RSA BASED CPDP WITH ENCHANCED CLUSTER FOR DISTRUBED CLOUD STORAGE SERVICES

[1]Z.Ismail, [2]K.Ashfaque Ahamed
[1]PG Scholar, Department of Computer Science, C.Abdul Hakeem College of Arts and Science, Melvisharam
[2]Assitant Professor, Department of Computer Science, C.Abdul Hakeem College of Arts and Science, Melvisharam
[1]Ashfaque184@gmail.com

Abstract: A cluster distributed cloud storage service should be presented with secured client data in indexed way. The execution level of complexity that is involved in bilinear mapping should be minimized. The cloud data storage presents an Enhanced RSA for the client's multiple integrity of data storage outsourcing is performed using provable data possession of the client. The existing works concentrate on the Cooperative Provable Data Possession (CPDP) mechanism for cloud storage in distributed way. The operation of CPDP is carried out using Homo-morphic Verifiable Response and Hash Index Hierarchy. The security of CPDP is determined by using multi-prover zero knowledge proof system. The performance optimization is to provide minimal Computation Complexity Communication Overhead. For cloud storage providers this technique proves the integrity and ownership of client's data essentially in case for large files and folders. The existing work presents a Cooperative Provable Data Possession (CPDP) mechanism for cloud storage services in distributed way by maximizing security and transparent verification in extraordinary performance. The CPDP operation is based on the techniques of hash index hierarchy (HIH) and Homo-morphic verifiable response (HVR). The first technique comprises of three layers and denotes the relationships between all blocks for stored resources. The Express Layer provides with the abstract representation of the stored resources. The second layer, service Layer manages cloud storage services and finally, the storage Layer realizes data storage on many physical devices. The second technique provides a map between two groups and provides with two messages that anyone can aggregate them into a value corresponding to the sum of the messages. It constructs the CPDP without compromising data privacy using interactive proof system (IPS). The analysis is made to prove that CPDP construction is a multi-prover zero-knowledge proof system (MP-ZKPS). The CPDP implement security against data leakage attack and tag the forgery attack. The probabilities queues are analyzed for detecting abnormal situations. It minimized the computation and communication overheads.

1. INTRODUCTION

Cloud Computing is the process of providing computer resources like hardware and software as a service on-demand. It also provides remote services with a user's data, software and computation.

Figure 1: Basic Cloud Model

2. SERVICE MODELS

2.1 Infrastructure as a Service (IaaS)

Iaas is a basic cloud service model where cloud providers offer computers as physical or as virtual machines. It also offers servers, storage, load balancers etc. It serves on a utility basis (i.e.) cost reflect the amount of resources allocated Cloud Providers: IBM Blue Cloud, Joyent, GoGrid, SunGrid, Amazon EC2

2.2 Platform as a Service (PaaS)

In PaaS model, cloud providers deliver a computing platform like operating system, database and web server. The resources here scale automatically to match demand and users not have to allocate resources manually.

- Platform as a Service: Google App Engine, Oracle SaaS Platform, MS Azure

- Data: Amazon S3, Google Base, Amazon SimpleDB, Microsoft SSDS

2.3 Software as a Service (SaaS)

In SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software. The cloud users do not manage the cloud infrastructure and platform on which the application is running. It provides features like elasticity, virtual desktop, emulator etc.

2.4 Cloud Clients:

Cloud clients are users who access this service model based on their need. They can access resource through web browser, mobile apps, thin client etc. The user can get the resource based on their need and are charged as per their usage.

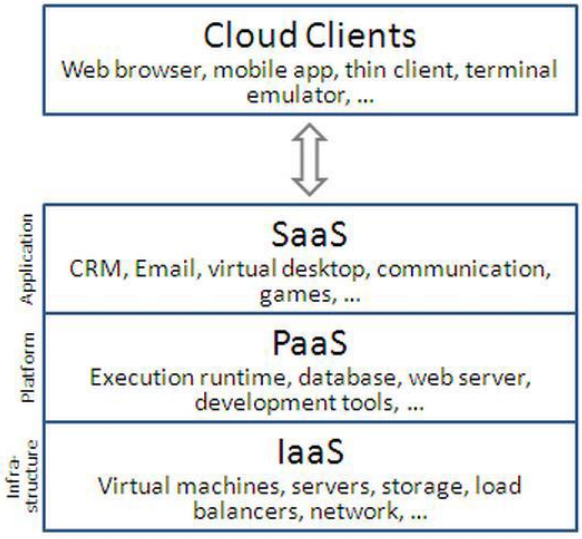


Figure 2: Cloud Service Model

3. CLOUD TYPES

3.1 Public cloud

A large organization owns the cloud infrastructure and sells cloud services to industries or public. Public cloud applications, storage, and other resources are made available to the general public by a service provider. These services are free or offered on a pay-per-use model.

3.2 Community cloud

Several organizations that have similar polices, objectives, aims and concerns share the cloud infrastructure. The common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally.

3.4 Hybrid cloud

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. It enables data and application probability

3.5 Private cloud

The cloud infrastructure is owned or leased by a single organization and is operated solely for that organization Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally.

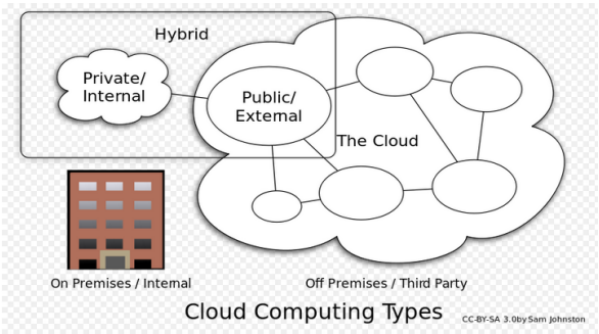


Figure 3: Cloud Types

4. CLOUD ARCHITECTURE

It is a systems architecture involved in the delivery of cloud computing, involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue. Elastic provision implies intelligence in the use of tight or loose coupling as applied to mechanisms such as these and others.

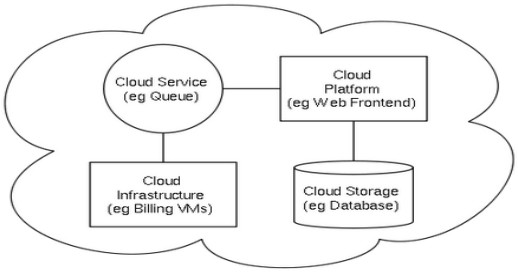


Figure 4: Cloud Architecture

5. OVERVIEW OF THE PROJECT

In cloud several users are shifting from networking to cloud paradigm due to its Minimum cost, Scalable operations and Independent platform. Clouds' Open architecture interface ensures highly interoperable varied cloud services operable both in internal or external environment, Makes clients to use the data in a remote mode with the help of interfaces or through web service. Multi-cloud is to build distributed cloud storage for client's data. Security attacks results in to provide security mechanisms for managing storage services.

6. EXISTING SYSTEM

Cooperative Provable Data Possession (CPDP) mechanism for cloud storage services in distributed way Maximizing security, transparent verification and extraordinary performance. CPDP operation based on techniques of Hash Index Hierarchy (HIH) and Homomorphic Verifiable Response (HVR).

6.1 Hash Index Hierarchical (HIH)

Hierarchical structure comprises of three layers. The Express Layer provides with the abstract representation of the stored resources. The second layer, service Layer manages cloud storage services. Finally, the storage Layer realizes data storage on many physical devices.

6.2 Homomorphic Verifiable Response (HVR)

A homomorphism provides a map between two groups. It provides with two messages anyone can aggregate them into a value corresponding to the sum of the messages.

6.3 Drawbacks

Evaluation of CPDP for large size files is affected by evolving bilinear mapping operations. Need to address issues about Integrate CPDP scheme with existing cloud storage provider systems and matching index hash hierarchy with HDFS's two layer name space. More concern related to CPDP is the production of tags with the length irrelevant to the size of data blocks. It provides support of Variable-length block verification.

7. PROBLEM DEFINITION

Provable data possession involves a technique related to probabilistic for cloud storage providers prove integrity and ownership of client's data. Ensures that the data is tampered with or deleted without downloading latest version of data. Most PDP schemes address scalability and dynamics of PDP, Compromised servers in single cloud storage provider.

8. PROPOSED SYSTEM

RSA based CPDP with enhanced cluster network for cloud storage services in distributed manner. RSA encryption is aggregated with CPDP group user's data possession for multiple cloud storage locations of the clients data. Enhanced clustered network are built to match the index structure of hash hierarchies of distributed cloud services.

Enhanced clustered network operations are based on adoptive parent tree hierarchy. Adoptive parent provide the advantage to support the cloud storage providers. Blanked child cloud services providers are supported by corresponding nearest hierarchy parent. Simulation is carried out with Cloud Simulator using java. Analyze and evaluate the performance of RSA based CPDP with enhanced cluster network scheme.

9. ADVANTAGE OF PROPOSED SYSTEM

Improve the compatibility of index structure with clustered networks. Minimize the bilinear Map Complexity. Increase data integrity rate. Better Scalability in terms of user quantification and file size.

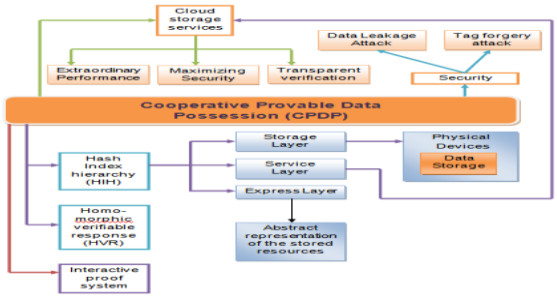


Figure 5: Architecture Diagram of Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage

10. MODULE DESCRIPTION

This project contains three modules. There are: Framework of Data Storage in Distributed Cloud. Index-Hash Table and Mapping of groups. Cooperative Provable Data Possessions.

10.1 Framework of Data Storage in Distributed Cloud

Framework of Distributed cloud data storage comprises of entities such as Clients, Cloud Service Providers and Trusted Third Party. Clients have large amount of data to be stored in multiple clouds and permissions to access and manipulate stored data.

Cloud Service Providers work together to provide data storage services and have enough storages and computation resources. Trusted Third Party trusted to store verification parameters and offer public query services for these parameters.

10.2 Index-Hash Table and Mapping of groups

Hash Index Hierarchical Structure of index hash table is similar to structure of file block allocation table in file systems. It Utilize hash function in PDPs. Hash hierarchical structure consists of three layers Express layer, Service layer and Storage layer.

HIH represent relationships among all blocks for stored resources. Provide simple index-hash table to record the changes of file blocks and generate the hash value of each block in the verification process. Index-hash table consists of serial number, block number, version number, and Random integer.

Homomorphic Verifiable Response integrates multiple responses from the different CSPs in CPDP scheme and Reduces communication bandwidth. Homomorphism is a map between two groups with Homomorphic Verifiable Tags (HVTs).

10.3 Cooperative Provable Data Possessions

CPDP scheme for multi-cloud system is constructed on collision-resistant hash bilinear map group aggregation algorithm, and homomorphic responses. Organizer initiates the protocol and sends a commitment to the verifier.

The organizer relays them into each cloud storage provider according to the exact position of each data block. Organizer synthesizes a final response from received responses and sends it to the verifier. The verifier accesses files without knowing on which CSPs or in what geographical locations their files reside.

11. CONCLUSION

The construction of an efficient PDP scheme for distributed cloud storage. Based on homomorphic verifiable response and hash index hierarchy, we have proposed a cooperative PDP 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.

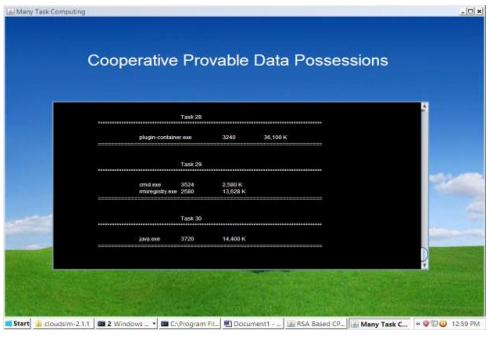
The probabilistic query and periodic verification to improve the audit performance. Our experiments clearly demonstrated that our approaches only introduce a small amount of computation and communication overheads. Therefore, our solution can be treated as a new candidate for data integrity verification in outsourcing data storage systems.

11. FUTURE ENCHANCEMENTS

To explore more effective CPDP constructions. Based upon the performance of CPDP scheme, especially for large files, is affected by the bilinear mapping operations due to its high complexity.

RSA based constructions may be a better choice, still this is a challenging task because the existing RSA based schemes have too many restrictions on the performance and security.

From a practical point of view, still need to address some issues about integrating our CPDP scheme smoothly with existing systems, for example, how to match index hash hierarchy with HDFS's two-layer name space, how to match index structure with cluster-network model, and how to dynamically update the CPDP parameters according to HDFS' specific requirements. Still this is a challenging problem for the generation of tags with the length irrelevant to the size of data blocks. Such an issue to provide the support of variable-length blocks verification.



REFERENCES

[1] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Senior Member, IEEE, Mengyang Yu "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage", IEEE Parallel and Distributed Systems. Vol. 12, no.3, pp. 11-25, 2012.

[2] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. T. Foster, "An Open Source Solution for Virtual Infrastructure Management in Private and Hybrid Clouds," IEEE Internet Computing, vol. 13, no. 5, pp. 14–22, 2009.

[3] 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," in ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 598–609.

[4] A. Juels and B. S. K. Jr., "PORs: Proofs of Retrievability for Large Files," in ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 584–597.

[5] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," in Proceedings of the 4th international conference on Security and privacy in communication networks, SecureComm, 2008, pp. 1–10.

[6] C. C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 213–222.

[7] Q. Wang, C.Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," in ESORICS, ser. Lecture Notes in Computer Science, M. Backes and P. Ning, Eds., vol. 5789. Springer, 2009, pp. 355–370.

[8] 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," in SAC, W. C. Chu, W. E. Wong, M. J. Palakal, and C.-C. Hung, Eds. ACM, 2011, pp. 1550–1557.

[9] K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability and integrity layer for cloud storage," in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 187–198.