ADVANCES in NATURAL and APPLIED SCIENCES

ISSN: 1995-0772
EISSN: 1998-1090
2016 Special 10(14): pages 118-121

Published BY AENSI Publication
http://www.aensiweb.com/ANAS
Open Access Journal

Privacy-Preserving Public Auditing For Data Storage Security In Cloud Computing

[1]B.Pavithra and [2]C.S. Anita

[1]M,E(CSE),R.M.D Engineering college,kavaraipettai, chennai-601206 TamilNadu
[2]Associate Professor of CSE Department,R.M.D Engineering college,kavaraipettai, chennai-601206 TamilNadu

Received 7 June 2016; Accepted 12 October 2016; Available 20 October 2016

Address For Correspondence:
C.S. Anita, Associate Professor of CSE Department, R.M.D Engineering college, kavaraipettai, chennai-601206 TamilNadu

ABSTRACT

In cloud computing to ensure data integrity on user uploaded data in multicolor maintaining security on cloud data and also provide dynamic reallocation of data at every access. The foundation of cloud computing lie in the outsourcing of computing task to the third-party. It entails the security risk in terms of confidentiality, integrity and availability of data and service. Cloud server allocates user files to verifier for data integrity checking. User privacy will be affected because of providing user file to verifier. User data always stored in static location of cloud server. In proposed model remote data integrity checking is required to secure users data in multicolor environment. Cloud server is managed by cloud service provider it has significant storage space and computation resource to maintain the clients data. Introducing the File allocation table (FAT) File System has proper indexing and metadata's (MD5) for the different chunks of the cloud storage and also gets data encoded using Base 64 Algorithm. Cloud provides random blocks to verifier for integrity checking which is to protect user privacy from third party. File recovery is done by the verifier automatically if the data gets corrupted during checking. At every access of the file by the user, blocks of the data will be dynamically reallocated between the cloud servers. This achieves access confidentiality in cloud computing.

KEYWORDS: Keyword 1 : Cloud computing Keyword 2 : data integrity Keyword 3 : public auditing
Keyword 4 : data confidentiality Keyword 5 : data recovery

INTRODUCTION

Cloud computing is a new computing paradigm connect to users elastically utilize a shared pool of cloud resources like processors, storages, applications, services are on-demand fashion applications. It takes the information to process service, such as storage, computing. It attracts more intention from the enterprises. The foundations of cloud computing lies in outsourcing tasks to the third party and so it entails the security risks in terms of confidentiality, integrity and availability with data and service. The issue to convince the cloud clients that their data are kept intact are especially vital in the clients does not store these data locally. Remote data integrity checking is a primitive to address this issue. When client stores his data on multicolor servers, distributed storage and integrity checking are indispensable. The integrity checking protocol should be efficient in order to make it suitable for capacity-limited end devices and it is based on distributed computation. In existing system remote data integrity checking is an important security problem in cloud computing. In PKI (Public Key Infrastructure), provable data possession protocol needs public key certificates, distributions and management. It meets with considerable overheads since the verifier checks certificates like the remote data integrity. In addition to the heavy certificate verification, the system suffers from the other complicated certificate management such as certificate generation, delivery, revocation, renewals. In cloud computing most verifiers only have low computation capacity. Cloud computing poses privacy concerns because the service provider can access the data that is in the cloud at any time. Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant. That is permitted in their privacy policies, which users must agree to before they start using cloud services. Solutions to privacy include policy and legislation as well as end users choices for how data is stored.

Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access. The content of this paper is organized as follows. In section 2 we review all related work. Section 3 will be proposed analysis and working principles section 4 will be conclusion.

2. Related Work:

Some techniques that are popularly used to ensure data integrity on user uploaded data in multicolor maintaining security on cloud data and also provide dynamic reallocation of data at every access. Ateniese introduces the scalable and efficient provable data possession on cloud computing. In this paper the main issue is how to frequently, efficiently and securely verify that a server is faithfully storing its clients outsourced data. The storage server is assumed to be entrusted in terms of both security and reliability. They construct a highly efficient and provably secure PDP technique based entirely on symmetric key cryptography, while not requiring any bulk encryption. PDP technique allows outsourcing of dynamic data, i.e., it efficiently supports operations, such as block modification, deletion, and append. The features of this scheme is very low cost and support for dynamic outsourced data make it attractive for realistic applications. Remote data integrity checking is an important security problem in cloud computing. The clients massive data is outside his control so the malicious cloud server may corrupt the clients data in order to gain more benefits. Many researchers have proposed the corresponding system model and security model. Ateniese [1] have proposed the provable data possession paradigm. In the PDP model the verifier can check remote data integrity with a high probability. Based on the RSA, they designed two provably secure PDP schemes. After they have proposed the dynamic PDP model and concrete scheme [2] and it does not support insert operation. [3] Erway has proposed a full dynamic PDP scheme based on the authenticated flip table and also the similar work has been done by the Sebe [4]. PDP have allows a verifier to verify the remote data integrity without retrieving or downloading the whole data. It is a Probabilistic proof of possession by sampling random set of blocks from the server and it can reduces the I/O cost. The verifier can maintain a small metadata to perform the integrity checking. PDP is an interesting remote data integrity checking model. In [5] Wang proposed the security model and concrete scheme of proxy PDP in public clouds. At the same time Zhu [6] have proposed the cooperative PDP in multicolor storage. Many remote data integrity checking models and protocols have been proposed [7],[8],[9],[10],[11],[12]. In this paper Haunt wang have focuses on distributed provable data possession in multicolor storage and it is based in identity-based public key cryptography. The protocol can be made efficient by eliminating the certificate management. They proposed the new remote data integrity checking model i.e. ID-DPDP. The system model and security model are formally proposed. Then based on the bilinear pairings, the concrete ID-DPDP protocol is designed. In the random oracle model, ID-DPDP is provably secure. On the other hand, the protocol is more flexible besides the high efficiency. Based on the client's authorization the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.

3. Proposed Analysis:

The proposed work considers remote data integrity checking is required to secure user's data in multicolor environment and the cloud provides random blocks to verifier for integrity checking which is to protect user privacy from the third party. File recovery is done by the verifier automatically if the data gets corrupted during checking. User cans complaint cloud for file recovery. At every access of the file by the user, blocks of the data will dynamically reallocated between the cloud servers. This achieves access confidentiality in cloud computing. In this analysis have four modules are:

- Admin configuration
- Data upload and block split
- Verifier integrity checking
- Automatic and on demand file recovery.

3.1 Architecture Diagram for Proposed System:

In Fig 1, the system architecture contains four entities i.e.,

1. Client
2. Cloud server
3. Attacker
4. Verifier

Client:

It is an entity , which has massive data to be stored on the multicolor for maintenance and computation, can be either individual consumer or corporation.

Cloud server:

It is an entity, which is managed by cloud service provider, has significant storage space and computation resource to maintain the client's data.

Attacker:

If attacker corrupts data in multicolor, the continuous auditing process helps the verifier to perform block level and file level checking.

Verifier:

It performs integrity checking on cloud data. Cloud allocates random combination of all the blocks to the verifier, instead of the whole file is retrieved during integrity checking. This is to protect user privacy from a third party. File recovery is done by the verifier.

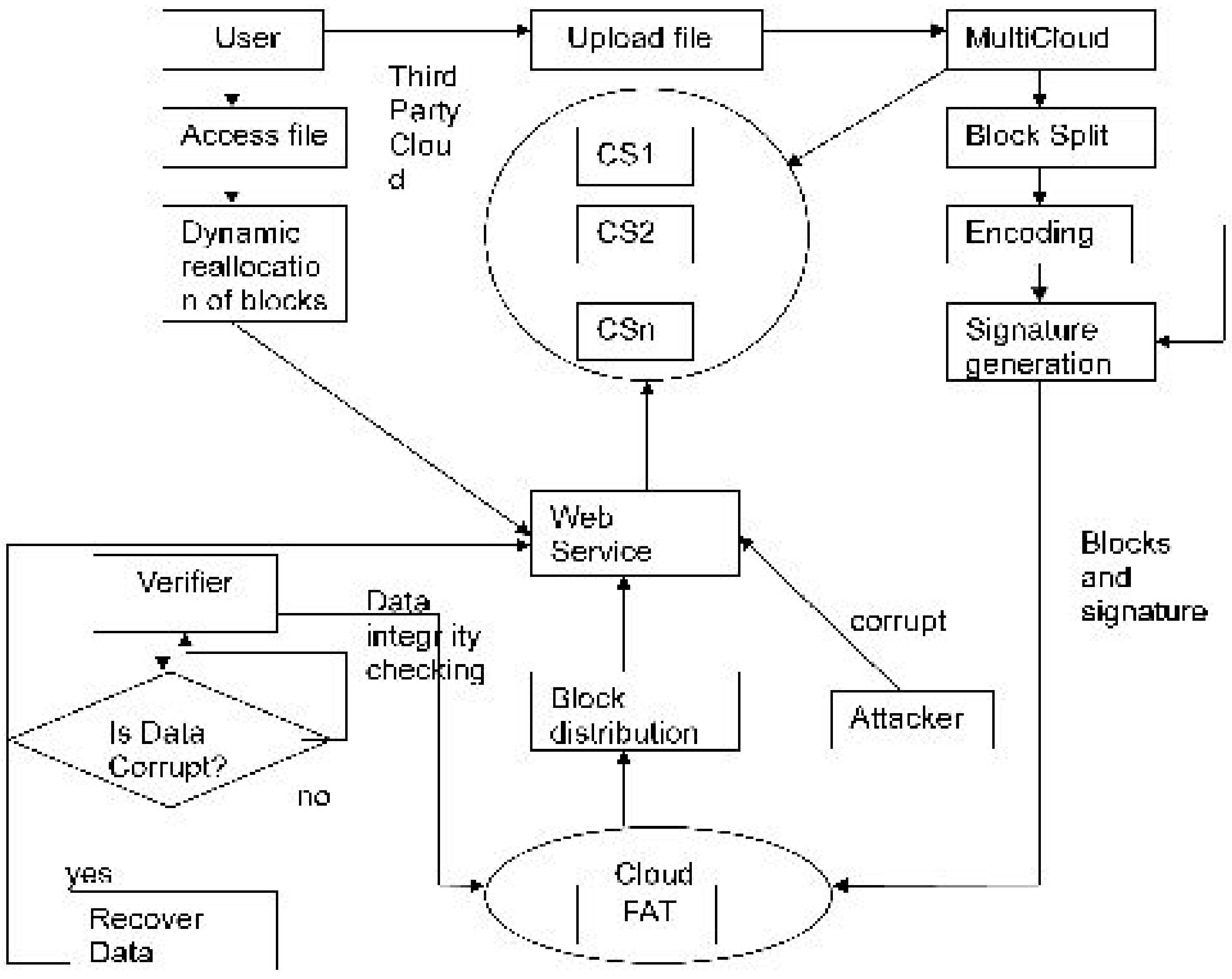

Fig. 1: System Architecture

3.2 Working Principles:

3.2.1 Admin configuration:

Admin **c**onfigure multicolor server setup. Server IP address and port number is given by the admin for each cloud. Now server architecture is created for multicolor storage. If the admin has to reconfigure the old multicolor server setup, it can be done. For old server setup, FAT file can be modified or remain same. Audit time will be set by the admin for data integrity checking process.

3.2.2 Data upload and block split:

User has an initial level registration process at the web end. The users provide their own personal information for this process. The server in turn stores the information in its database. After registration, user can upload files to the server. Uploaded files will be stored in a server. When the user upload the data to different cloud by the time it is spitted into different blocks using dynamic block generation method and each block will be appended with signatures before storing the data in FATFS. Signature generated using MD5 algorithm. Also the data gets encoded using for Base 64 algorithm.

3.2.3 Verifier Integrity checking:

FATFS has proper indexing and metadata's for the different chunks of the data that is being uploaded by user. Verifier performs remote integrity checking on cloud data. Cloud allocates random combination of all the blocks to the verifier, instead of the whole file is retrieved during integrity checking. This is to protect user privacy from a third party. Verifiable data integrity checking method is done in two steps i.e block checking and files checking. In block checking three signatures are generated.

1. A signature of a block retrieved from a FATFS.
2. A new signature is generated for block to be checked.
3. A signature is retrieved from the block appended with the signature which is stored in the cloud.

The above three signatures are cross checked for block level integrity checking and the block contents are appended to verify with file level integrity checking.

3.2.4 Automatic and on demand file recovery:

Attacker can corrupt data in any one of the clod servers. On data integrity checking done by the verifier, verifier informs corrupted blocks to the cloud. Recovery process will be done by the verifier automatically when data gets corrupted. User cans complaint to the cloud if the user file gets corrupted. Whenever user access file blocks will be reallocated dynamically to provide access confidentiality in cloud and FAT file system will get updated.

Conclusion:

Cloud computing is emerging technique which allows the user to have scalable data storage over cloud. Users outsource their files to the cloud server in an encrypted form so that unauthorized users do not able to read the actual content of the file. In such cases the privacy, access control are to be preserved and also it should be easy to retrieve the encrypted data stored in the cloud server. Our focus of this paper is to proposed a three algorithms and two techniques for data integrity checking and access confidentiality in multicolor storage. This scheme generates cloud provides random blocks to verifier for integrity checking which is to protect user privacy from third party. At every access of the file by the user, blocks of the data will be dynamically reallocated between the cloud servers. This achieves access confidentiality in cloud computing. The future enhancement of this paper is shuffle index can be used for dynamic reallocation of blocks.

The enhancement of this paper is to follows as

1. File recovery
2. Access confidentiality: Dynamic reallocation of blocks at every access.
3. Privacy preservation on public auditing.
4. Dynamic block split

REFERENCES

1. Ateniese, G., R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Petersonn and D. Song, 2007. “Provable data possession at untrusted stores”, in proc. CCS, pp: 598-609.
2. Ateniese, G., R. Dipietro, L.V. Mancini and G. Tsudik, 2008. “Scalable and efficient provable data possession,” in proc. SecureComm, pp: 1-10.
3. Erway, C.C., A. Kupcu, C. Papamanthou and R. Tamassia, 2009. “Dynamic provable data possession,” in proc. CCS, pp: 213-222.
4. Sebe, F., J. Domingo-Ferror, A. Martinez-Balleste, Y. Deswarte and J. Quisquater, 2008. “Efficient remote data integrity checking in critical information infrastructures,” IEEE Trans. Knowl.Data Eng., 20(8): 1034-1038.
5. Wang, H.Q. 2013. Proxy provable data possession in public clouds. IEEE Trans.Serv.Comput. [Online] 6(4): 551-559. Available: http:// doi.ieeecomputerssociety.org/10.1109/ TSC.2012.35
6. Zhu, Y., H. Hu, G.J. Ahn and M.Yu, 2012. “Cooperative provable data possession for integrity verification in multicloud storage”, IEEE Trans. Parallel Distrib. Syst., 23(12): 2231-2244.
7. Zhu, Y., H. Wang, Z.Hu, G.J. Ahn, H. Hu and S.S. Yau, 2010. “Efficient provable data possession for hybrid clouds,” in proc. CCS, pp: 756-758.
8. Curtmola, R., O. Khan, R. Burns and G. Ateniese, 2008. “MR-PDP: Multiple Replica Provable Data Possession,” in proc. ICDCS, pp: 411-420.
9. Barsoum, A.F. and M.A. Hasan, 2010. “Provable possession and replication of data over cloud servers,” Centre Appl. Cryptogr. Res., Univ. Waterloo, Waterloo, ON, Canada, Rep. 2010/32. [Online]. Available: http://www.cacr.math.uwaterloo.ca/techreports/2010/cacr2010-32.pdf
10. Hao, Z. and N. Yu, 2010.” A Multiple-Replica Remote Data Possession Checking Protocol with Public Verifiability,” in proc. 2nd Int.Symp.Data, Privacy, E-Comm., pp: 84-89.
11. Barsoum, A.F. and M.A. Hasan, 2011. “On verifying dynamic multiple data copies over cloud servers,” Int. Assoc. Cryptol. Res., New York, NY, USA, IACR eprint Rep. 447, 2011.[online]. Available:http:// eprint.iacr.org/2011/447.pdf
12. Juels, A. and B.S. Kaliski, Jr., 2007. “PORs:Proof of retrievability for large files ,” in proc. CCS, pp: 584-597.