ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 3, March 2015

An Implementation of Secured Communication in Hybrid Cloud Model Using Public Key Infrastructure

Mr.B.Santhosh Kumar[1], Dr.Latha Parthiban[2]

Assistant Professor, Department Of CSE, G.Pulla Reddy Engineering College, Kurnool, India [1]

Assistant Professor, Department Of CSE, Community College, Pondicherry University, India [2]

Abstract: As Cloud Computing evolved it created an efficient way of pay per usage model for all the resources available on the network. In spite of its several advantages it has been suffering from the major drawback of providing secure communication. This paper makes an attempt to use Public Key Infrastructure (PKI) and provide secure way of communication among different branches of an organization. Each organization is implemented as a private cloud and the central branch usually where the CEO of the organization works to whom each branch needs to report is implemented as a public cloud together giving a hybrid cloud infrastructure.

Keywords: Public Key Infrastructure (PKI), Security, Hybrid Cloud.

I. INTRODUCTION

In the early days the major source of communication in an organization was through postal manner. As technology grown rapidly people used to make use of fax, internet to exchange information. Today technology led to a new advancement of implementing and using the resources as per the time they have been used. This led to a concept of cloud architecture. The major services offered by a cloud can be categorized as follows:

1. **Software as a Service (SAAS):** This service mainly aims in delivering the software to the users. The software developed is deployed on the service provider's architecture and the user is charged according to the usage of the software. Ex: Gmail, face book.
2. **Platform as a Service (PAAS):** This layer provides all the necessary software used for developing the application. The concepts of virtualization, load balancing are mainly implemented in these services. Ex: VMware, Google App Engine, Microsoft Windows Azure.
3. **Infrastructure as a Service (IAAS):** The servers and databases required for the application are implemented using Infrastructure services. Ex: Google Compute Engine, Amazon EC2.

The services provided by the cloud have to be deployed for use. The deployment models of the cloud can be classified as follows:

1. **Private Cloud:** This architecture is mainly used for a particular company or organization for their maintenance. If the data has to be maintained internally without any outside interactions then this deployment model will be well suitable.
2. **Public Cloud:** This deployment model allows all the services to be utilized by any of the users in the network. If the data has to be catered to a large percentage of users then this model can be employed.
3. **Hybrid Cloud:** This is a combination of at least one private cloud and one public cloud. The architecture of the hybrid cloud can be depicted as follows:

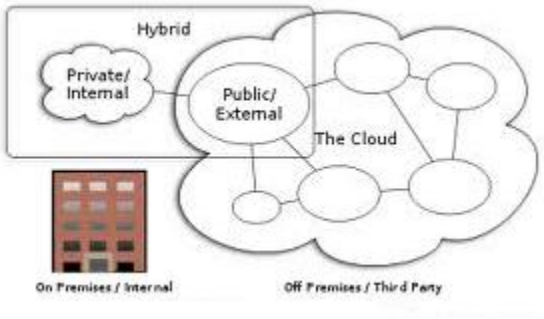

Figure 1[11]: Hybrid cloud architecture

The core portion of this paper is mainly implemented using hybrid cloud architecture. Each branch of the organization is implemented using private cloud and all of them will be posting the data to a centralized branch which can be the head quarters of the organization where the CEO of the company wants the data related to each branch. By this implementation all the branches can also exchange information as well as they can communicate securely without the data being tampered by external sources.

Further the paper is organized as follows. Section II will discuss the related work that led to the idea behind this paper. Section III will discuss the proposed work in which the organizations can exchange the data in a secure manner. Section IV gives an analysis of the performance of the proposed model. Section V concludes the paper and gives the future enhancements that can be done to extend the proposed architecture.

II. RELATED WORK

The proposed work is mainly based on the concept which is implemented in [2] where the concept of storage service provider has been introduced which gives a provision to the users to submit data even they are offline. . The works in [3], [4] and [5] mainly concentrates on providing efficient access to the outsourced data. The encryption

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 3, March 2015

techniques which led to the current work have been improvised from the works done in [6] and [7].
The secured distributed storage architecture has been enhanced from the works done in [8] and [9] where the work related to distributed file systems have been discussed extensively. The data sharing architecture has been derived from [10] where a platform was proposed for sharing the data in outsourced enterprise storage environments.

III. PROPOSED WORK

It is assumed that public key infrastructure is established in private organization cloud and public organization cloud and both Certificate Authorities (CA) have issued certificates. All the assumptions which have been made in research paper [2] are also extended to this model.
The proposed architecture can be pictographically represented as in figure 2.The steps followed for secure communication can be described as follows:
The process in private organization of a cloud takes place as follows:

1. The employees (EMP) who are the authorized persons appointed by the managers of the organization (MGR) will encrypt the data to be sent using secret keys Ke_1, Ke_2.....Ke_n As $C_{emp} = E(K_{ei}(data))$. The secret keys are distributed between employees and managers of the organization in secure manner.
2. The Access Control Matrix (ACM) and digital signature for the data will be created by the employees and will be forwarded to Storage Service Provider (SSP).
3. If the managers (MGR) want to verify the data they provide their certificates $CERT_{authi}$ to the SSP which in turn verifies the certificates and checks the ACM for authorization.
Then the data is sent as follows:
4. The SSP creates a random session key K_{sp} and again does the encryption of C_{emp} as

$C_{emp} = E(K_{sp}(C_{emp})) = E(K_{sp}(E(Ke_i(data))))$.The secret key can also be encrypted as $C_{Ksp} = E(K_{pmgr}(K_{sp}))$ where K_{pmgr} is public key of manager of the organization.
5. When both the encrypted data and key is sent to the manager (MGR) the key K_{sp} is got back using his private key and the data is decrypted with $K_{ei}$to get back the data sent by the corresponding employee (EMP) of the organization.
6. Then the manager (MGR) scrutinizes the data and in case of any discrepancies the data will be sent back to the corresponding employee (EMP) who does the necessary changes and returns the data back to the manager (MGR).

The manager (MGR) is responsible for submitting the data to the Chief Executive Officer (CEO) of the company but he gets the work done through the employees of the organization.

After the manager (MGR) verifies the data and found it to be genuine he submits the data to the public organization cloud in the steps mentioned from 7 through 12.

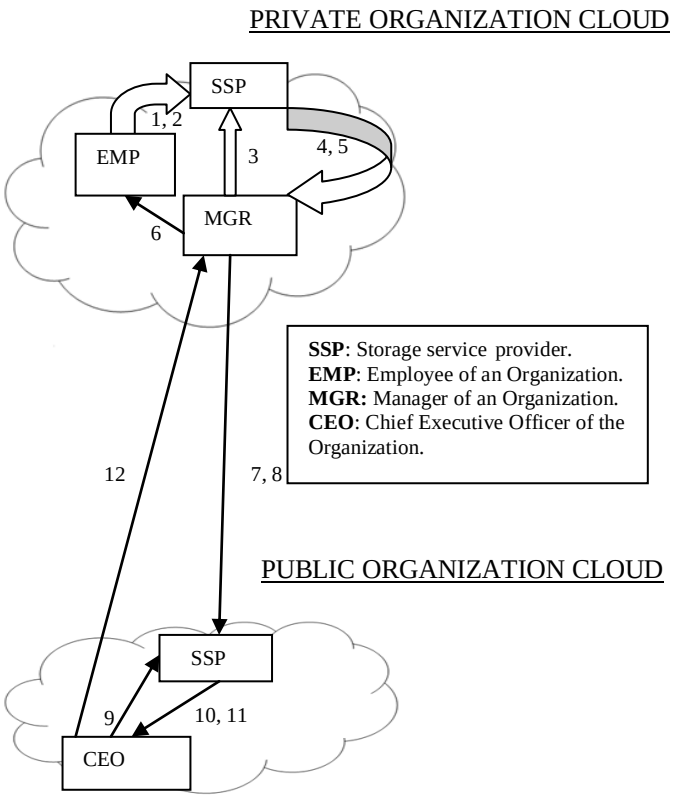

Figure 2: Data Interaction for a Single organization.

7. The manager (MGR) encrypts the data using secret key K_{mgr} as $C_{mgr} = E(K_{mgr}(data))$. Distribution of secret key is done in a secure manner between the manager (MGR) and chief executive officer (CEO) of the organization.
8. Both the access control matrix (ACM) and digital signature are created by the manager (MGR) and are sent to storage service provider (SSP) which is located in public organization cloud.
9. If the Chief Executive Officer (CEO) wants to see the data he submits his certificate $CERT_{auth}$ to SSP. The SSP in the public organization cloud verifies the certificate and checks ACM for authorization. Next the flow of data happens as follows:
10. A random session key Ksp is created by storage service provider (SSP) and again the C_{mgr} is encrypted as $C_{mgr} = E(K_{sp}(C_{mgr})) = E(K_{sp}(E(K_{mgr}(data))))$. The session key K_{sp} is also encrypted as $C_{Ksp} = E(K_{pceo}(K_{sp}))$ where $K_{pceo}$is the public key of CEO of the organization.
11. After receiving the encrypted data and key the CEO retains the key K_{sp} using his private key and the data is decrypted with K_{pceo} to get the original data sent by corresponding manager of the company (MGR).
12. After thorough scrutiny of data in case of any discrepancies CEO sends the data back to MGR for changes. The manager of each individual branch in turn verifies the data and in case of bulk changes will reassign the tasks back to the employee (EMP) of the company for further changes.

DOI 10.17148/IARJSET.2015.2306

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 3, March 2015

If the same procedure is repeated for multiple branches of the organization which is implemented as a private cloud then the secure communication can be done to public organization cloud where the CEO verifies the data. It is pictographically illustrated in figure 3:

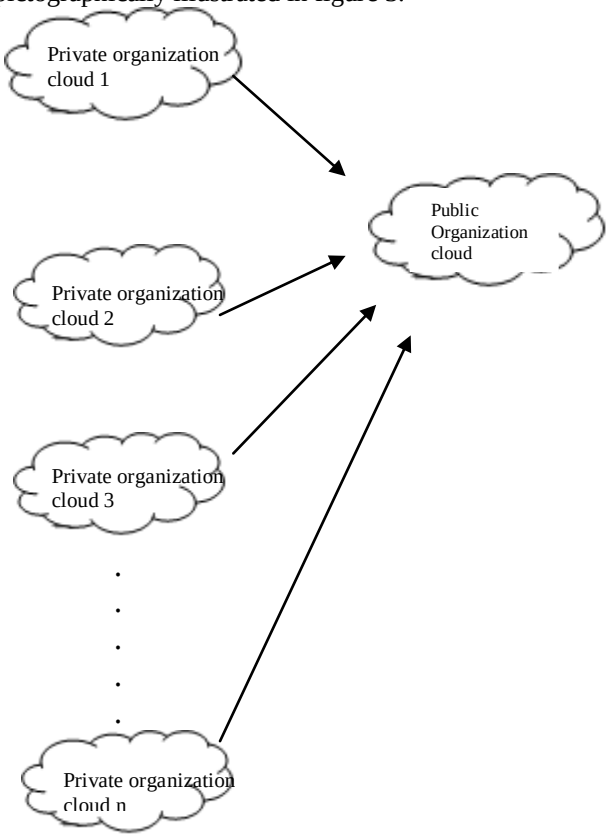

Figure 3: Hybrid Cloud Organization

IV. PERFORMANCE ANALYSIS

The proposed model has several features which makes it suitable to apply for all the existing organizations.

The important features can be mentioned as below:

(i) **Multi Level Security:** The employees of the organization are unaware of where the data is being submitted as they will be only in contact with the managers. The manager can in turn verify the data and submit it to the CEO. He also can add some confidential data which he wants to send to CEO.

(ii) **Efficient Data Transfer:** The data can be sent to the CEO securely when compared to the online submission.

(iii) **Attain maximum efficiency with lower cost:** Since it is cloud architecture the existing infrastructure of the organization can be adopted and the same can be implemented in the hybrid cloud model with security which will be more efficient.

(iv) **Offline submission of bulk data:** In spite of CEO being offline he can still view the data securely because of the storage service provider concept adopted in the model.

V. CONCLUSION AND FUTURE WORK

The main area of concern in cloud architecture has been to provide security. This paper makes an attempt to implement hybrid cloud architecture so that organizations can communicate with their central branch efficiently. This approach can also be extended to scenarios like institutions, banks and many more in future.

REFERENCES

[1] Diagram by Sam Joton http://en.wikip edia.org/wiki/File Cloud_ computin g_types.svg .
[2] liazhu Dai, QinZhou. A PKI-based Mechanism for Secure and Efficient Access to Outsourced Data.In proceedings of 201O International Conference on Networking and Digital Society.
[3] Weichao Wang,Zhiwei Li,Rodney Owens,Bharat,Bhargava.Secure and efficient access to outsourced data.In Proceedings of ACM Cloud Computing Security Workshop 2009.
[4] S. D. C. di Vimercati, S. Foresti, S. Jajodia,S. Paraboschi, and P. amarati. A data outsourcing architecture combining cryptography and access control. In Proceedings of the ACM workshop on Computer security architecture, pages 63-69, 2007.
[5] S. D. C. di Vimercati, S. Foresti, S. Jajodia,S. Paraboschi, and P. Samarati. Over-encryption: management of access control evolution on outsourced data. In Proceedings of the international conference on Very large databases, pages 123-134, 2007.
[6] Seny Kamara and Kristin Lauter. Cryptographic cloud storage.http://research.microsoft. com/,20 1 O.
[7] Josh Benaloh, Melissa Chase, Eric Horvitz, Kristin Lauter.Patient controlled encryption:ensuring privacy of electronic medical records. In Proceedings of ACM Cloud Computing Security Workshop 2009,pages85-90,2009.
[8] E. Miller, D. Long, W. Freeman, and B. Reed. Strong security for distributed file systems. In Proceedings of IEEE International Conference on Performance, Computing,and Communications,pages 34-40, 200l.
[9] Y. Kher and Y. Kim. Securing distributed storage:challenges,techniques, and systems. In Proceedings of the ACM workshop on Storage security andsurvivability, pages 9-25, 2005.
[10] A. Singh and L. Liu. Sharoes: A data sharing platform for outsourced enterprise storage environments. In Proceedings of the IEEE International Conference on Data Engineering, pages 993-1002, 2008.

BIOGRAPHIES

B.Santhosh Kumar did his B.Tech from Rajeev Gandhi Memorial College Of Engineering and Technology and M.S from Western Kentucky University, USA. He is currently working as an assistant professor in CSE department in G.Pulla Reddy Engineering College, Kurnool. His areas of interests include Cloud Computing, Cryptography and Web Technologies. He is currently pursuing his Ph.D. from Pondicherry University. He has published papers in three international journals.

Dr.Latha Parthiban has obtained her B.E in Electronics and Communication Engineering from University of Madras.

Her experience spans over 16 years in various Engineering colleges and her research interest includes Soft computing, Expert systems, Image Processing and cloud computing. She has published papers in 40 international journals and presented papers in 45 international and national conferences. She has also published a book in the area of computer aided diagnosis.