Implementation of Hybrid Cloud Model Based University Scenario Using PKI

[1]B. Santhosh Kumar, [2]Dr. Latha Parthiban, [3]Sabout Nagaraju
[1]Dept. of CSE, G.Pulla Reddy Engineering College, JNTUA, Kurnool, AP, India
[1,2]Dept. of CSE, Community College, Pondicherry University, Laws Pet, Pondicherry, India

Abstract
Education plays a vital role in every human's life. The purpose of maintaining the education quality and imparting them through various educational institutions is taken up by a university. In the present day education system many colleges will be affiliated to a university which takes the responsibility of maintaining good standards. In this paper a Hybrid cloud model is proposed through which many colleges affiliated to a university can exchange the confidential data with the university in a secure way. Each of the college is implemented as a private cloud with the Public Key Infrastructure (PKI) and the university as a public cloud with the PKI. So the combination of them gives a hybrid cloud model based approach.

Keywords
Hybrid cloud, University, Public Key Infrastructure (PKI)

I. Introduction

In the early days of education all the information pertaining to a college like attendance particulars of students, examination results etc.., were sent to their corresponding universities through postal services. As the technology advanced some of the softwares like FoxPro are being used in the colleges to update their college particulars and they are sent to the universities by taking a consolidated report of all the data either through fax or email. Adaptation of this method leads to lot of time consumption and there is a possibility for the data to be stolen by some malicious users. This might result in incorrect judgement of grade, attendance at the universities.

So using the current emerging technology of cloud computing this issue can be resolved to a large extent. All the confidential details of the college can be entered by the faculties of that particular college who are chosen by the college central representatives like chairman, director or principal of that college. Since the whole process is happening within a college this entire scenario can be implemented as a private cloud. The faculties will submit the details to the central representatives of that college by following the PKI. The central representative after verifying the entire data will submit it to the university. The university representatives can only read the data sent by the college and in case of any discrepancies can be reverted back to the college central representatives.

First the hybrid cloud architecture is discussed in brief which forms the core of this paper. Hybrid cloud can be defined as a combination of at least one private cloud and one public cloud. It can be illustrated using the following figure.

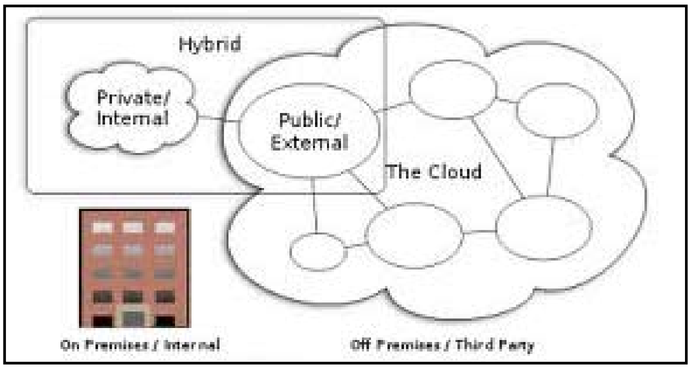

Fig. 1: [2] Hybrid Cloud Architecture

The main components of a hybrid cloud are:

A. Private/Internal Cloud

This cloud can be implemented as a part of organization or a company which can be treated as on premises. Hence it can be also called as internal cloud.

B. Public/External Cloud

This cloud can be implemented off premises and the services offered can be used by the public. It is also referred as External cloud.

The main advantages of hybrid cloud over remaining cloud types are:

C. Scalability

A company or organization can plan to increase their resources without change in the architecture.

D. Lower Cost

It gives the reluctant companies on cloud architecture an idea to go for the cloud computing model at a low cost and reduced risk.

Various reports have been submitted over the years on cloud computing security. [3-7], proposed cryptographic access control model in owner-write-user-read scenario which formed the basis for PKI proposed model in [1]. Using the above discussed hybrid cloud architecture and the public key infrastructure which is discussed in research paper [1] a model is proposed in section II through which a college can communicate with a university in a confidential way. In section III the performance analysis of the proposed model with the present existing system is considered. Section IV draws the conclusion and in section V the future work that can be done on the proposed model is discussed.

II. Proposed Model

It is assumed that PKI is established in private college cloud and public university cloud and both Certificate Authorities (CA) have issued certificates. All the assumptions which have been made in research paper [1] are also extended to this model.

The proposed architecture can be pictographically represented as in fig. 2.

III. Private College Cloud

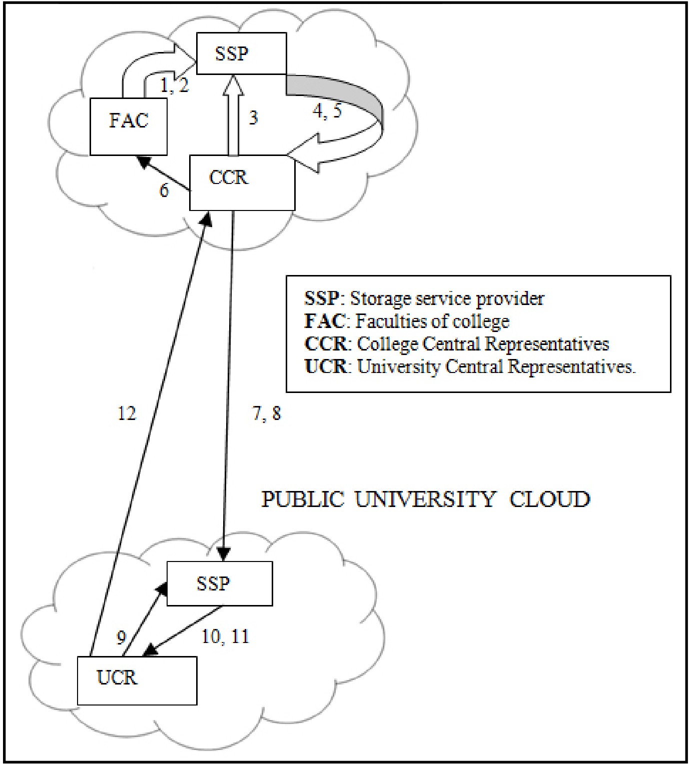
SSP
1, 2
FAC
3
4, 5
CCR
6
SSP: Storage service provider
FAC: Faculties of college
CCR: College Central Representatives
UCR: University Central Representatives.
12
7, 8
PUBLIC UNIVERSITY CLOUD
SSP
9
10, 11
UCR

Fig. 2: Proposed Hybrid Cloud Model Based University Scenario for Single College

The entire process in private college cloud takes place as follows:

1. The faculties who are the authorized persons appointed by the central representatives of the college will encrypt the data to be sent using secret keys K_{f1}, K_{f2}...As C_f = E (K_{fi} (data)). The secret keys are distributed between faculties and central representatives of college in secure manner.

2. The faculties create the Access Control Matrix(ACM) And digital signature for the data and send them to Storage Service Provider (SSP).

3.When the College Central Representatives (CCR) want to get back the data they provide their certificates CERTauthi. The SSP verifies the certificates and checks the ACM for authorization. Then the data is sent as follows:

4. The SSP creates a random session key Ksp and again does the encryption of Cf as

C_{ef} = E(K_{sp} (C_f)) = (K_{sp}(E(K_{fi}(data))). The secret key can also be encrypted as C K_{sp} = E(K_{pccr}(K_{sp})) where K_{pccr} is public key of central representative of college.

5. When both the encrypted data and key is sent to college central representatives the key K_{sp} is got back using his private key and the data is decrypted with K_{fi} to get back the data sent by the corresponding faculty.

6. The CCR thoroughly goes through the data and in case of any discrepancies will sent back the data to the corresponding faculty who does the necessary changes and returns it back to the CCR. The CCR is responsible for

Submitting the data to the university central representatives (UCR) but he gets the work done through the faculties of the college. After the CCR verifies the data and found it to be genuine he submits the data to the public university cloud in the following manner:

7. The CCR encrypts the data using secret key K_{ccr} as C_{ccr} = E (K_{ccr} (data)). Distribution of secret key is done in a secure manner between CCR and UCR.

8. Both the Access Control Matrix (ACM) and digital signature is created by CCR and are sent to Storage Service Provider (SSP) which is located in public university cloud.

9. To get back the data at the university UCR provides his certificate CERTauth to SSP. The SSP 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 SSP and again the Cccr is encrypted as C_{eccr}= E (K_{sp} (C_{ccr})) =E (K_{sp} (E (K_{ccr} (data))). The session key K_{sp} is also encrypted as C K_{sp}=E (K_{pucr} (K_{sp})) where Kpucr is the public key of UCR.

11. After receiving the encrypted data and key the UCR gets back the key Ksp using his private key and the data is decrypted with Kccr to get the original data sent by corresponding CCR.

12. After verifying data and in case of any discrepancies UCR sends the data back to CCR for changes. The CCR inturn verifies the data and in case of huge changes will be sent back to corresponding faculty for updating the data. After updating is done again the whole process is repeated to send the genuine data back to the university.

Until now the idea is implemented in a single college. If it is extended further to multiple colleges then many colleges will be able to interact with the university through hybrid cloud model. The scenario can be depicted with the following fig.

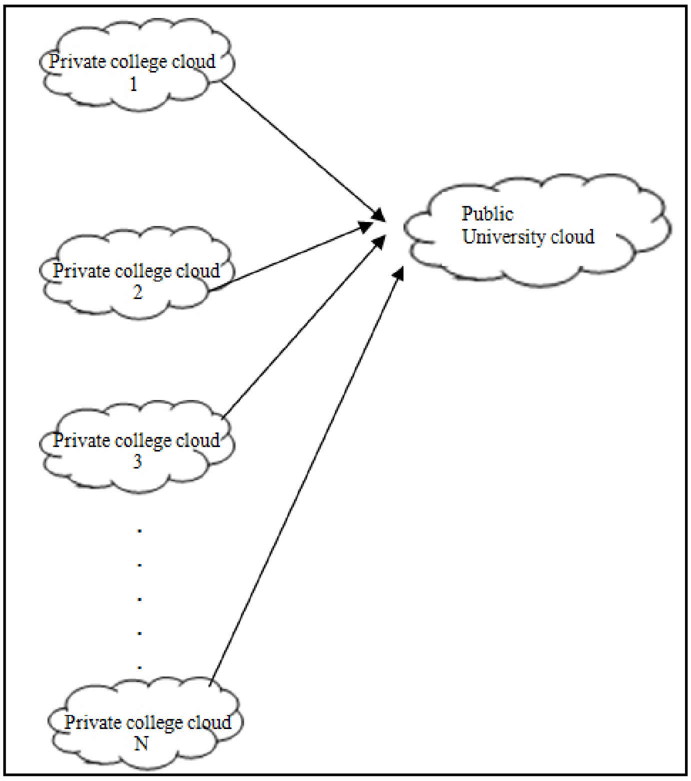

Fig. 3: Hybrid Cloud Model for Interaction of Multiple Colleges in a University

As shown above many colleges can interact with the university through a hybrid cloud model approach. Each college is implemented as a private cloud and the university as a public cloud. In the next section the performance of the proposed model with the traditional approach followed by the university is discussed.

III. Performance Analysis

The proposed hybrid cloud based model of the university has many advantages over the traditional approach. some of the important concepts are discussed here.

A. Security at Multiple Levels

The faculty of the college is unaware of where the data is being sent and they can only submit it to the CCR. The CCR after verifying the data will submit it to the UCR. The data is submitted only after the certification and identity verification.

B. Faster Transfer of Data

when compared to the traditional approach this model allows all the colleges to submit their data to the university in a faster way.

C. Low cost with Maximum Efficiency

Taking the advantage of hybrid cloud model approach all the colleges can follow existing infrastructure and move to the cloud computing approach. There is no need to make major changes and so it can be offered at low cost.

D. Offline Submission of Bulk Data

Even though the UCR is not online the colleges can submit their data and they will be stored in SSP.Whenever the university wants to verify they can do so by issuing their certificate.

IV. Conclusion

Based on a hybrid cloud model architecture and PKI based mechanism a model for a university scenario has been proposed. The main idea is to make the interaction between the colleges and university in a more secure and efficient way. The private college cloud architecture allows the colleges to follow their own infrastructure and submit the details to the university which is implemented as a public cloud.

V. Future Work

The idea has to be practically implemented at different colleges as private clouds and the data has to be submitted to the university. This model can also be extended so that all the colleges can share the academic related information among themselves and if some of them want to pass any resolution together they can do it securely.

References

[1] 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.

[2] Sam Joton,"Diagram", [Online] Available: http://en.wikipedia.org/wiki/File:Cloud_computing_types.svg .

[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, P. Samarati,"A data outsourcing architecture combining cryptography and access control", In Proceedings of the ACM workshop on Computer security architecture, pp. 63-69, 2007.

[5] S. D. C. Di Vimercati, S. Foresti, S. Jajodia,S. Paraboschi, P. Samarati,"Over-encryption: management of access control evolution on outsourced data", In Proceedings of the international conference on Very large databases, pp. 123-134, 2007.

[6] Seny Kamara, Kristin Lauter,"Cryptographic cloud storage", [Online] Available: http://www.research.microsoft. com/, 2010.

[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, pp. 85-90.

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 CloudComputing, Cryptography and Web Technologies. He is currently pursuing his Ph.D. from Pondicherry University.

Dr.Latha Parthiban has obtained her B.E in Electronics and Communication Engineering from University of Madras, M.E. in Computer Science and Engineering from Anna University, Chennai and has obtained her PhD from Pondicherry University.

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 6 international journals and presented papers in 18 international and national conferences. She has also published a book in the area of computer aided diagnosis.

Sabout Nagaraju is currently working as assistant professor in Pondicherry University. He graduated from G.Pulla Reddy Engineering College, Kurnool and did his post graduation from NIT, Calicut. His areas of interest include cloud computing, Design and analysis of algorithms, Cryptography. He is pursuing his Ph.D. from Pondicherry University.