IRA-International Journal of Technology & Engineering
ISSN 2455-4480; Vol.05, Issue 01 (2016)
Pg. no. 1-5
Institute of Research Advances
http://research-advances.org/index.php/IRAJTE

A Survey on Audit Free Cloud Storage via Deniable Attribute Based Encryption

[1] P. Santhi, [2] S. Thilagamani

[1] Associate Professor, Department of Computer Science and Engineering, M.Kumarasamy College of Engineering, Karur, India.

[2] Dean & Professor, Department of Computer Science and Engineering, M.Kumarasamy College of Engineering, Karur, India.

Type of Reviewed: Peer Reviewed.
DOI: http://dx.doi.org/10.21013/jte.v5.n1.p1

How to cite this paper:
Santhi, P., & Thilagamani, S. (2016). A Survey on Audit Free Cloud Storage via Deniable Attribute Based Encryption. *IRA-International Journal of Technology & Engineering* (ISSN 2455-4480), 5(1), 1-5. doi:http://dx.doi.org/10.21013/jte.v5.n1.p1

ABSTRACT

Cloud computing is a rising technology which provider an assortment of opportunities for online distribution of resources or services. The most effective advantage of using cloud computing is higher availability of services with less cost and simple scalability. While the storage space of shared data on remote servers is not a new development, current development of cloud computing validates a more careful look at its actual consequences involving privacy and confidentiality issues. As users no longer actually possess the storage of their data, traditional cryptographic primitives for the purpose of data protection cannot be directly accepted. In particular, simply downloading all the data for its integrity confirmation is not a realistic explanation due to the expensiveness in I/O and transmission cost across the network. Besides, it is often not enough to detect the data corruption only when contacting the data, as it does not offer users correctness assurance for those un-accessed information and might be too late to recover the data loss or damage. To fully make sure the data integrity and save the cloud users' calculation resources as well as online burden, it is of critical importance to allow public auditing service for cloud data, so that users may choice to an independent third party auditor (TPA) to audit the contract out data when needed. The TPA, who has expertise and abilities that users do not, can occasionally check the honesty of all the data stored in the cloud on behalf of the users, which provides a much more better and reasonable way for the users to ensure their storage rightness in the cloud. In a word, allowing public auditing services will play an important role for this emerging cloud market to become fully recognized; where users will need ways to evaluate risk and gain hope in the cloud.

Keywords: Storage, Auditing, ABE algorithm, security

I. INTRODUCTION

There is a style for sensitive customer data to be stored by third parties on the internet. For example special email, information and individual preferences are stored on web portal sites such as Google and yahoo. The attack association center, dshield.org, presents combined views of attacks on the internet, but stores interruption reports separately submitted by users. Given the variety, quantity and the significance of information stored at these sites, there is reason for concern that private data will be compromised. In distributed settings with untrusted servers, such as the cloud applications need mechanisms for composite access control over encrypted data [9]. ABE is a new public key based one-to-many encryption that allows access control over encrypted data using access policies and ascribed attributes related with private keys and cipher texts the cryptosystem allowed for decryption while at least k attributes overlapped between a cipher text and a secret key[2].

II. LITERATURE REVIEW

Waters present three constructions within framework. The system is confirmed selectively secure under a hypothesis that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) supposition which can be viewed as a sweeping statement of the BDHE assumption. The next two constructions provide concert tradeoffs to achieve provable security in that order under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions [3].

Hohenberger implement the original key-policy ABE system where cipher texts can be decrypted with a invariable digit of pairings. They show that GPSW cipher texts can be decrypted with simply 2 pairings by growing the private key size by a reason of |T|, where T is the set of different attributes that appear in the private key. Then they present a general construction that allows all system user to in competition tune various efficiency tradeoffs to their liking on a field where the extremes are GPSW on single end and our very fast scheme on the other. This tuning requires no changes to the public parameter or the encryption algorithm. Strategies for choose an individualized user optimization plan are discuss. Finally, we discuss how these ideas can be translate into the cipher text-policy ABE setting at a higher cost [6].

Tysowski presents novel modifications to attribute based encryption are used to allow certified users access to cloud data based on the agreement of required attributes such that the higher computational load from cryptographic operation is assign to the cloud supplier and the total statement cost is lowered for the mobile user. Furthermore, data re-encryption may be optionally complete by the cloud provider to reduce the expense of user revocation in a mobile user setting while preserving the privacy of user data store in the cloud. The proposed protocol has been realized on commercially accepted mobile and cloud platforms to reveal real-world benchmarks which show the efficiency of the scheme. A simulation regulated with the standard results shows the scalability potential of the scheme in the background of a classic workload in a mobile cloud computing system [5].

Lewko use a novel information-theoretic argument to adapt the dual system encryption method to the more complicated structure of ABE systems. The construct our system in complex orders bilinear groups, where the order is an item for consumption of three primes. They prove the privacy of their system from three static assumptions. ABE scheme supports random monotone access formula. Their second final is a fully secure predicate encryption (PE) scheme for inner formation predicates. As for ABE, previous construction of such scheme was only confirmed to be selectively secure. Security is proven under a non-interactive statement whose size does not depend on the digit of query. The scheme is comparably competent to existing selectively secure schemes and also there a fully secure hierarchical PE method under the similar assumption. The key technique used to get these results is a complex grouping of the dual system encryption method (adapted to the structure of inner produce PE systems) and a new move in the direction of on bilinear pairings using the idea of dual pairing vector spaces (DPVS) implement [7].

Kappes grow a new cryptosystem for fine-grained sharing of encrypted data so as to we call Key-Policy Attribute-Based Encryption (KPABE). In this crypto system, cipher texts are label with sets of attributes and secret keys are emotionally implicated with entrance structure that organize which cipher texts a user is able to decrypt. The current application of construction is to distribution of audit-log data and show encryption. Their construction chains designation of private keys which subsume Hierarchical Identity-Based Encryption (HIBE) [1].

Rikke Bendli presents Non-interactive receiver-deniable cryptosystem with healthier than polynomial safety. This also explains that it is not possible to make a non-interactive bi-deniable public-key encryption scheme with improved polynomial security. Specially, give an explicit bound relating the security of the scheme to how ancient the scheme is in terms of key size. Their impossibility result establishes a lower bound on the safety. As anal contribution gives constructions of deniable public-key encryption schemes which creates upper bounds on the protection in terms of key length. There is a break between our lower and upper bounds, which leaves the interesting undo problem offending the tight bounds [11**]**.

Paolo Gasti introduce the concept of deniable cloud storage that warranties privacy of data even when one's message and storage can be opened by an adversary. It shows that existing techniques and systems do not adequately explain this problem. This paper designs the first sender-and-receiver deniable public-key encryption method that is both reasonable and is construct from standard tools. Furthermore, we treat practical phase of user collaboration and provide an implementation of a deniable shared file system the original formulation of deniable encryption assumes that an opponent captures only message traffic. However, view as one of the most important uses of deniable encryption wherever encrypted contents are stored on a processor or a desktop computer and on a remote server also, and the adversary forces the owner of the machine to release its encrypted contents [10].

Ran Canetti proposed the Non-interactive proofs of well-for madness which were shown to underlie most previous constructions. Furthermore, applying our alteration to various recently-proposed

IBE schemes results in CCA-secure schemes whose exigency makes them moderately practical. This method extends to provide an easy and reasonably ancient method for securing any binary tree encryption (BTE) method against adaptive chosen-cipher text attacks. This, in turn, gives up more ancient CCA-secure hierarchical identity-based and forward-secure encryption schemes in the usual model [13].

Kaitai Liang to make data sharing be more powerfully, Proxy Re-Encryption (PRE) is proposed. Defined by Blaze, Bleumer and Strauss, PRE supports the designation of decryption rights. It allows a semi-trusted party called alternative to transform a cipher text proposed for Alice into another cipher text of the similar plaintext intended for Bob. The proxy, however, learns neither the decryption keys nor the original plaintext. PRE is applicable to many applications, such as secure distributed files systems and email forwarding. To date, PRE has been extended to adapt the context of ABE. Liang et al. proposed the earliest Cipher text- Policy Attribute-Based PRE (CP-ABPRE) scheme, in which a proxy is allowed to alter a cipher text under a particular access policy into the one under another access policy (i.e. attribute-based re-encryption). The proxy, however, find out nothing about the underlying plaintext. CP-ABPRE has many real world applications, such as fine-grained access control in cloud storage methods and medicinal records sharing among different hospitals. Previous CP-ABPRE schemes go away how to be secure beside Chosen-Cipher text Attacks (CCA) as an open problem. This paper, for the first time, proposes a new CP-ABPRE to begin the problem. The latest method supports attribute-based re-encryption with any monotonic contact structures. Despite our scheme is constructed in the random oracle model, it can be proved CCA secure below the decisional q-parallel bilinear Diffie-Hellman model assumption [12].

Markus Durmuth proposes the primary sender-deniable public key encryption system with a distinct encryption algorithm and negligible detection probability. It describe a generic interactive creation based on a public key bit encryption method that has definite properties, and offer two examples of encryption schemes with these assets, one based on the quadratic residuosity assumption and the other on trapdoor permutations[14].

III. PROBLEM STATEMENT

Most deniable public key schemes are bitwise, which defines these methods can only practice one bit a time; thus, bitwise deniable encryption schemes are ineffective for real use, especially in the cloud storage service. To solve this problem, this paper planned a hybrid encryption scheme that parallel applies symmetric and asymmetric encryption. They utilize a deniably encrypted plan-ahead symmetric data encryption key, while real data are encrypted through a symmetric key encryption method. Most deniable encryption schemes have decryption error troubles. These errors arrive from the designed decryption mechanisms. It uses the subset decision mechanism for decryption. The receiver finds out the decrypted message according to the subset decision answer. If the sender chooses an aspect from the worldwide set but unluckily the element is located in the specific subset, then mistake occurs. The same error takes place in all translucent set- based deniable encryption schemes.

IV. CONCLUSION

In this paper, current enabling data reliability proof and constancy services over multi cloud system using ABE which helps in informative violation as much as possible. The cloud reliability model and local auditing, global auditing that helps user to confirm the cloud service provider (CSP) provide the promised constancy or not and count the severity of the violations. Therefore system monitor consistency service model as well as level of data uploads which helps the user to get the data in updated version. User can recognize various sub servers in CSP. It is a considered to provide regular update mechanism to confirm fragments simply and provide the data to users after updating only.

V. REFERENCES

[1] 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.
[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.
[3] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography, 2011, pp. 53–70
[4] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in Crypto, 2012, pp. 199–217.
[5] P. K. Tysowski and M. A. Hasan, "Hybrid attribute- and reencryption- based key management for secure and scalable mobile applications in clouds." IEEE T. Cloud Computing, pp. 172–186, 2013.
[6] S. Rosenberger and B. Waters, "Attribute-based encryption with fast decryption," in Public Key Cryptography, 2013, pp. 162–179.
[7] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Eurocrypt, 2010, pp. 62–91.
[8] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. R`afols, "Attribute-based encryption schemes with constant-size ciphertexts," Theor. Comput. Sci., vol. 422, pp. 15–38, 2012.
[9] M. D¨urmuth and D. M. Freeman, "Deniable encryption with negligible detection probability: An interactive construction," in Eurocrypt, 2011, pp. 610–626
[10] P. Gasti, G. Ateniese, and M. Blanton, "Deniable cloud storage: sharing files via public-key deniability," in WPES, 2010, pp. 31–42.
[11] R. Bendlin, J. B. Nielsen, P. S. Nordholt, and C. Orlandi, "Lower and upper bounds for deniable public-key encryption," Cryptology ePrint Archive, Report 2011/046, 2011, http://eprint.iacr. org/.
[12] K. Liang, L. Fang, D. S. Wong, and W. Susilo, "A ciphertextpolicy attribute-based proxy re-encryption with chosen-ciphertext security," *IACR Cryptology ePrint Archive*, vol. 2013, p. 236, 2013.
[13] 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.
[14] M. D¨urmuth and D. M. Freeman, "Deniable encryption with negligible detection probability: An interactive construction," in *Eurocrypt*, 2011, pp. 610–626.