ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Identity-Based Integrity Verification Using PDP in Multi Cloud Storage

P.Venkata Amarnath
M.Tech,
Dr.K.V.Subbareddy Institute of Technology,
Kurnool, Andhra Pradesh.

H.Ateeq Ahmed, M.Tech
Asst Prof,
Dept of CSE,
Dr.K.V.Subbareddy Institute of Technology,
Kurnool, Andhra Pradesh.

Abstract:

Identity-Based Provable data possession (PDP) is a technique for ensuring the integrity of data in storage outsourcing construction of an efficient scheme for distributed cloud storage to support the scalability of service and data migration, in which of multiple cloud service providers to cooperatively store and maintain the clients' data. Based on verifiable response and hash index hierarchy, we have proposed a cooperative PDP scheme to support dynamic scalability on multiple storage servers. According to zero knowledge interactive proof system having security with using RSA algorithm for data transfer.

Keywords:

Multi-cloud storage, Cooperative Provable Data Possession, Zero Knowledge Property, Hash Index Hierarchy, Homomorphic Verifiable Response.

I. INTRODUCTION:

Provable Data Possession (PDP) is one such scheme proposed in this scheme ensures that the data integrity is not lost. However, this scheme needs the users to download data for verification which causes security problem again. Therefore it is essential to have a scheme where data downloading is not required for verification. Towards this end PDP scheme such as Scalable PDP and Dynamic PDP came into existence. These schemes focused on single cloud storage providers. There are schemes like SPDP, DPDP and Merkle Hash Tree (MHT) make use of authenticated skip list in order to verify the adjacent blocks for integrity. These schemes do not work in multi-cloud environments as they can't construct MHT for such environment.

The other schemes such as CPOR and PDP make use of homomorphic verification tags where downloading data for verification is not required. To overcome the drawbacks of all existing methods, it is essential to build a cooperative PDP scheme that works in distributed multi-cloud environment. Data Leakage Attack and Tag Forgery Attack are the attacks to be prevented with new PDP scheme.

Multi cloud storage :

Distributed computing is used to refer to any large collaboration in which many individual personal computer owners allow some of their computer's processing time to be put at the service of a large problem. In our system the each cloud admin consist of data blocks.

The cloud user uploads the data into multi cloud. Cloud computing environment is constructed based on open architectures and interfaces; it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. We call such a distributed cloud environment as a multi-Cloud .A multi-cloud allows clients to easily access his/her resources remotely through interfaces.

Cooperative PDP :

Cooperative PDP (CPDP) schemes adopting zero-knowledge property and three-layered index hierarchy, respectively. In particular efficient method for selecting the optimal number of sectors in each block to minimize the computation costs ofclients and storage service providers. Cooperative PDP (CPDP) scheme without compromising data privacy based on modern cryptographic techniques

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Data Integrity :

Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.

Third Party Auditor :

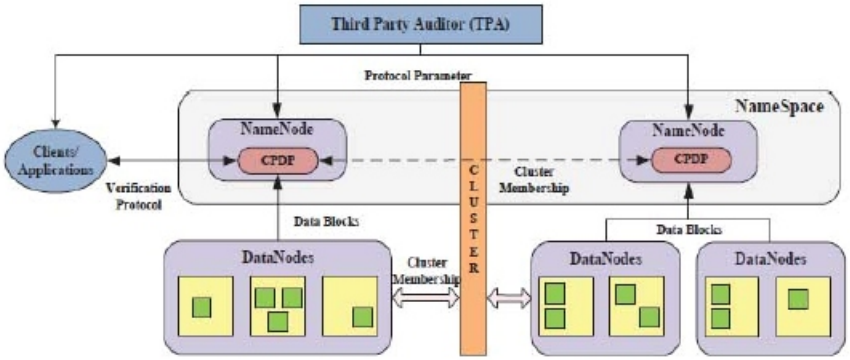
Trusted Third Party (TTP) who is trusted to store verification parameters and offer public query services for these parameters. In our system the Trusted Third Party, view the user data blocks and uploaded to the distributed cloud.

In distributed cloud environment each cloud has user data blocks. If any modification tried by cloud owner a alert is send to the Trusted Third Party.

Cloud User :

The Cloud User who has a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data. The User's Data is converted into data blocks. The data blocks are uploaded to the cloud. The TPA views the data blocks and Uploaded in multi cloud. The user can update the uploaded data. If the user wants to download their files, the data's in multi cloud is integrated and downloaded.

ARTHECHCTURE:



In this architecture, we consider the existence of multiple CSPs to cooperatively store and maintain the clients' data. Moreover, a cooperative PDP is used to verify the integrity and availability of their stored data in all CSPs. The verification procedure is described as follows: Firstly, a client (data owner) uses the secret key to pre-process a file which consists of a collection of blocks, generates a set of public verification information that is stored in TTP, transmits the file and some verification tags to CSPs, and may delete its local copy; Then, by using a verification protocol, the clients can issue a challenge for one CSP to check the integrity and availability of outsourced data with respect to public information stored in TTP. We neither assume that CSP is trust to guarantee the security of the stored data, nor assume that data owner has the ability to collect the evidence of the CSP's fault after errors have been found. To achieve this goal, a TTP server is constructed as a core trust base on the cloud for the sake of security.We assume the TTP is reliable and independent through the following functions :

to setup and maintain the CPDP cryptosystem; to generate and store data owner's public key; and to store the public parameters used to execute the verification protocol in the CPDP scheme. Note that the TTP is not directly involved in the CPDP scheme in order to reduce the complexity of cryptosystem.

II. MOTIVATION:

To provide security first PDP scheme is proposed but due to I/O burden on the cloud. Secondly SPDP scheme is proposed it removes the limitation of I/O burden of first scheme but this scheme is unsuitable for third party verification. Then DPDP scheme is proposed but it takes very large time in integrity verification.After then CPOR Scheme is proposed the Limitation of this work is a Lack of some security issues for large files Lastly CPDP scheme is proposed which removes all the flaws of all the scheme for integrity verification One of the most important and most attention issues, that is in the cloud environment, servers within the data storage

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

with security and integrity verification in this, we give an overview of our motivation in constructing CPDP. Our motivation is based on the following challenging questions that need to be addressed, which help us define our objectives in this paper.

III. CONTRIBUTION :

The main contributions of this work are summarized as follows:

1. We introduce a formal framework for provable data possession (PDP)

2. Then we provide the first efficient fully Scalable PDP solution

3. After we present a DPDP scheme with computation and communication.

4. We give an detailed construction of CPOR Scheme

5. Lastly we discuss all about our proposed Scheme which is nothing but the CPDP

HASH INDEX HIERARCHY FOR CPDP :

To support distributed cloud storage, we illustrate a representative architecture used in our cooperative PDP scheme as shown in Figure 2. Our architecture has a hierarchy structure which resembles a natural representation of file storage. This hierarchical structure H consists of three layers to represent relationships among all blocks for stored resources. They are described as follows:

1) Express Layer: offers an abstract representation of the stored resources;

2) Service Layer: offers and manages cloud storage services; and

3) Storage Layer: realizes data storage on many physical devices.

We make use of this simple hierarchy to organize data blocks from multiple CSP services into a large size file by shading their differences among these cloud storage systems.

The resources in Express Layer are split and stored into three CSPs that are indicated by different colors, in Service Layer. In turn, each CSP fragments and stores the assigned data into the storage servers in Storage Layer. We also make use of colors to distinguish different CSPs. Moreover, we follow the logical order of the data blocks to organize the Storage Layer. This architecture also provides special functions for data storage and management, e.g., there may exist overlaps among data blocks (as shown in dashed boxes) and discontinuous blocks but these functions may increase the complexity of storage management.

IV. SECURITY ANALYSIS:

We give a brief security analysis of our CPDP construction. This construction is directly derived from multi-prover zero- knowledge proof system (MPZKPS), which satisfies following properties for a given assertion,

1) Completeness: whenever €,there exists a strategy for the provers that convinces the verifier that this is the case;

2) Soundness: whenever not in€ , whatever strategy the provers employ, they will not convince the verifier that €

3) Zero-knowledge: no cheating verifier can learn anything other than the veracity of the statement. According to existing , these properties can protect our construction from various attacks, such as data leakage attack (privacy leakage), tag forgery attack (ownership cheating), etc. In details, the security of our scheme can be analyzed as follows:

Security of Public Key Schemes :

- Like private key schemes brute force exhaustive search attack is always theoretically possible
- But keys used are too large (>512bits)
- Security relies on a large enough difference in difficulty between easy (en/decrypt) and hard (cryptanalyse) problems
- More generally the hard problem is known, its just made too hard to do in practise
- Requires the use of very large numbers
- Hence is slow compared to private key schemes

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

RSA :

- By Rivest, Shamir &Adleman of MIT in 1977
- Best known & widely used public-key scheme
- RSA is a block cipher in which the plain text and cipher text are integers between 0 and n-1 for some n.
- n uses large integers (eg. 1024 bits / 309 decimal digits).

RSA Algorithm :

- Each user generates a public/private key pair by:
- Select two large primes at random - p, q
- Compute N=p.q
- Calculate ø(N)=(p-1)(q-1)
- Select at random the encryption key e
- where 1<e<ø(N), gcd(e,ø(N))=1
- Find decryption key d

-e.d=1 mod ø(N) -->

- Public encryption key: KU={e,N}
- Private decryption key: KR={d,N} or {d,p,q}

RSA Use:

- To encrypt a message M the sender:

-Obtains public key of recipient KU={e,N}

-Computes: C= where M<N

- To decrypt the ciphertext C the owner:

-Uses their private key KR={d,N}

-Computes: M=

- Note that the message M must be smaller than the modulus N (block if needed)

DESCRIPTION:

- C=
-
- Both sender and receiver must know the value of N.
- The sender knows the value of e,and the receiver knows the value of d.
- Thus Public key KU={e,N}.
- Private Key KR={d,N}

RSA EXAMPLE:

- Select primes: p=17 &q=11
- Compute n = pq=17×11=187
- Compute ø(n)=(p–1)(q-1)=16×10=160
- Select e : gcd(e,160)=1; choose e=7
- Determine d: de=1 mod 160 and d < 160 Value is d=23 since 23×7=161= 10×160+1
- Publish public key KU={7,187}
- Keep secret private key KR={23,17,11}

- Sample RSA encryption/decryption is:
- Given message M = 88 (nb. 88<187)
- Encryption:

C = 88 mod 187 = 11

88 mod 187= (88 mod 187 X 88 mod 187 X 88 mod 187) mod 187

- Decryption:

M = 11 mod 187 = 88

11 mod 187=(mod 187 X mod 187 X mod 187 X mod 187 X mod 187)

COMPUTATIONAL ASPECTS :

Encryption and Decryption :

- Both involve raising an integer to an integer power mod n
- Efficiency of exponentiation
- Algorithm for computing

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

V. CONCLUSION:

Our experiments clearly demonstrated that our approaches only introduce a small amount of computation and communication overheads. Therefore, our solution can be treated as a new candidate for data integrity verification in outsourcing data storage systems. As part of future work, we would extend our work to explore more effective CPDP constructions. Finally, it is still a challenging problem for the generation of tags with the length irrelevant to the size of data blocks. We would explore such a issue to provide the support of variable-length block verification. Scheme to support dynamic scalability on multiple storage servers. We also showed that our scheme provided all security properties required by zero knowledge interactive proof system, so that it can resist various attacks even if it is deployed as a public audit service in clouds by using this construction we are Deprecating all the limitation which is to be found in previously derived scheme

References :

1.Yan Zhu, Hongxin Hu, Gail-JoonAhn, Mengyang Yu, "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 12, DECEMBER 2012.

2.G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J. Peterson, and D.X. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp. 598-609, 2007.

3.A. Juels and B.S.K. Jr., "Pors: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, 2007.

4.H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), pp. 90-107, 2008.

5.G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Netowrks (SecureComm '08), pp. 1-10, 2008.

6.C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession", In CCS '09, pp. 213-222, April 24,2012.

7.Feifei Liu, DavuGu, HainingLu,"An Improved Dynamic Provable Data Possession", Proceedings of IEEE CCIS2011, pp 290-295, 2011.

8.Zhifeng Xiao and Yang Xiao, "Security and Privacy in Cloud Computing", The University of Alabama, Tuscaloosa, 24 March 2012.

9.Venkatesa Kumar V, Poornima G, "Ensuring Data Integrity in Cloud Computing", Journal of Computer Applications ISSN: 0974 – 1925, Volume-5, Issue EICA2012-4, February 10, 2012.

10.Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds," Proc. ACM Symp. Applied Computing, pp. 1550-1557, 2011.

11.Y. Zhu, H. Hu, G.-J. Ahn, Y. Han, and S. Chen, "Collaborative Integrity Verification in Hybrid Clouds," Proc. IEEE Conf. Seventh Int'l Conf. Collaborative Computing: Networking, Applications.

12.Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS '09), pp. 355-370, 2009.