ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 10, October 2018

A Survey on Novel Method for Delegatable Proofs of Storage to Prevent Data Leakage Based on AVL Tree

Rajashri Chandrakantrao Bhongale[1], Prof. Aarti D. K[2]

Department of Computer Engineering, Savitribai Phule University of Pune, JSPM COE, Hadapsar, Pune[1,2]

Abstract*:* Cloud computing is widely use in today's time which removes user's burden of local data storage. While providing storage it is important to provide security and integrity of the outsourced data. A Proof Of Storage (POS) is the main technique introduced to address this problem. Publically verifiable POS allows the third party to verify data integrity on behalf of the data owner which significantly improves the scalability of cloud service. There are existing publically verifiable POS schemes which are extremely slow to compute authentication tags for all data blocks. In this paper we are proposing a new variant called 'Delegable Proofs of Storage'. The tag generation process is speed up by at least several hundred times, without sacrificing efficiency in any other aspect. The propose scheme is extended to support fully dynamic operations with high efficiency. We are going to divide data files into blocks and going to use double encryption. Which will obviously provide more security to users data again we are going to divide our data into blocks and store it on different cloud server. So if attackers get access to data on one server, the remaining data will be secure

Keywords*:* AVL Tree, Proof of Storage, Delegable Proofs of Storage

I. INTRODUCTION

Cloud storage has been in widespread use nowadays, due to the great benefits that it brings into our life such as decreasing infrastructure costs, providing high scalability and availability. Ensuring the security and integrity of the outsourced data without keeping the local copy for data owners is an imperative concern to address. Solution to this problem is apply proof of storage in which integrity of the data stored in cloud server can be verified without having to download all the data. The basic idea is dividing the whole data file into multiple blocks, each of which is used to generate a Homomorphic Verifiable Tag (HVT) sent to cloud server together with the data file. The verifier selects a set of data blocks rather than the whole file to audit the outsourced data from the cloud server with the help of those HVTs, which can significantly reduce the communication overheads. Public verifiability of POS enables any third party to verify the integrity of data in cloud storage, which significantly eliminates the burden from data owner. POS scheme is supporting dynamic operations, in which data owners may request to modify, insert, or delete data blocks after outsourcing its original data to a cloud server. The cloud server will update the file blocks and the corresponding HVTs once it receives the update request from the data owner. The data owner could delegate the auditing task to some semi-trusted third party auditor, and this auditor is fully responsible to audit the data stored in cloud storage on behalf of the data owner, in a controlled way, with proper frequency.

To address the issues of existing publicly verifiable POS schemes, we propose a new variant formulation called Delegatable Proofs of Storage, which on one hand(DPOS) supports delegation of data auditing task, like publicly verifiable schemes, and on the other hand is as efficient POS as a privately verifiable scheme POS. To provide more security, we are going to divide the data files into blocks and going to use double encryption by using two algorithms Bastion and modified RSA algorithm, First we will encrypt the data using Bastion and cipher text will be re-encrypted using modified RSA algorithm. So that data will be more secure as dual encryption is given in proposed system. Once we get dual encrypted cipher text, it will be divided in blocks and theses blocks will be stored on different servers. As well as when key is generated it will also be divided in blocks to keep it safe from adversary, as he got the encryption key he will get only half key so that attack will not be taken place and data will not be disclosed and will be more secured. Proposed Bastion and modified RSA algorithm, a scheme which ensures the confidentiality of encrypted data even when the adversary has the encryption key, and all but re-encrypted cipher text blocks.

Bastion is most suitable for settings where the cipher text blocks are stored in multi-cloud storage systems and modified RSA generates long bit encryption key so that data should remain secure even the adversary tries to decrypt it. As well as encryption key will be divided and will be stored in the blocks for more security. To provide security and integrity of the user's data by dividing the file into blocks, these files are double encrypted and then uploaded to cloud server. We

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 10, October 2018

are going to generate keys to different blocks too which will provide more security to user's data. First we will encrypt the data using Bastion and cipher text will be re-encrypted using modified RSA algorithm. So that data will be more secure as dual encryption is given in proposed system. Once we get dual encrypted cipher text, it will be divided in blocks and theses blocks will be stored on different servers. As well as when key is generated it will also be divided in blocks to keep it safe from adversary, as he got the encryption key he will get only half key so that attack will not be taken place and data will not be disclosed and will be more secured. Proposed Bastion and modified RSA algorithm, a scheme which ensures the confidentiality of encrypted data even when the adversary has the encryption key, and all but re-encrypted cipher text blocks. Bastion is most suitable for settings where the cipher text blocks are stored in multi-cloud storage systems and modified RSA generates long bit encryption key so that data should remain secure even the adversary tries to decrypt it. As well as encryption key will be divided and will be stored in the blocks for more security. The proposed structure borrows the idea of tree AVL which is a binary search tree such that for each internal node v, the heights of its left sub-tree and right sub-tree differ by at most. Our goal is to manage the syntactic indices efficiently, so that whenever the data owner inserts deletes or modifies a data block of a file, the computation and storage overhead due to these updates should be minimized.

II. RELATED WORK

Clients who have limited storage resources or that desire to outsource the management of a data center distribute data to storage service providers (SSPs) that agree by contract to preserve the data and to keep it readily available for retrieval. Verifying the authenticity of stored data remotely on untrusted servers has emerged as a critical issue. It occurs in peer-to-peer storage systems network file systems, long-term archives, web-service object stores and database systems. Such systems control storage servers from misrepresenting or modifying data by providing authenticity checks when accessing data.

Archival of storage servers retain tremendous amounts of data, little of which is accessed. They also hold data for long periods of time, in which there may be exposure to data loss from administration errors as the physical implementation of storage evolves, backup and restore of system, data migration to new systems, and changing memberships in peer-to-peer systems [16]. Cloud Computing are not only limited to archive or backup data only. They have prior works on ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations. To support efficient handling of multiple auditing tasks they have used technique of bilinear aggregate signature to extend their main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously [17]. To deal with data storage outsourcing services, it is important to allow data owners to efficiently and securely verify that the storage server stores their data correctly [18]. Cloud storage provides services to users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Even though the benefits are clear, such a service is also relinquishing user's physical possession of their outsourced data, which inevitably poses new security risks toward the correctness of the data in cloud [19]. A new two-dimensional data structure which is, Dynamic hash table (DHT), located at a third parity auditor (TPA) to record the data property information for dynamic auditing [20].

III. PROOF OF STORAGE

This paper presents a proofs of storage that is cryptographic tool. In which data owner or third party auditor can check audit integrity of data stored remotely in a cloud storage server, without keeping a local copy of data or downloading data back during auditing[9].This paper presents a three-move interactive identification scheme in which it ensures the discrete logarithm problem. The scheme which is proposed in a paper is as secure as Schnorr identification scheme. We also propose practical digital signature schemes based on these identification schemes[12]. This paper proposes provable data possession model (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The clients maintain a constant amount of metadata to verify the proof [2]. To ensure the availability and durability of the user data in an untrusted storage system's many storage systems rely on replication which increases systems performance. MR-PDP scheme extends previous work on data possession proofs for a single copy of a file in a client/server storage system. This allows a client to query the distributed system to ensure that there are multiple unique copies of its file stored in the network even when storage sites collude [6]. Proofs of storage (PoS) are the protocols which allows a client to verify that a server faithfully stores a file. One problem associated is whether the server continually and faithfully storing the entire file entrusted to it by the client.

The server which we have considered is untrusted in terms of both security and reliability, it can maliciously or accidentally erase the data or can place that data into a temporarily unavailable storage media. This is done by the server intentionally for cost-saving or due to the external pressures. The server might also accidentally erase some data and choose not to notify the client [10].

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 10, October 2018

IV. PRIVACY PRESERVING IN CLOUD STORAGE

Using cloud storage users can access applications, services and software's whenever they want over internet. This the main concern about cloud storage in which integrity and privacy of data of user can arise. The users can make use of third party auditor to check integrity of the data which will remove the issue of giving public auditing process for cloud storage which can be used by the intended users. The multiple TPA are used for the auditing process which handles multiple users through batch auditing [18]. To ensure the integrity of data in cloud storage is the subject of skepticism and scrutiny, this is because the data stored in an untrusted cloud can easily be lost or corrupted; it may be due to hardware failures and human errors too. To enable each user in the group to easily modify data and share the latest version of data with the rest of the group, Oruta should also support dynamic operations on shared data [7]. With increasing number of clients the data stored on remote servers in the cloud, without storing a copy in their local computers. Sometimes the data which is stored on cloud is so important that the clients must ensure it is not lost or corrupted. It can be checked by downloading the data to be checked, but downloading such large amount of a data just for checking data integrity is totally the waste of communication bandwidth [20].In a cloud computing environment the data owners can host their data on cloud servers and users can access the data from cloud servers. An efficient and secure protocol which will ensure data owners about the data, that is the data is stored in the cloud correctly. It protects the data privacy against the auditor by combining the cryptography method with the bilinearity property of bilinear paring, rather than using the mask technique [21]. To use data storage outsourcing services, it is important to allow data owners to efficiently and securely verify that the storage server stores their data correctly. There are several Proof-Of-Retrievability (POR) schemes in which storage server must prove to a verifier that all of a client's data are stored correctly. While existing POR schemes offer decent solutions addressing various practical issues, they either have a non-trivial communication complexity, or only support private verification, i.e., only the data owner can verify the remotely stored data. It remains open to design a POR scheme that achieves both public verifiability and constant communication cost simultaneously [22].

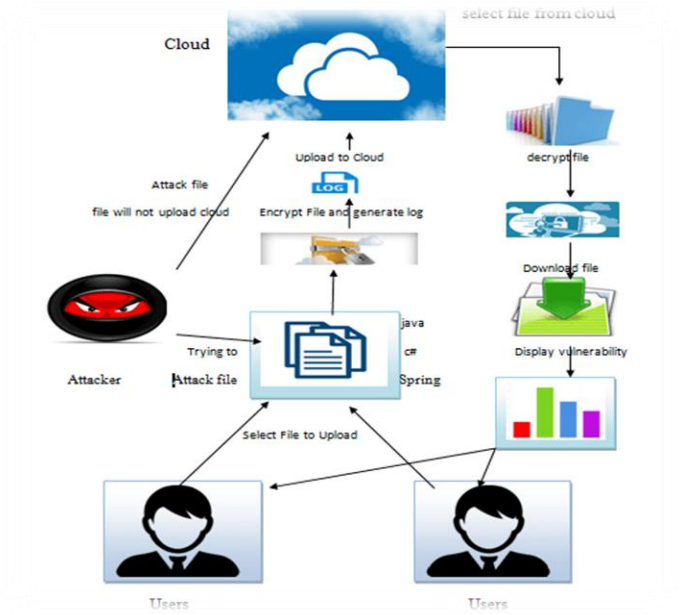

Fig. 1 System Overview

The system model consists of cloud, user and advisory. The authenticated user first interacts with the system, he selects the file that file will be encrypted using Bastion and ciphertext will be re-encrypted using modified RSA algorithm. So that data will be more secure as dual encryption is given in proposed system. Once we get dual encrypted ciphertext, it will be divided in blocks and theses blocks will be stored on different servers. As well as when key is generated it will also be divided in blocks to keep it safe from adversary, as he got the encryption key he will get only half key so that attack will not be taken place and data will not be disclosed and will be more secured. Proposed Bastion and modified RSA algorithm, a scheme which ensures the confidentiality of encrypted data even when the adversary has the encryption key, and all but re-encrypted cipher text blocks. Bastion is most suitable for settings where the cipher text blocks are stored in multi-cloud storage systems and modified RSA generates long bit encryption key so that data should remain secure even the adversary tries to decrypt it. As well as encryption key will be divided and will be stored in the blocks for more security. The proposed structure borrows the idea of tree AVL which is a binary search tree such that for each internal node v, the heights of its left sub-tree and right sub-tree differ by at most. our goal is to manage the syntactic indices efficiently, so that whenever the data owner inserts deletes or modifies a d block of a data file, the

computation and storage overhead due to these updates should be minimized. Once user gets the keys he can decrypt the file and download the original content of the file.

V. CONCLUSION AND FUTURE WORK

This paper proposes the problem of securing data outsourced to the cloud against an adversary which has access to the encryption key. For that purpose, we introduced a novel security definition that captures data confidentiality against the new adversary. We then proposed Bastion and modified RSA algorithm, a scheme which ensures the confidentiality of encrypted data even when the adversary has the encryption key, and all but re-encrypted cipher text blocks. Bastion is most suitable for settings where the cipher text blocks are stored in multi-cloud storage systems and modified RSA generates long bit encryption key so that data should remain secure even the adversary tries to decrypt it. As well as encryption key will be divided and will be stored in the blocks for more security. In these settings, the adversary would need to acquire the encryption key, and to compromise all servers, in order to recover any single block of plaintext.

ACKNOWLEDGEMENT

I profoundly grateful to **Prof. Aarti D. K.** for his/her expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion. I would like to express my deepest appreciation towards **Principal M. G. Jadhav, Prof. S. B. Chaudhari, HOD** department of computer engineering and PG coordinator **Prof. M. D. Ingale**. I must express my sincere heartfelt gratitude to all staff members of computer engineering department who helped me directly or indirectly during this course of work. Finally, I would like to thank my family and friends, for their precious support.

REFERENCES

[1]. A. Juels and J. Burton S. Kaliski, "PORs: Proofs of retrievability for large files," in Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2007, pp. 584–597, ACM, 2007.
[2]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2007, pp. 598–609, ACM.
[3]. H. Shacham and B. Waters, "Compact proofs of retrievability," in Advances in Cryptology - ASIACRYPT 2008, vol. 5350 of LNCS, pp. 90–107, Springer, 2008.
[4]. C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS 2009, pp. 213– 222, ACM, 2009.
[5]. C. C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," ACM Transactions on Information and System Security, vol. 17, pp. 15:1–15:29, April 2015.
[6]. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-replica provable data possession," in Proceedings of the 28th International Conference on Distributed Computing Systems, ICDCS 2008, pp. 411–420, IEEE, 2008.
[7]. B.Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in Proceedings of 5th International Conference on Cloud Computing, Cloud 2012, pp. 295–302, IEEE, 2012.
[8]. C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," IEEE Transactions on Computers, TC 2013, vol. 62, no. 2, pp. 362–375, 2013.
[9]. J. Xu, A. Yang, J. Zhou, and D. S. Wong, "Lightweight Delegatable proofs of storage," in Proceedings of 21st European Symposium on Research in Computer Security, ESORICS 2016, pp. 324–343, Springer International Publishing, 2016.
[10]. G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Advances in Cryptology -ASIACRYPT 2009, vol. 5912 of LNCS, pp. 319–333, Springer, 2009.
[11]. I. G. Aniket Kate, Gregory M. Zaverucha, "Constant-Size Commitments to Polynomials and Their Applications," in Advances in Cryptology - ASIACRYPT 2010, pp. 177–194.
[12]. T. Okamoto, "Provably secure and practical identification schemes and corresponding signature schemes," in CRYPTO '92: Annual International Cryptology Conference on Advances in Cryptology, pp. 31– 53.
[13]. J. Alwen, Y. Dodis, and D. Wichs, "Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model," in CRYPTO '09: Annual International Cryptology Conference on Advances in Cryptology, pp. 36–54, 2009.
[14]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song, "Remote data checking using provable data possession," ACM Transaction on Information and System Security, TISSEC 2011, vol. 14, no. 1, pp. 12:1–12:34, 2011.
[15]. H. Shacham and B. Waters, "Compact proofs of retrievability," Journal of Cryptology, JOC 2013, vol. 26, no. 3, pp. 442–483, 2013.
[16]. G., Burns, R., Curtmola, R., Herring, J., Khan, O., Kissner, L., Peterson, Z., and Song, "Remote Data Checking Using Provable Data Possession," ACM Trans. Info. Syst. Sec. 14, 1, Article 12
[17]. Qian Wang, Cong Wang, KuiRen,Wenjing Lou "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5, MAY 2011
[18]. Jiawei Yuan, Shucheng Yu, and Song, "Proofs of retrievability with Public Verifiability and Constant Communication Cost in Cloud," ACM Trans. May 8, 2013, Hangzhou, China.
[19]. Cong Wang, Qian Wang, KuiRen, Ning Cao, and Wenjing Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 5, NO. 2, APRIL-JUNE 2012
[20]. HuiTian, Yuxiang Chen, Chin-Chen Chang, "Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage," IEEE TRANSACTIONS ON SEVICE COMPUTING, MANUSCRIPT ID
Dan Boneh, Ben Lynn, and HovavShacham, "Short Signatures from the Weil Pairing," J. Cryptology (2004) 17: 297–319