab Institute of Engineering & Technology, Vijayapur, Karnataka, India
Naurasarpur,Bagalkot raod,Vijayapur, Karnataka,India

ABSTRACT

Storage service in the cloud is gaining appreciation in the world. Cloud storage provides confidentiality and security to protect data from others who don't have access. This is done by many cloud storage encryption schemes; attribute-based-encryption (ABE) is most proper encryption schemes for cloud storage. Encryption schemes used in the cloud storage believe that data stored in the cloud are secure and confined from the hacker; but, in reality some authorities may force cloud storage provider to reveal users details and undisclosed information stored on the cloud. Once cloud storage providers are compromised, all encryption schemes loss their effectiveness. It is very complex to fight against such authorities to keep users information safe and protected. A design for new cloud storage encryption scheme that helps the cloud providers to produce fake user secrets to defend user information and privacy. As authorities cannot inform whether the obtained information are true or not.

I. INTRODUCTION

Cloud storage services have rapidly become popular. Users can store their data on the cloud and access their data anywhere at any time. Because of user confidentiality, the data stored on the cloud is typically encrypted and protected 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.

Most of the planned 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. As an example, in 2010, without notifying its users, Google released user documents to the FBI after receiving a search warrant. In 2013, Edward Snowden disclosed the existence of global surveillance programs that collect such cloud data as emails, texts, and voice messages from some technology companies. Once cloud storage providers are compromised, all encryption schemes lose their effectiveness. Though we hope cloud storage providers can fight against such entities to maintain user privacy through legal avenues, it is seemingly more and more difficult. As one example, Lava bit was an email service company that protected all user emails from outside coercion; unfortunately, it failed and decided to shut down its email service.

Since it is difficult to fight against outside coercion, we aimed to build an encryption scheme that could help cloud storage providers avoid this predicament. In our approach, we offer cloud storage providers means to create fake user secrets. Given such fake user secrets, outside coercers can only obtained forged data from a user's stored cipher text. Once coercers think the received secrets are real, they will be satisfied and more importantly cloud storage providers will not have revealed any real secrets. Therefore, user privacy is still protected.

This concept comes from a special kind of encryption scheme called deniable encryption, first proposed in. Deniable encryption involves senders and receivers creating convincing fake evidence of forged data in cipher texts such that outside coercers are satisfied. Note that deniability comes from the fact that coercers cannot prove the proposed evidence is wrong and therefore have no reason to reject the given evidence. This approach tries to altogether block coercion efforts since coercers know that their efforts will be useless. We make use of this idea such that cloud storage providers can provide audit-free storage services. In the cloud storage scenario, data owners who store their data on the cloud are just like senders in the deniable encryption scheme. Those who can access the encrypted data play the role of receiver in the deniable encryption scheme, including the cloud storage providers themselves, who have system wide secrets and must be able to decrypt all encrypted data1.

A deniable ABE scheme for cloud storage services. ABE characteristics can be used for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing. This scheme is based on Waters cipher text policy-attribute based encryption (CP-ABE) scheme. This scheme 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.

II. RELATED WORK

In [1], Amit Sahai, Brent Waters "Fuzzy Identity-Based Encryption" Produce A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a cipher text encrypted with an identity, $\omega\_$, if and only if the identities ω and $\omega\_$ are close to each other as measured by the "set overlap" distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term "attribute-based encryption".

In[2], Vipul Goyal, Amit Sahai, Omkant Pandey, Brent Waters Introduce,ABE for Fine-Grained Access Control of Encrypted Data" .As more sensitive 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 drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KPABE). In our cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

In [3], Brent Waters, introduce Cipher text-Policy Attribute-Based-Encryption (ABE).In this solutions CP-ABE allow to encrypt or to specify access control in terms of any access formula over the attributes in the system. In our most efficient system, cipher text size, encryption, and decryption time scales linearly with the complexity of the access formula. We present three constructions within our framework. Our first system is proven selectively secure under a assumption that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption. Our next two constructions provide performance tradeoffs to achieve provable security respectively under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions.

In [4], Susan Hohenberger, Brent Waters ,Analyses of Attribute-Based Encryption with Fast Decryption. which present the first key-policy ABE system where cipher texts can be decrypted with a constant number of pairings. We show that GPSW cipher texts can be decrypted with only 2 pairings by increasing the private key size by a factor of j□j, where □ is the set of distinct attributes that appear in the private key. We then present a generalized construction that allows each system user to independently tune various efficiency tradeoffs to their liking on a spectrum where the extremes are GPSW on one end and our very fast scheme on the other. This tuning requires no changes to the public parameters or the encryption algorithm. Strategies for choosing an individualized user optimization plan are discussed. Finally, we discuss how these ideas can be translated into the cipher text-policy ABE setting at a higher cost.

In[5],Ran Canetti, Cynthia Dwork, Moni Naor, Rafi Ostrovsky “Deniable Encryption” Consider a situation in which the transmission of an encrypted message can be intercepted by an authority, and subsequently (say, in response to court order) the sender can be coerced to reveal the keys and random choices used in generating the cipher text, thereby revealing the message sent. An encryption scheme is deniable if the sender can generate “plausible” keys and random choices that will satisfy the authority and at the same time keep the past communication private. Analogous requirements can be formulated with respect to coercion of the receiver and with respect to coercion of both parties. Deniable encryption is a strong primitive. In particular, it yields the first solution to the problem of incoercible (“receipt-free”) voting requiring no physical security assumptions.

In[6], Markus Durmuth, David Mandell Freeman, Introdude Deniable Encryption with Negligible Detection Probability.It Guarantees that the sender or the receiver of a secret message is able to “fake” the message encrypted in a specific cipher text in the presence of a coercing adversary, without the adversary detecting that he was not given the real message. We propose the first sender-deniable public key encryption system with a single encryption algorithm and negligible detection probability. We describe a generic interactive construction based on a public key bit encryption scheme that has certain properties, and we give two examples of encryption schemes with these properties, one based on the quadratic residuosity assumption and the other on trapdoor permutations.

In[7], Allison Lewko, introduced Tools for Simulating Features of Composite Order Bilinear Groups in the Prime Order Setting.Here, we explore a general methodology for converting Composite order pairing based cryptosystems into the prime order setting. We employ the dual pairing vector space approach initiated by Okamoto and Takashima and formulate versatile tools in this framework that can be used to translate Composite order schemes for which the prior techniques of Freeman were insufficient. Our techniques are typically applicable for Composite order schemes relying on the canceling property and proven secure from variants of the subgroup decision assumption, and will result in prime order schemes that are proven secure from the decisional linear assumption.

In[8],Ran Canetti, Shai Halevi, and Jonathan Katz ,Prensents Chosen-Cipher text Security from Identity-Based Encryption. Here CPA-secure identity-based encryption (IBE) scheme construction requires the underlying IBE scheme to satisfy only a relatively weak notion of security which is known to be achievable without random oracles; thus, our results provide a new approach for constructing CCA-secure encryption schemes in the standard model. Our approach is quite different from existing ones; in particular, it avoids non-interactive proofs of “well forkedness" which were shown to underlie most previous constructions. Furthermore, applying our conversion to some recently-proposed IBE schemes results in CCA-secure schemes whose efficiency makes them quite practical. Our technique extends to give a simple and reasonably efficient method for securing any binary tree encryption (BTE) scheme against adaptive chosen cipher text attacks.

In [9], Kaitai Liang, Liming Fang, Duncan S. Wong, Willy Susilo,introduced A Cipher text-Policy Attribute-Based Proxy Re-Encryption with Chosen Cipher text Security. Cipher text-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE) extends the traditional Proxy Re-Encryption (PRE) by allowing a semi-trusted proxy to transform a cipher text under an access policy to the one with the same plaintext under another access policy (i.e. attribute-based re-encryption). The proxy, however, learns nothing about the underlying plaintext. CP-ABPRE has many real world applications, such as fine-grained access control in cloud storage systems and medical records sharing among different hospitals. Previous CP-ABPRE schemes leave how to be secure against chosen-cipher text attacks (CCA) as an open problem. This paper, for the first time, proposes a new CP-ABPRE to tackle the problem. ..

III. SCHEME DESCRIPTION

Most deniable public key schemes are bitwise, which means these schemes be able to process one bit a time. Hence, bitwise deniable encryption schemes are incompetent for real use, mainly in the cloud storage service case. To resolve this problem, considered a hybrid encryption scheme that concurrently uses symmetric and asymmetric encryption. They use a deniably encrypted plan-ahead symmetric data encryption key, while real data are encrypted by a symmetric key encryption mechanism. Mainly deniable encryption schemes have decryption error problems. These errors come from the considered decryption mechanisms. Uses the subset decision mechanism for decryption. The receiver decides the decrypted message according to the subset decision result. If the sender desires an element from the universal set but unluckily the element is located in the specific subset, then an error occurs. The identical error occurs in all transparent set- based deniable encryption schemes. Scope the policy of a file might be unused to under the request by the customer, when concluding the time of the agreement or totally move the files starting with one cloud then onto the next cloud nature's domain. The position when any of the above criteria exists the policy will be rejecting and the key director will totally withdraw from the public key of the associated file. So no one can pick up the control key of a repudiated file in future. Due to this reason we can say the file is certainly erased. To get well the file, the user must ask for the key controller to fabricate the public key. For that the user must be verified. The key policy attribute based encryption standard is utilized for file access which is confirmed by means of an attribute connected with the file.

Deniable Encryption process: Deniable encryption involves senders and receivers creating believable fake proof of fake data in cipher texts such that outside coercers are pleased. Note that deniability comes from the truth that coercers cannot confirm the proposed facts is incorrect and as a result no reason to decline the given evidence. This approach tries to overall block coercion efforts since coercers know that their efforts will be useless. We make use of this idea such that cloud storage providers can give audit-free storage services. In the cloud storage situation, data owners who store their data on the cloud are just like senders in the deniable encryption scheme. Those who can access the encrypted data play the role of receiver in the deniable encryption scheme, including the cloud storage providers themselves, who have system wide secrets and must be able to decrypt all encrypted data. We make use of ABE characteristics for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing.

Attribute Based Encryption: Cloud storage services have rapidly become increasingly popular. Users can store their data on the cloud and access their data anywhere at any time. For the reason of user privacy, the data stored on the cloud is typically encrypted and protected from access by other users. Considering the mutual property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage. There are several ABE schemes that have been proposed, including. Most of the proposed schemes assume cloud storage service providers or trusted third parties managing key management are trusted and cannot be hacked; yet, in practice, some entities may cut off 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 understood to be known and storage providers are requested to release user secrets

Distributed Key Policy Attribute Based Encryption: KP-ABE is a public key cryptography primitive for one-to-many correspondences. In KP-ABE, information is associated with attributes for each of which a public key part is described. The encrypt or acquaintances the set of attributes to the message by scrambling it with the comparing public key parts. Each client is assigned an access arrangement which is normally characterized as an access tree over information attributes. Client secret key is characterized to reproduce the access structure so the client has the skill to decipher a cipher-text if and just if the information attributes fulfil his access structure.

IV. CONCLUSIONS

A survey work carried out on deniable CP-ABE scheme to construct an audit-free cloud storage service. The deniability quality makes intimidation unacceptable, and the ABE property ensures secure cloud data sharing with a fine-grained access control mechanism. planned scheme provides a potential way to fight beside immoral interference with the precise of confidentiality and more schemes can be created to protect cloud user privacy.

REFERENCES

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

[2]. 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]. B.Waters, “Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in *Public Key Cryptography*, 2011, pp. 53–70.R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, “High-speed digital-to-RF converter,” U.S. Patent 5 668 842, Sept. 16, 1997.

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

[5]. R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, “Deniable encryption,” in *Crypto*, 1997, pp. 90–104./

[6]. M. D¨urmuth and D. M. Freeman, “Deniable encryption with negligible detection probability: An interactive construction,” in *Eurocrypt*, 2011, pp. 610–626. “PDCA12-70 data sheet,” Opto Speed SA, Mezzovico, Switzerland.

[7]. B. Lewko, “Tools for simulating features of composite order bilinear groups in the prime order setting,” in *Eurocrypt*, 2012, pp. 318–335.

[8]. D. Boneh, R. Canetti, S. Halevi, and J. Katz, “Chosen-ciphertext security from identity-based encryption,” *SIAM J. Comput.*, vol. 36, no. 5, pp. 1301–1328, 2007.

[9]. K. Liang, L. Fang, D. S. Wong, and W. Susilo, “A ciphertextpolicyattribute-based proxy re-encryption with chosen-ciphertextsecurity,” *IACR Cryptology ePrint Archive*, vol. 2013, p. 236, 2013