DATA FILE DISTRIBUTION IMPLEMENTATION FOR MULTIPLE CLOUD SERVER WITH SECURE KEY GENERATION

Mahendra Gatwar
[1](Computer Science & Engineering , Takshshila Group of Institutes ,Jabalpur, India ,mahandra12@gmail.com)

Abstract—*In this paper, we develop an efficient auditing mechanism, which support batch auditing for multiple data files in multi-cloud environment. By utilizing the bilinear map, the proposed protocol achieves full stateless and transparent verification. By constructing a sequence-enforced Merkle Hash Tree, the proposed protocol can resist the re-place attack. In addition, our protocol protects the position information of the data blocks by generating fake data blocks to confuse the organizer. By compute intermediate values of the verification on cloud servers, our method can greatly reduce the computing overhead of the auditor. The performance analysis proves the good efficiency of the proposed protocol.*

Keywords—Cloud Computing;, Cloud Service Model; Bilinear Map; Hash Tree

1. INTRODUCTION

T Cloud computing was coined for what happens when applications and services are moved into the internet "cloud." Cloud computing is not something that suddenly appeared overnight; in some form it may trace back to a time when computer systems remotely time-shared computing resources and applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications .Cloud Computing is an evolutionary platform, has been served as a next generation infrastructure of the industry. It is a model which enables broad network access, resource pooling, and rapid elasticity. With the increasing demand of security the servers are not secure enough to meet user's demand. Hence the cloud platform is designed in such a manner so that it meets all the requirements of the user.

As per the definition provided by the National Institute for Standards and Technology [1](NIST) "cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

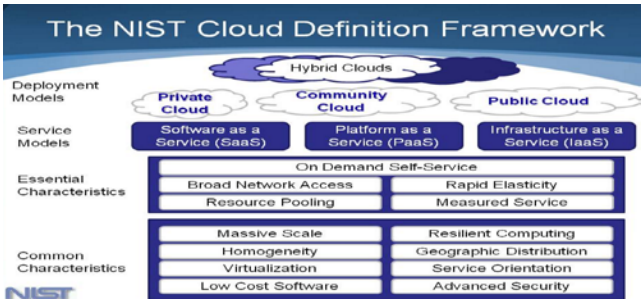

Figure 1.1 NIST Cloud Framework

2.CHARACTERISTICS OF CLOUD -

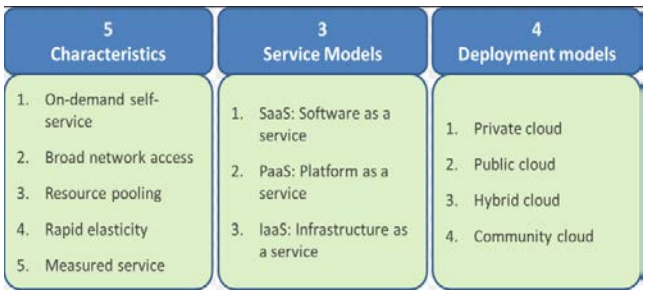

Figure 1.2 Characteristics of Cloud Computing

Infrastructure as a Service (IaaS) –

where the expert user implements their own software to optimize use of the computing facility. . At the base of the stack, Infrastructure-as-a-Service solutions deliver infrastructure on demand in the form of virtual hardware, storage, and networking. Virtual hardware is utilized to provide compute on demand in the form of virtual machine instances. These are created at users" request on the providers infrastructure, and users are given tools and interfaces to configure the software stack installed in the virtual machine.

Platform as a Service (PaaS)- where the client customizes their application to run inside the cloud management software. Platform-as-a-Service solutions are the next step in the stack. They deliver scalable and elastic runtime environments on demand and host the execution of applications. These services are backed by a core middleware platform that is responsible for creating the abstract environment where applications are deployed and executed.

Software as a Service (SaaS)- like Gmail, where the user simply uses the software provided. At the top of the stack, Software-as-a-Service solutions provide applications and services on demand. Most of the common functionalities of desktop applications—such as office automation, document management, photo editing, and

customer relationship management (CRM) software—are replicated on the providers infrastructure and made more scalable and accessible through a browser on demand.

Difference Between IaaS and PaaS-

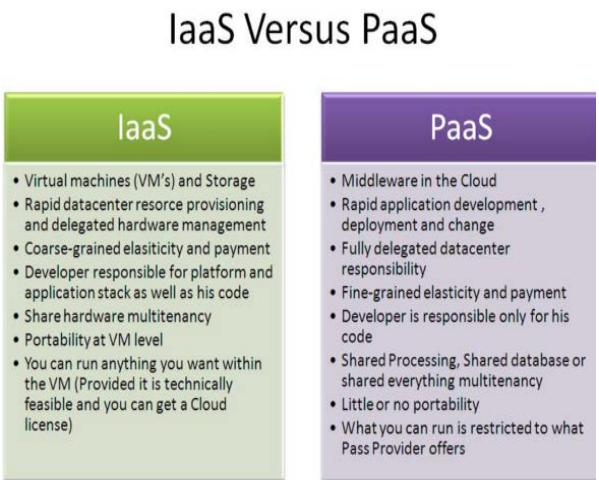

Figure 1.3 Difference Between IaaS and PaaS

3.LITERATURE ANALYSIS

Checking data possession in networked information systems such as those related to critical infrastructures (power facilities, airports, data vaults, defense systems, and so forth) is a matter of crucial importance. Remote data[2] possession checking protocols permit checking that a remote server can access an uncorrupted file in such a way that the verifier does not need to know beforehand the entire file that is being verified. Unfortunately, current protocols only allow a limited number of successive verifications or are impractical from the computational point of view. In this paper, we present a new remote data possession checking protocol such that 1) it allows an unlimited number of file integrity verifications and 2) its maximum running time can be chosen at set-up time and traded off against storage at the verifier. Storage [3] outsourcing is a rising trend which prompts a number of interesting security issues, many of which have been extensively investigated in the past. However, Provable Data Possession (PDP) is a topic that has only recently appeared in the research literature. The main issue is how to frequently, efficiently and securely verify that a storage server is faithfully storing its client's (potentially very large) outsourced data. The storage server is assumed to be untrusted in terms of both security and reliability. (In other words, it might maliciously or accidentally erase hosted data; it might also relegate it to slow or off-line storage.) The problem is exacerbated by the client being a small computing device with limited resources. Prior work has addressed this problem using either public key cryptography or requiring the client to outsource its data in encrypted form. In this paper, we construct a highly efficient and provably secure PDP technique based entirely on symmetric key cryptography, while not requiring any bulk encryption. Also, in contrast with its predecessors, our PDP technique allows outsourcing of dynamic data, i.e, it efficiently supports operations, such as block modification, deletion and append. Wang et al.propose a protocol for ensuring remote storage security in the environment of multiple servers, and Ateniese et al. [4] propose a framework that can build a public verifiable proof of storage system from any public key homomorphic linear authenticators. Hao and Yu [5] propose a remote data possession checking protocol for the multiple replica setting, which supports public verifiability and privacy against third party verifiers. The proposed protocol can be viewed as an adaptation of [6] to support more functionalities. It inherits the support of data dynamics from , and supports public verifiability and privacy against third-party verifiers, while at the same time it doesn't need to use a third-party auditor. On the other hand, Proof of Retrievability (PoR) [7] has been proposed as another technology for ensuring remote .

4.PROBLEM IDENTIFIED

PDP model and concrete scheme does not support insert operation.Handles only static data, thus handles only static files.Block modification not supported.Led to security loopholes.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. Proposed dynamic PDP model and concrete scheme although it does not support insert operation. In order to support the insert operation, in 2009, Erway et al. proposed a full-dynamic PDP scheme based on the authenticated flip table. The similar work has also been done by F. Seb´e et al. PDP 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, which drastically reduces I/O costs. The verifier only maintains small metadata to perform the integrity checking. PDP is an interesting remote data integrity checking model.

5.PROPOSED SOLUTION

In identity-based public key cryptography, this dissertation work we focuses on distributed provable data possession in multi-cloud storage. The protocol can be made efficient by eliminating the certificate management. We propose the new remote data integrity checking model: 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, our ID-DPDP protocol is provably secure. On the other hand, our 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.

- Identity-based public key cryptography focuses on distributed provable data possession in multi-cloud storage.
- The protocol can be made efficient by eliminating the certificate management.
- To propose the new remote data integrity checking model: ID-DPDP.
- The system model and security model are formally proposed.

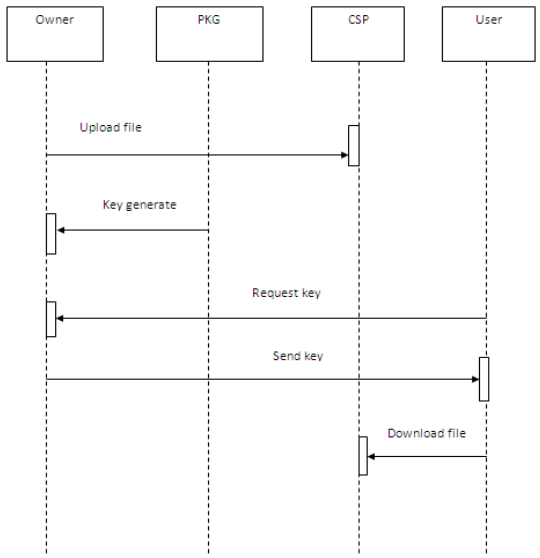

Figure1.4 Sequence Diagram

6.RESULT – IMPLEMENTATION SCREEN

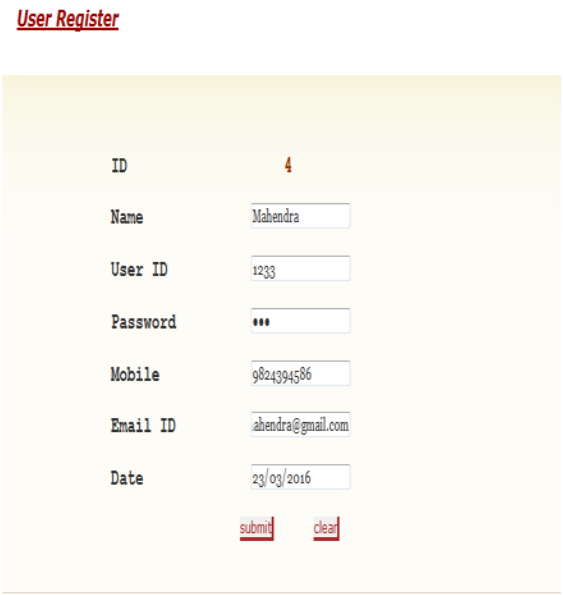

Figure1.5 User Registration

Figure 1.6 Operation Window of cloud User

7.CONCLUSION –

In multi-cloud storage, this paper formalizes the ID-DPDP system model and security model. At the same time, we propose the first ID-DPDP protocol which is provably secure under the assumption that the CDH problem is hard. Besides of the elimination of certificate management, our ID-DPDP protocol has also flexibility and high efficiency. At the same time, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification based on the client's authorization.

REFERENCES

[1] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] F. Sebe, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," Knowledge and Data Engineering, IEEE Transactions on, vol. 20, pp. 1034 –1038, aug. 2008.

[3] Scalable and Efficient Provable Data Possession Giuseppe Ateniese, Roberto Di Pietro, Luigi V. Mancini, and Gene Tsudik

[4] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in ASIACRYPT 2009, pp. 319–333, Springer Berlin / Heidelberg, 2009.

[5] Z. Hao and N. Yu, "A multiple-replica remote data possession checking protocol with public verifiability," in Data, Privacy, and E-Commerce, 2010. The Second International Symposium on, IEEE, September 2010.

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song, "Provable Data Possession at Untrusted Stores", CCS'07, pp. 598-609, 2007.

[7] A. Juels and B. S. Kaliski, Jr., "PORs: proofs of retrievability for large files," in CCS '07: Proceedings of the 14th ACM conference on Computer and communications security, (New York, NY, USA),pp. 584–597, ACM, 2007.