International Journal of Electrical Electronics & Computer Science Engineering
Volume 2, Issue 4 (August, 2015) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

A Secure Mechanism for Eliminating Redundancy in Hybrid Cloud Environment

M. Ranjith Raju[1], A. Shiva Kumar[2]
[1]Scholar, Computer Science, Tudi Ram Reddy Institute of Technology & Sciences, Hyderabad, Telangana, India
[2]Associate Professor, Computer Science, Tudi Ram Reddy Institute of Technology & Sciences, Hyderabad, Telangana, India
[1]ranjithraj539@gmail.com, [2]aluri.kumar@gmail.com

Abstract: ***Cloud computing has emerged to be a new computing model that serves the world with plethora of advantages. The services in cloud are offered in pay per use fashion. There are many cloud deployment models such as private cloud, public cloud, community cloud and hybrid cloud. Out of them hybrid cloud is the cloud that combines both private and public clouds. It does mean that a company's own cloud (private cloud) is integrated with public cloud. This has many benifits besides having high availability of resources. However, this model might throw challenges when data is duplicated multiple times. The process of removing redundant copies is known as dedeplication. This procedure has to be done in a secure environment. In this paper we build a framework that facilities a secure mechanism which eliminates redundancy in hybrid cloud environment. We built a prototype application to demonstrate that duplicate copies can be removed only by authorized users and the application reduces burden on cloud data centers. The proposed solution causes minimum overhead and enhances security of the system.***

Keywords: ***Deduplication, authorized duplicate check, confidentiality, hybrid cloud.***

I. INTRODUCTION

Cloud computing is a new computing paradigm which was conceived in 1960s became a reality now. This technology is able to commoditize computing resources as water and electricity are commoditized. This will enable individuals and small, medium and big enterprises to gain access to the computing resources provided by the Cloud Service Providers (CSPs) through Internet. The cloud resources and services can be obtained by users in pay per use fashion with the need for capital investment. Cloud has three important service layers namely Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). While these services are part of cloud, the cloud can have various deployment models such as private cloud, public cloud, community cloud and hybrid cloud. When people use public cloud, their data is stored in cloud servers remotely. Due to the bulk of data, users outsource the data to cloud and therefore need to relay on cloud for their data. This comes under IaaS. In the same fashion, all the three layers have opportunities and security challenges. The success of cloud computing largely depends on the solutions to security concerns of cloud users. This research focuses on the investigation into the three service layers of cloud in terms of opportunities and security challenges.

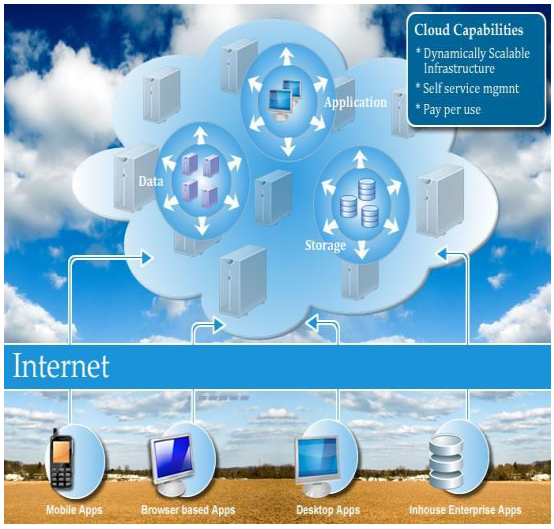

Figure 1. Cloud Computing Environment

As shown in Figure 1, it is evident that the computing resources are being accessed through Internet. There is dynamically scalable infrastructure that can be shared in pay as you use fashion.

In this paper our focus on handling duplicate data in hybrid cloud environment. We built a mechanism that can help in handling duplicates in secure fashion. Only authorized people can perform such activities. Our contribution in this paper is that we built a framework with underlying security mechanism to handle duplicate copies in hybrid cloud environment. The remainder of the paper is structured as follows. Section 2 provides review of literature. Section 3 presents the proposed system. Section 4 presents experimental results while section 5 concludes the paper.

II. RELATED WORKS

Cloud service architectures have been providing service architectures that are providing more security features. For instance, SaaS layer of cloud takes care of malware detection through scanning and filtering of content through cloud-based proxies. Some of the commercial cloud services are also offering enterprise level security configuration facilities that can prevent many security attacks including SQL injection. Third party management is the main concern in cloud security. Other security concern is the technical issues such as non-availability of

International Journal of Electrical Electronics & Computer Science Engineering
Volume 2, Issue 4 (August, 2015) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

encrypted communications. Other security issues are related to the architectural concerns where cloud depends on Internet and that dependence can have inherent security threats since Internet is untrusted network (Dorey and Leite, 2011). Cloud security challenges can be related to trust and assurance, data security and identity and access management. The risk of cloud service provider gaining access to sensitive information of client always exists. Cloud service providers can have access to software being deployed in cloud so as to provide software services in pay per use fashion. The float corporate architectures and possibility of social engineering are the other possible security issues in cloud computing (Dorey and Leite, 2011).

SaaS throws challenges with respect to testing. They include service function testing, regression testing, compatibility testing, performance testing, connectivity testing, and integration testing. In order to address all these challenges Gao *et al*. (2011) proposed a framework that can be integrated with cloud. The framework introduces a new service into the service stack of cloud. The name of the new stack is Testing as a Service (TaaS). In SaaS applications there are many security elements such as authentication and authorization, data access, data segregation, data integrity, data locality, network security, and data security (Subashini and Kavitha, 2011). The security for SaaS stack is as shown in Figure 2.

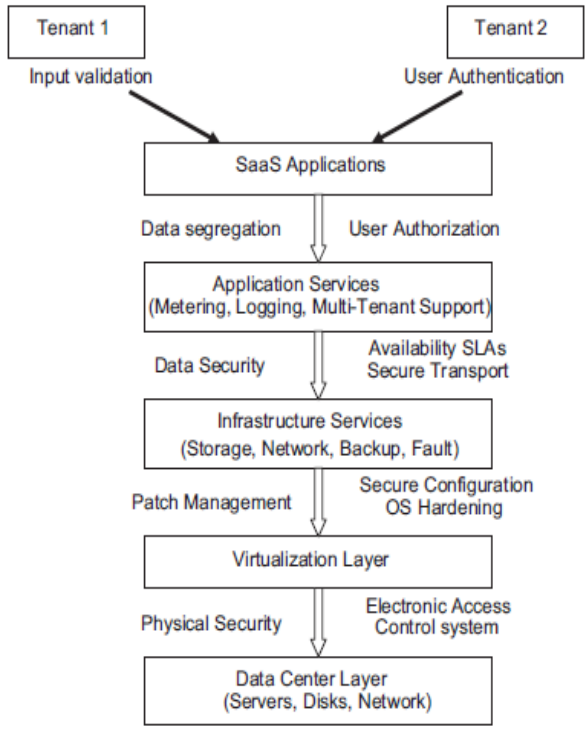

Figure 2. Security Stack of SaaS (Subashini and Kavitha, 2011)

There are different layers that need to support applications of SaaS layer. They include data center layer, virtualization layer, infrastructure services, and applications services. Both physical security and data security affects the SaaS applications (Subashini and Kavitha, 2011). There was research on the issue of duplicates as explored in [1]-[7].

III. PROPOSED SYSTEM

In this paper, we enhance our system in security. Specifically, we present an advanced scheme to support stronger security by encrypting the file with differential privilege keys. In this way, the users without corresponding privileges cannot perform the duplicate check. Furthermore, such unauthorized users cannot decrypt the cipher text even collude with the S-CSP. Security analysis demonstrates that our system is secure in terms of the definitions specified in the proposed security model.

IV. SALIENT FEATURES OF PROPOSED SYSTEM

The user is only allowed to perform the duplicate check for files marked with the corresponding privileges. We present an advanced scheme to support stronger security by encrypting the file with differential privilege keys. Reduce the storage size of the tags for integrity check. To enhance the security of deduplication and protect the data confidentiality

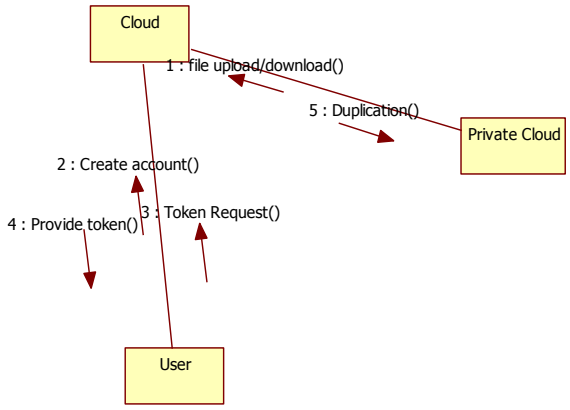

Figure 3. UML Modelling - Collaboration Diagram Reflecting User Operations

As seen in Figure 3, it is evident that all operations of user are shown. These operations are performed with user-friendly application that demonstrates the proof of concept. There is interaction among different parties such as user, private cloud and public cloud. Only authorized users can perform deduplication operations in secure environment.

International Journal of Electrical Electronics & Computer Science Engineering
Volume 2, Issue 4 (August, 2015) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

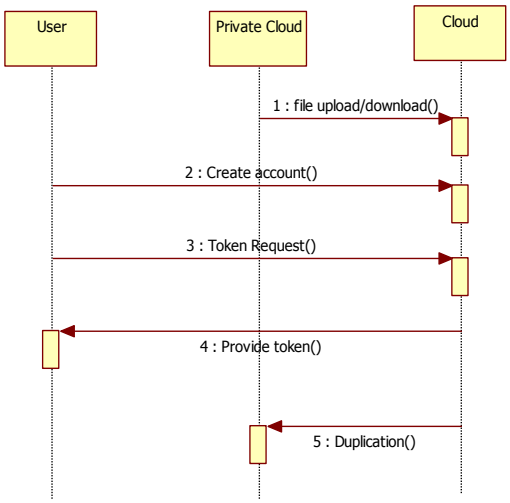

Figure 4. User Interactions with Cloud System

As seen in Figure 4, it is evident that all operations of user are shown. These operations are performed with user-friendly application that demonstrates the proof of concept. There is interaction among three objects such as user, private cloud and public cloud. Data can be outsourced to public cloud. User can access to data as per the privileges and also perform removal of duplicates in secure fashion.

V. IMPLEMENTATION

We implemented the proposed application using Java platform. The application is built with user interface that provides interaction with end users. Since the hybrid cloud contains private and public clouds, there is ever possibility of having duplicate data. We built simulation application that demonstrates the duplicates and help the users to eliminate them in secure fashion. Only the authenticated users can eliminate duplicates. The data when sent to cloud it is encrypted and when downloaded that is decrypted with secure key sharing approach.

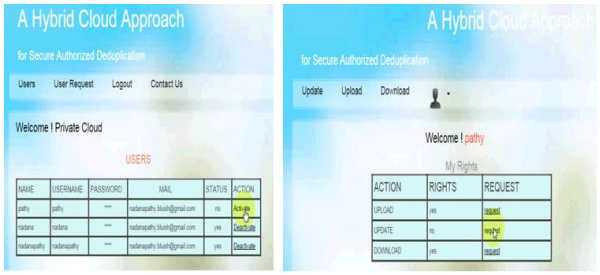

Figure 5. UI for Both Admin and User Roles

As can be seen in Figure 5, it is evident that all operations supported by the system for both administrator and user roles are presented. The prototype application can demonstrate the operations in secure and scalable fashion with underlying cloud database for computing resource rich environment. The users are able to perform intended operations and the data can be outsourced to public cloud. The data can be updated, uploaded and downloaded in the context of secure computations. Users can request for doing the intended operations as per the privileges they are entitled to.

Figure 6. Uploads and Downloads Pages

As can be seen in Figure 6, the database was built using cloud platform. The backend for Hybrid cloud system is the MY SQL database. The data is uploaded and downloaded to and from the cloud in secure fashion. Users need a key to decrypt the data that has been encrypted at the time of uploading the files into cloud. The users also are allowed to identify duplicates ad remove them. However, removal is possible when with due authentication. It does mean that users cannot perform any illegal operations. And only authorized users can perform intended operations subject to the privileges they have.

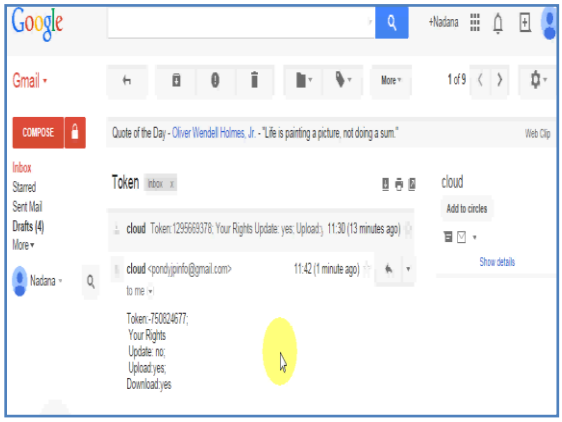

Figure 7. Token Generation Page

As can be seen in Figure 5, it is evident that the users can do intended operations after obtaining security key only. Along with the key the privileges are also mailed to users. With the mailed information, the users and perform the operations based on the rights. The token that came to mail is nothing but security key that can be used to perform operations.

International Journal of Electrical Electronics & Computer Science Engineering
Volume 2, Issue 4 (August, 2015) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

VI. EXPERIMENTAL RESULTS

Experiments are made using the proposed application. The experiments are made in terms of secure computations and also the secure handling of duplicates in hybrid cloud environment. Two experiments are made each one containing 100 runs to know the performance of the proposed system.

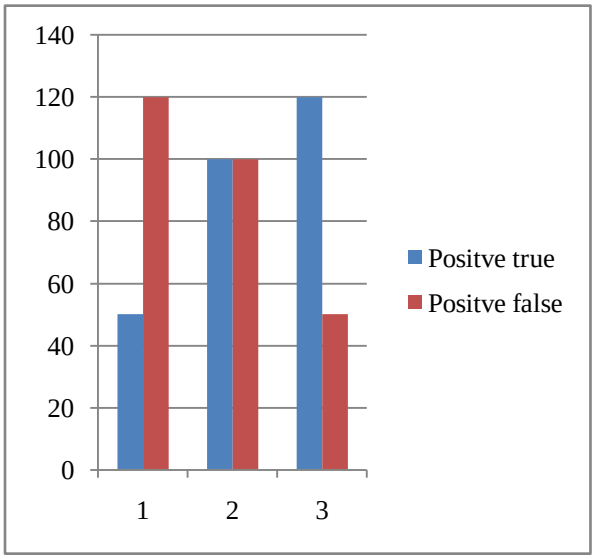

Figure 8. Experimental Results in Terms of Hybrid Cloud Approach

As can be seen in Figure 6, the proposed system is 100% secure and the same is revealed in the results. Out of 100 experiments, all experiments succeeded without security lapses.

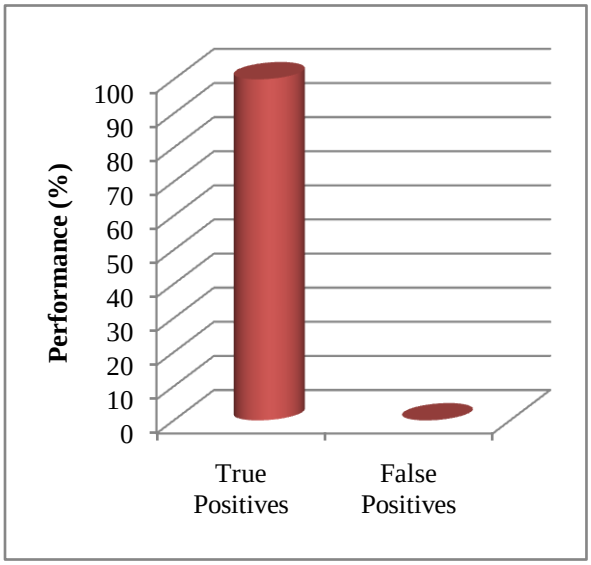

Figure 9. Experimental Results for Secure Handling of Duplicates

As can be seen in Figure 7, it is evident that out of 100 runs, duplicates are handled securely. There is no security breaches encountered while handling duplicates and only authorized users could perform this activity.

VII. CONCLUSIONS AND FUTURE WORK

In this paper we studied hybrid cloud environment where there is combination of private and public clouds. The hybrid could is prone to have duplicates of data being outsourced. The duplication has to be avoided. At the same time it is essential to have users with privileges and secure means of handling duplicates. Only authorized users can participate in secure communications. In the same fashion only authorized users are allowed to handle duplicates. Towards this end, we built a custom simulator using Java platform. The application contains simulated parties like user, private cloud and public cloud. The user is able to perform operations like accessing shared data based on the privileges. Users can also perform download operations that need key for decryption. Users who have privileges get the required key through a secure means in order to complete secure computations. At the same time users are allowed to handle duplicate data in order to optimize storage resources in hybrid cloud computing environment. We performed 100 experiments for secure computations and secure handling of duplicates each and the results revealed that the proposed solution is highly secure and can optimize cloud resources.

VIII. RFERENCES

[1] P. Anderson and L. Zhang. Fast and secure laptop backups with encrypted de-duplication. In Proc. of USENIX LISA, 2010.

[2] M. Bellare, S. Keelveedhi, and T. Ristenpart .Message- locked encryption and secure deduplication. In EUROCRYPT, pages 296–312, 2013.

[3] M. Bellare, S. Keelveedhi, and T. Ristenpart. Dupless: Serve raided encryption for deduplicated storage. In USENIX Security Symposium, 2013.

[4] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider. Twin clouds: An architecture for secure cloud computing. In Workshop on Cryptography and Security in Clouds (WCSC 2011), 2011.

[5] J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou. Secure deduplication with efficient and reliable convergent key management. In IEEE Transactions on Parallel and Distributed Systems, 2013.

[6] Bugiel, S., N¨urnberger, S., Sadeghi, A.-R., Schneider, T.: Twin Clouds: An architecture for secure cloud computing (Extended Abstract). In:

Workshop on Cryptography and Security in Clouds (WCSC 2011), March 15-16 (2011)

[7] Chung, K.-M., Kalai, Y., Vadhan, S.: Improved delegation of computation using fully homomorphism encryption. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 483–501. Springer, Heidelberg (2010)

[8] Cloud Security Alliance. Top threats to cloud computing, v. 1.0 (2010)