iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** III **Month of publication:** March 2017

DOI: http://doi.org/10.22214/ijraset.2017.3070

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

DeyPoS: Using Revocable Storage Identity-Based Encryption

Ashwini S Afre[1], Manisha Bharati[2]
[1]Student, [2]Professor , Department of Computer Engineering, Pune University

Abstract*: Dynamic Proof of Storage (PoS) is a useful cryptographic primitive that enables a user to check the integrity of outsourced files and to efficiently update the files in a cloud server. A practical multi-user cloud storage system needs the secure client-side cross-user deduplication technique, which allows a user to skip the uploading process and obtain the ownership of the files immediately, when other owners of the same files have uploaded them to the cloud server. Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. It is necessary to place cryptographically enhanced access control on the shared data. Identity-based encryption is a promising cryptographical primitive to build a practical data sharing system. Revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of cipher-text by introducing the functionalities of user revocation and cipher-text update simultaneously. Furthermore, we present a concrete construction of RS-IBE, and prove its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system.
Keywords: Cloud storage, dynamic proof of storage, deduplication, data sharing, revocation, Identity-based encryption, ciphertext update, decryption key exposure.

I. INTRODUCTION

Data integrity is one of the most important properties when a user outsources its files to cloud storage. Users should be convinced that the files stored in the server are not tampered. Traditional techniques for protecting data integrity, such as message authentication codes (MACs) and digital signatures, require users to download all the files from the cloud server for verification, which incurs a heavy communication cost. These techniques are not suitable for cloud storage services where users may check the integrity frequently, such as every hour. Thus, researchers introduced *Proof of Storage* (PoS) for checking the integrity without downloading files from the cloud server. Furthermore, users may also require several dynamic operations, such as modification, insertion, and deletion, to update their files, while maintaining the capability of PoS. Dynamic PoS is proposed for such dynamic operations. In contrast with PoS, dynamic PoS employs authenticated structures, such as the Merkle tree. Thus, when dynamic operations are executed, users regenerate tags (which are used for integrity checking, such as MACs and signatures) for the updated blocks only, instead of regenerating for all blocks. To better understand the following contents, they present more details about PoS and dynamic PoS.

While outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data. A natural solution to conquer the afore mentioned problem is to use cryptographically enforced access control such as identity-based encryption (IBE). Furthermore, to overcome the above security threats, such kind of identity-based access control placed on the shared data should meet the following security goals:

A. Data Confidentiality

Unauthorized users should be prevented from accessing the plaintext of the shared data stored in the cloud server. In addition, the cloud server, which is supposed to be honest but curious, should also be deterred from knowing plaintext of the shared data.

B. Backward Secrecy

Backward secrecy means that, when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the subsequently shared data that are still encrypted under his/her identity.

C. Forward Secrecy

Forward secrecy means that, when a user's authority is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her.

II. RELATED WORK

The objective of this literature review is to study the work carried and published by different researchers and authors in the domain of Document Annotation and tagging. Kun He, Jing Chen, Ruiying Du, Qianhong Wu, Guoliang Xue, and Xiang Zhang proposed in "DeyPoS: Deduplicatable Dynamic Proof of Storage for Multi-User Environments" the comprehensive requirements in multi-user cloud storage systems and introduced the model of deduplicatable dynamic PoS. They designed a novel tool called HAT which is an efficient authenticated structure. Based on HAT, proposed the first practical deduplicatable dynamic PoS scheme called DeyPoS and proved its security in the random oracle model.The theoretical and experimental results show that our DeyPoS implementationis efficient, especially when the file size and the number of the challenged blocks are large.[1]

Jianghong Wei, Wenfen Liu, Xuexian Hu proposed in paper "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption" proves cloud computing brings great convenience for people. Particularly, it perfectly matches the increased need of sharing data over the Internet. In this paper, to build a cost-effective and secure data sharing system in cloud computing, they proposed a notion called RS-IBE, which supports identity revocation and ciphertext update simultaneously such that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data. Furthermore, a concrete construction of RS-IBE is presented. [2]

Pietro and Sorniotti proposed in paper "Boosting Efficiency and Security in Proof of Ownership for Deduplication" proves another proof of ownership scheme which improves the efficiency. Xu et al.[4] proposed a client-side deduplication scheme for encrypted data, but the scheme employs a deterministic proof algorithm which indicates that every file has a deterministic short proof. Thus, anyone who obtains this proof can pass the verification without possessing the file locally. Other deduplication schemes for encrypted data were proposed for enhancing the security and efficiency. Note that, all existing techniques for cross-user deduplication on the client-side were designed for static files. Once the files are updated, the cloud server must regenerate the complete authenticated structures for these files, which causes heavy computation cost on the server-side. [3]

The concept of proof of storage was introduced by Ateniese et al. in paper "Provable data possession at untrusted stores", and Juels and Kaliski, respectively. The main idea of PoS is to randomly choose a few data blocks as the challenge. Then, the cloud server returns the challenged data blocks and their tags as the response. Since the data blocks and the tags can be combined via homomorphic functions, the communication costs are reduced. The subsequent works extended the research of PoS, but those works did not take dynamic operations into account. Erway et al. and later works focused on the dynamic data. Among them, the scheme in is the most efficient solution in practice. However, the scheme is stateful, which requires users to maintain some state information of their own files locally. Hence, it is not appropriate for a multiuser environment. Halevi et al. introduced the concept of proof of ownership which is a solution of cross-user deduplication on the client-side. It requires that the user can generate the Merkle tree without the help from the cloud server, which is a big challenge in dynamic PoS. [5]

Zheng and Xu proposed in paper "Secure and efficient proof of storage with deduplication" proves a solution called proof of storage with deduplication, which is the first attempt to design a PoS scheme with deduplication. Du et al. Introduced proofs of ownership and retrievability, which are like but more efficient in terms of computation cost. Note that neither can support dynamic operations. Due to the problem of structure diversity and private tag generation, cannot be extended to dynamic PoS. Wang et al. and Yuan and Yu considered proof of storage for multi-user updates, but those schemes focus on the problem of sharing files in a group. Deduplication in these scenarios is to deduplicate files among different groups. Unfortunately, these schemes cannot support deduplication due to structure diversity and private tag generation. In this paper, they consider a more general situation that every user has its own files separately. [6]

Jingwei Li, Jin Li, Dongqing Xie, and Zhang Cai "Secure Auditing and Deduplicating Data in cloud" proves both data integrity and deduplication in cloud, they propose SecCloud and SecCloud+. SecCloud introduces an auditing entity with maintenance of a MapReduce cloud, which helps clients generate data tags before uploading as well as audit the integrity of data having been stored in cloud. In addition, SecCloud enables secure deduplication through introducing a PoS protocol and preventing the leakage of side channel information in data deduplication. Compared with previous work, the computation by user in SecCloud is greatly reduced during the file uploading and auditing phases. SecCloud+ is an advanced construction motivated by the fact that customers always want to encrypt their data before uploading, and allows for integrity auditing and secure deduplication directly on encrypted data. Compared with previous work, the computation by user in SecCloud is greatly reduced during the file uploading and auditing phases.

SecCloud+ is designed motivated by the fact that customers always want to encrypt their data before uploading, and enables integrity auditing and secure deduplication on encrypted data. [7]

III. CONCLUSIONS

This survey is mainly focused on techniques and algorithm to suggest need of sharing data and avoid deduplication using cloud storage over the Internet. Using the concept of system and algorithm, it builds a cost-effective DeyPos for Multi-User Environments and secure data sharing system in cloud computing using RS-IBE, which supports identity revocation and cipher-text update simultaneously such that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data and it will help in preventing deduplication of shared information over cloud, which provides more feasible for practical applications.

IV. ACKNOWLEDGMENT

The authors would like to thank Indira Group of Institutions and the Director/Principal Dr. Sunil Ingole, colleagues from Computer Engineering and Indira College of Engineering and Management, Pune Dist. Pune Maharashtra, India, for their support, counsels and inspiration.

REFERENCES

[1] Kun He, Jing Chen, Ruiying Du, Qianhong Wu, Guoliang Xue, and Xiang Zhang, "DeyPoS: Deduplicatable Dynamic Proof of Storage for Multi-User Environments", DOI 10.1109/TC.2016.2560812, IEEE Transactions on Computers

[2] Jianghong Wei, Wenfen Liu, Xuexian Hu, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption", Journal Of Latex Class Files, Vol. 14, No. 8, August 2015

[3] R. Di Pietro and A. Sorniotti, "Boosting Efficiency and Security in Proof of Ownership for Deduplication," in Proc. of ASIACCS, pp. 81–90, 2012.

[4] J. Xu, E.-C. Chang, and J. Zhou, "Weak leakage-resilient clientside deduplication of encrypted data in cloud storage," in Proc. of ASIACCS, pp. 195–206, 2013.

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS, pp. 598–609, 2007.

[6] Q. Zheng and S. Xu, "Secure and efficient proof of storage with deduplication," in Proc. of CODASPY, pp. 1–12, 2012.

[7] Jingwei Li, Jin Li, Dongqing Xie, and Zhang Cai "Secure Auditing and Deduplicating Data in cloud", IEEE transaction on computers, vol. 65, no. 8, august 2016

[8] Jin Li, Xiaofeng Chen, Xinyi Huang, Shaohua Tang, Yang Xiang, Mohammad Mehedi Hassan, and Abdulhameed Alelaiwi "Secure Distributed Deduplication Systems with Improved Reliability", ", IEEE transaction on computers, vol. 64, no. 12, December s 2015

[9] Xinyi Huang, Joseph K. Liu, Shaohua Tang, Yang Xiang, Senior, Kaitai Liang, Li Xu, and Jianying Zhou "Cost-Effective Authentic and Anonymous Data Sharing with Forward security" IEEE transaction on computers, vol. 64, no. 4, april 2015

[10] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. of FC, pp. 136–149, 2010.

[11] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340–352, 2016.

[12] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Communications Surveys Tutorials, vol. 15, no. 2, pp. 843–859, 2013.

[13] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Proc. of ASIACRYPT, pp. 319–333, 2009.

[14] C. Erway, A. K¨upc ¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. of CCS, pp. 213–222, 2009.

[15] R. Tamassia, "Authenticated Data Structures," in Proc. of ESA, pp. 2–5, 2003.

[16] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS, pp. 355–370, 2009.

[17] F. Armknecht, J.-M. Bohli, G. O. Karame, Z. Liu, and C. A. Reuter, "Outsourced proofs of retrievability," in Proc. of CCS, pp. 831–843, 2014.

[18] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Journal of Cryptology, vol. 26, no. 3, pp. 442–483, 2013.

[19] Z. Mo, Y. Zhou, and S. Chen, "A dynamic proof of retrievability (PoR) scheme with o(logn) complexity," in Proc. of ICC, pp. 912– 916, 2012.

[20] E. Shi, E. Stefanov, and C. Papamanthou, "Practical dynamic proofs of retrievability," in Proc. of CCS, pp. 325–336, 2013.

[21] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[22] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563, 2012.

[23] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[24] G. Anthes, "Security in the cloud," Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010.

[25] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE

Volume 5 Issue III, March 2017
ISSN: 2321-9653

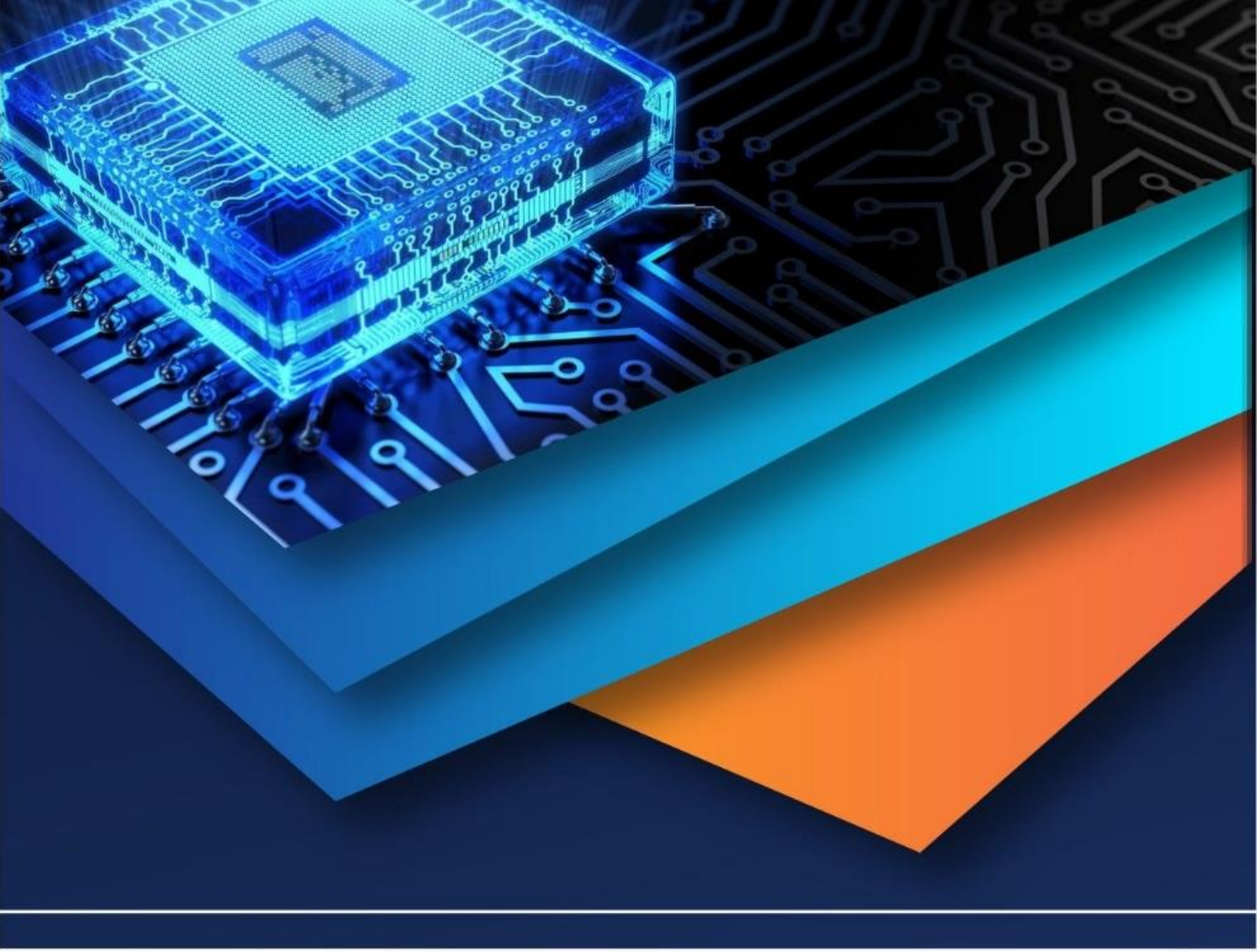
Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.

[26] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2904–2912.

[27] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.

[28] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," Computers, IEEE Transactions on, 2014, doi: 10.1109/TC.2014.2315619.

[29] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," Parallel and Distributed Systems, IEEE Transactions on



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY