



Secure Encryption Key Generation Distribution File in Multiple Cloud Server

Mahendra Gatwar

Research Scholar M.Tech.
Takshshila Institute of Engineering & Technology
Jabalpur (M.P.), [INDIA]
Email: mahendra123@gmail.com

Abhishek Pandey

Assistant Professor
Department of Computer Science & Engineering
Takshshila Institute of Engineering & Technology
Jabalpur (M.P.), [INDIA]
Email: abhishekpandey@takshshila.org

Abstract—Cloud Computing is the environment where the client store their data in the cloud server and fetch a particular data from the cloud when they need some of the application in the cloud computing where the cloud user store information in the single cloud or in a multi- cloud servers. So in the current scenario cloud computing faces the problem of client verification. In the cloud storage, remote data integrity checking plays a vital role. This process can make the clients verification during the data fetching from the cloud or data loading to the cloud. For this process it must be necessary for cloud provider ICP to be in order to optimize the verifier's cost in terms of time and complexity. This is the major task in the cloud environment, so for solving this problem we propose a novel approach in cloud storage for the identity verification during the data distribution in the single cloud or multiple cloud servers. This dissertation work includes the strategies of client identity verification evidence certificate that is used in single cloud server and multiple cloud server. This proposed system is also able to provide good security for the cloud data. Proposed system is very efficient and flexible and is based on the cloud user authorization. This system includes private verification, public verification and delegated verification of cloud user in the optimized cost.

Keywords—Platform as a Service, Software as Service, Virtual Machine Cloud Computing, Cloud Domain, Cloud Environment.

1. INTRODUCTION

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.

Cloud Service Model

As in figure 1 showing cloud service model in this figure a cloud computing include the hybrid cloud, public cloud, private cloud and community cloud each have its unique working concept.

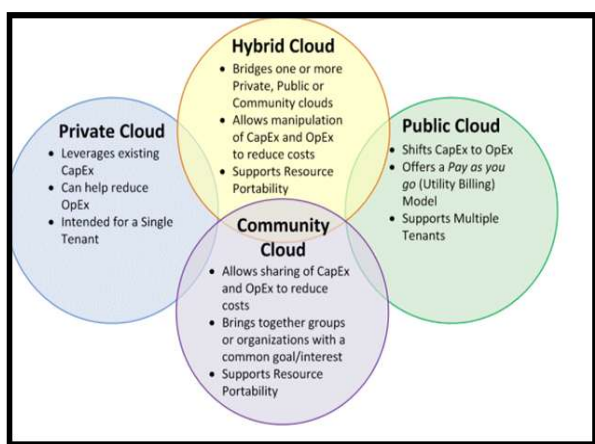


Figure 1 cloud service model [1]

Cloud Security Concerns

The Cloud different service models are IAAS, PAAS, SAAS and its deployment service models are Private, Public, Hybrid, and Community these all are face a number of security[2] issues/concerns with cloud computing but these issues fall due to : security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the on the cloud). The main responsibility goes both direction, it may be the cloud provider must ensure that their cloud environment is secure or not and that their user ' all the information and data are secure and ported when the user use it data and cloud application now here cloud client are make a very strong passwords and fulfill the all the authentication measures. When an the cloud manager or agencies selects to cloud

application that are already store in cloud data center store data user upload his her information at on the public cloud. It's output is very potentially sensitive and confidential data is at risk from some attacks. As a recent Cloud Security of the some attack is very major issue in cloud computing. Now the cloud service provider must ensure that all the background detail information. In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers often 33 store more than one customer's data on the same server. As a result there is a chance that one user's private data can by viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.[3].

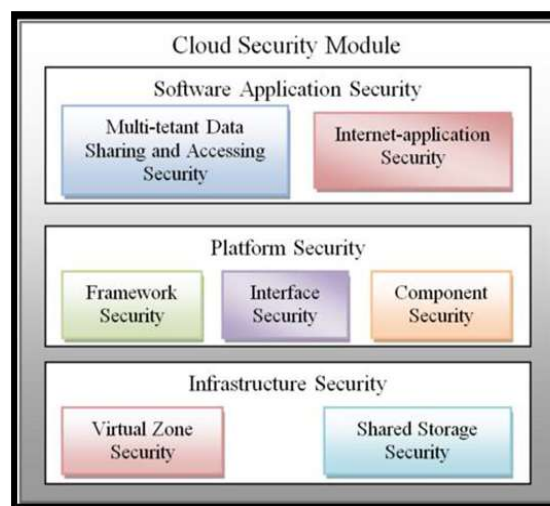


Figure 2 Cloud Security Model [3]

Cloud Storage

Cloud storage[9] means "the storage of data online in the cloud," wherein a company's data is stored in accessible from multiple distributed and connected resources that comprise a cloud. Cloud storage can provide the benefits of greater accessibility and reliability; rapid deployment; strong protection or data backup, archival and disaster recovery purposes; and lower overall storage costs as a result of not having to purchase, manage and maintain expensive hardware. However, cloud storage does have the potential for security and compliance concerns.

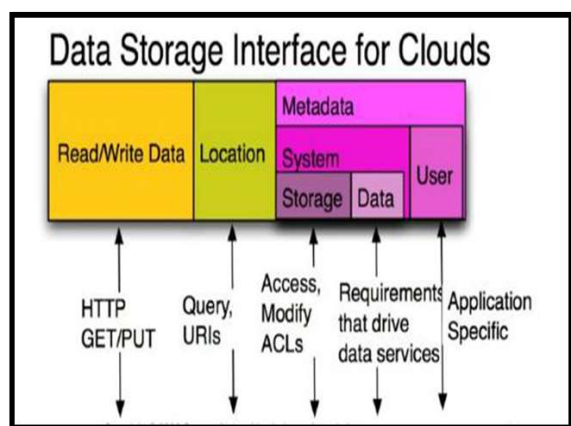


Figure 3 Data Storage in cloud [6]

2. LITERATURE SURVEY

In the PDP[4] model, the verifier can check remote data integrity with a high probability. Based on the RSA, they designed two provably secure PDP schemes. After that, Ateniese *et al.* proposed dynamic PDP model and concrete scheme [4] 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 [5][6]. 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. In 2012, Wang proposed the security model and concrete scheme of proxy PDP in public clouds [7] At the same time, Zhu *et al.* proposed the cooperative PDP in the multi-cloud storage [8]. In POR, the verifier can check the remote data integrity and retrieve the remote data at any time. The state of the art can be found in [9] On some cases, the client may delegate the remote data integrity checking task to the third party. It results in the third party auditing in cloud computing [10], [11], [12], [13] One of benefits of cloud storage is to enable universal data access with independent geographical locations. This implies that the end devices may be mobile and limited in computation and storage. Efficient integrity checking protocols are more suitable for cloud

clients equipped with mobile end devices. The problem of remote data integrity checking is first introduced in which independently propose RSA based methods for solving this problem. After that Shah *et al.* propose a remote storage auditing method based on pre-computed challenge-response pairs. Heitzmann *et al.* propose a data checking method with use of authenticated skip lists propose two provable data possession (S-PDP, E-PDP) schemes to provide integrity protection for remote data. The S-PDP and E-PDP support data block append operation, and a variant of their main PDP scheme has public verifiability. propose a remote data possession checking protocol for critical information infrastructures. Their protocol supports unlimited times of file integrity verifications and has a trade off between the running time and the storage cost at the verifier. Their protocol can be easily adapted to support data dynamics, but it doesn't support public verifiability. After that several studies, propose two efficient PDP constructions with data dynamics by using rank-based skip lists and RSA trees. Wang *et al.* propose a method which uses merkle hash tree to support fully data dynamics and uses BLS signature.

Table 2.1 Comparison of RSA, DES with some Methods

Methods	DES	RSA
Approach	Symmetric	Asymmetric
Encryption	Faster	Slow
Decryption	Faster	Slow
Key Distribution	Difficult	Easy
Security	Moderate	Highest
Secure Services	Confidentially	Confidentially, Integrity, Non-Repudiation

Some Method in Existing System 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.

3. PROPOSED SYSTEM

- 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.

4. OUTPUT SCREENS

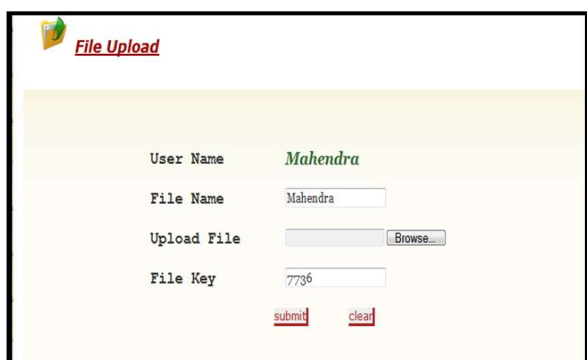


Figure 4. File Upload Screen

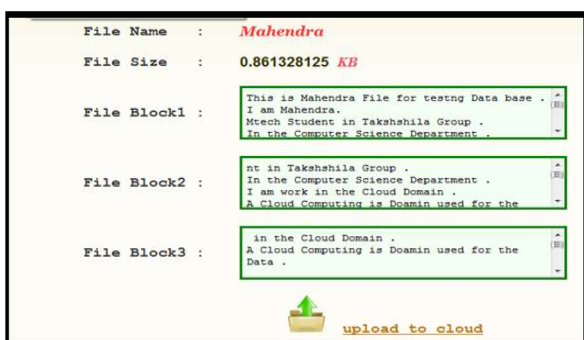


Figure 5. Cloud File Cluster

5. CONCLUSION AND FUTURE ENHANCEMENT

The work can be enhanced for security of data uploaded. As the cloud server is considered to be third party server, there could be possibility of attacker attack the server. So

in our enhancement work, the uploading data can be encrypted by using traditional encryption method and store in cloud server to avoid data leakage and data loss.

REFEREBCES:

- [1] <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- [2] <http://www.jisajournal.com/content/pdf/1869-0238-4-5.pdf>
- [3] G. Ateniese, R. DiPietro, L. V. Mancini, G. Tsudik, "Scalable and Efficient Provable Data Possession", Secure Comm 2008, 2008.
- [4] 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.
- [5] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, Dynamic Provable Data Possession, Proc. 16th ACM Conf. Computer and Comm. Security (CCS 09), 2009.
- [6] F. Seb'e, J. Domingo-Ferrer, A. Mart'inez-Ballest'e, Y. Deswarte, J. Quisquater, "Efficient Remote Data Integrity checking in Critical Information Infrastructures", IEEE Transactions on Knowledge and Data Engineering, 20(8), pp. 1-6, 2008.
- [7] H.Q. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, 2012. <http://doi.ieeecomputersociety.org/10.1109/TSC.2012.35>.
- [8] Y. Zhu, H. Hu, G.J. Ahn, M. Yu, "Cooperative Provable Data Possession for Integrity Verification

- in Multicloud Storage”, IEEE Transactions on Parallel and Distributed Systems, 23(12), pp. 2231-2244, 2012.
- [9] Y. Dodis, S. Vadhan, D. Wichs, “Proofs of Retrievability via Hardness Amplification”, TCC 2009, LNCS 5444, pp. 109-127, 2009.
- [10] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” in InfoCom2010, IEEE, March 2010.
- [11] Q. Wang, C. Wang, K. Ren, W. Lou, J. Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing”, IEEE Transactions on Parallel And Distributed Systems, 22(5), pp. 847-859, 2011.
- [12] C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, “Toward Secure and Dependable Storage Services in Cloud Computing,” IEEE Transactions on Services Computing, 5(2), pp. 220-232, 2012.
- [13] Y. Zhu, G.J. Ahn, H. Hu, S.S. Yau, H.G. An, S. Chen, “Dynamic Audit Services for Outsourced Storages in Clouds,” IEEE Transactions on Services Computing, 2011.