International Journal of Mathematical Archive-4(11), 2013, 216-219
Available online through www.ijma.info ISSN 2229 – 5046

TRUSTED AND MUTUAL MANAGER BASED APPROACH FOR CLOUD SECURITY

Jitendra Singh Rajawat[1*] and Sanjay Gaur[2]

[1]Research Scholar, Pacific Institute of Technology

[2]Associate Professor and Coordinator, Faculty of Computer Application, Pacific University

(Received on: 23-10-13; Revised & Accepted on: 18-11-13)

ABSTRACT

Cloud computing is the next immense mania after internet in the field of information technology. We can say that it is now running as metaphor for internet. Cloud computing is internet based computing technology where software, shared resources and information are provided to consumers or devices on-demand. Cloud is just a huge storage for ready on service of software and support services. It consist of giant database of software and software services. But the major problem associated with cloud is security measures. The traditional security measures are now not enough for that purpose. This study tries to give a secure model or algorithm for securing cloud during transaction of software and support services. The proposed framework clearly describes the objectives of algorithm and their utility in present scenario where cloud is going to be synonyms of internet.

Key Words: *Trusted, Security, Authentication, Encryption, Algorithm, Server.*

1. INTRODUCTION

Cloud computing deals with providing storage and computation resources as a service to the Cloud Service Users (CSU) in the form of Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Storage as a Service (SaaS) etc. Software as a Service ensures to provide services as pay-as-you-go pricing scheme where customer does not need to install configure or run the application on their local computers.

Platform as a Service offers a software execution environment to deploy Web-based applications. Users do not need to think about the cost and complexity of buying servers or setting the infrastructure. Therefore PaaS refers to provide a development platform to deploy, host or maintains their applications. Infrastructure as a Service shares hardware resources for executing services using virtualization

There are lots of attackers that violate data security concept in the cloud; they can be attackers from inside the cloud environment for instance suspicious employee at CSP. The CSP is responsible for storage infrastructure and web services interface that can be used for storing and checking the user data. In addition, attackers can be from outside the cloud environment like the intruders or network attackers.

Security of cloud is major issue at present scenario due to cloud become not part of routine life [4]. So there is need of trusted security model to enhance the security during the data transformation condition because these tasks are done at various stages [1]. In [2] study of risk and analysis of risk are discussed which are associated with the security of cloud and control of cloud in the general environment of data exchange.

The primary focus of this paper is to introduce a novel and trusted security framework for securing cloud resources.

2. PROPOSED FRAMEWORK

The proposed framework for Cloud Security has two stages. First is user stage and another is service provider stage .User stage is denoted by stage 1 and service provider stage is denoted by stage 2. This two stage proposed framework authenticates service user for accessing private information from cloud storage.

One of the major advantages of this framework is that user manager and provider manager maintain their own databases. Any demand for information made by service user is checked at two stage one after another and after fulfilling the basic requirements for trust demand for information is granted

Corresponding author: Jitendra Singh Rajawat[1]*

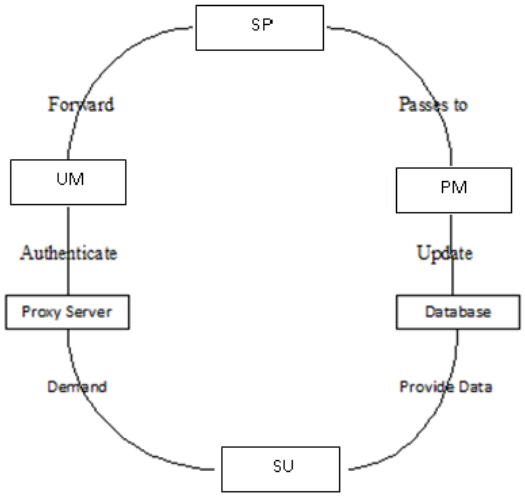

Fig 1: Cyclic Diagram of Proposed framework

The flow of information as denoted in Fig 1 is explained below to understand the working of proposed model:

Step1: SU supply identification to proxy server to demand for information.

Step 2: Proxy server performs validation of information given by SU if the information is correct in that case demand will pass to UM, otherwise information demand will be rejected.

Step 3: UM is checking demand to find trust degree of this SU if it found correct demand reaches to SP

Step 4: SP forward demand to PM who again check demand.

Step 5: If demand found correct and trusty then demand send to user via proxy server.

Step 6: Information reaches to SU via proxy server

Step 7: SU get the desired information which user demand

Step 8: UM update the database.

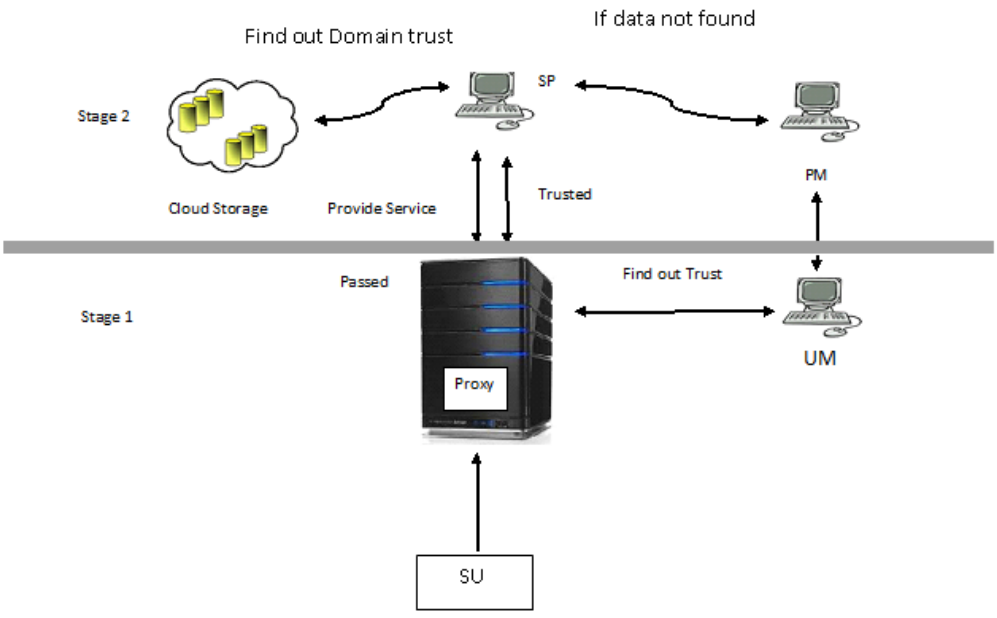

Fig 2: Proposed Two Stage Security Framework for Cloud Computing

The proposed two stage security framework for cloud has following components.

Service User (SU): Demand services from cloud storage.

1) Service Provider (SP): Give services to the demanding trusted SU.

2) Proxy Server (PXS): Perform checking of authentication for the SU & control flow of communication.

3) User Manager (UM): Check the authentication of demanding SU & updates accordingly.

4) Provider Manager (PM): Check the trust of the service demanding SU.

3. ALGORITHMS

In this part we proposed algorithms to determine the trustworthiness of any service demanding SU and providing information which user demands if the demand fulfill the basic trust requirements.

3.1 ALGORITHM FOR DEMANDING INFORMATION

Input: User id ID; password PSD; Trust Value TV; Service Demand (SD)

Output: SD to acceptance or deny

Start
1) Proxy server PXS checks (ID, PSD);
2) If authenticate
3) PXS forward the demand to User Manager (UM)
4) UM validates TV;
5) If TV found correct and trusty (If TV get authentication from UM and validate by cloud)
Demand SD for information reaches SP;
Else
Discard the demand SD;
End

3.2 ALGORITHM FOR SENDING INFORMATION

Input: Service demand SD, Trust Value TV,

Output: Sending information to Service User or refuse demand

Start

1) SP send incoming demand for SD to Provider Manager (PM);
2) If TV found correct and trusty
3) Send SD to user through PXS
4) SP updates the warehouse
Else
Refuse the demand SD;
5) PM notify UM regarding SD
6) UM updates warehouse
7) SU get the desired demand information
End.

4. CONCLUSION

The proposed framework is based on two stage interoperability to secure the cloud data. The strength of proposed algorithm is quite simple than any other security algorithm used in cloud computing for secure and trusted storage. This model guide, how to allow only authorized access to cloud data. It works on the information provided by user manager and provider manager, by this mutual approach it's provide a trusted and secure storage for cloud data storage. Although the framework is dependent on information provided by the managers but this model is the best approach to provide user friendly secure and trusted framework. For more secure and trusted model it is required that the framework should work independently. It would be a new site or direction we have to work to enhance the proposed framework.

5. REFERENCES

[1] Chandran S. and Angepat M.,(2010) 'Cloud Computing: Analyzing the risks involved in cloud computing environments' *in Proceedings of Natural Sciences and Engineering*, Sweden, pp. 2-4.

[2] Cyril Onwubiko,(2010), 'Security Issues to Cloud Computing', in Cloud Computing: Principles, Systems and Applications, Computer Communications and Networks, N. Antonopoulos and L. Gillam (Eds.), Springer-Verlag London Limited 2010, DOI 10.1007/978-1-84996-241- 4-16, pp. 271-288.

.

[3] Mell P. and Grance G.,(2011) ,'The NIST Definition of Cloud Computing (Draft)', *in Proceedings of the National Institute of Standards and Technology*, Gaithersburg, pp. 6, 2011.

[4] Wenjuan Li and Lingdi Ping, (2009),'Trust Model to Enhance Security and Interoperability of Cloud Environment', *Proc. of Cloud Com 2009*, Springer-Verlag Berlin Heidelberg 2009, LNCS 5931, pp. 69-79.

Source of support: Nil, Conflict of interest: None Declared

