ISSN 2229-5518

Modified Secure Cloud Computing Platform

Ashish Negi, Praveen Tiwari, Priti Dimri

Abstract— Cloud Computing presents a distinct way to share distributed resources and services with the help of internet. Cloud computing includes sharing of distributed resources via internet- an open network, therefore security becomes an essential issue. A secure data transmission and key management is needed in cloud computing, to overcome such problems. In this paper, we proposed an Encryption technique enabled platform to make a normal cloud computing platform to trusted cloud computing platform and assured a secure data transmission.

Index Terms— Cloud computing, Security, Encryption, Cryptography.

1 INTRODUCTION

Cloud computing platform is a set of Scalable large-scale data server clusters, it provide computing and storage services to customers. The cloud storage is a relatively basic and widely applied service which can provide users with stable, massive data storage space.[1]

Cloud computing is fast becoming a popular option for renting of computing and storage infrastructure services (called Infrastructure as a Service or IaaS); for remote platform building and customization for business processes (called Platform as a Service or PaaS); and for renting of business applications as a whole (called Software as a Service or SaaS). The cloud infrastructure has been further sub-divided into, Public cloud - where the infrastructure resides totally outside of the tenant / enterprises? firewall; Hybrid cloud - where the infrastructure and business processes reside partly within the enterprise and partly consumed from third party; and Private cloud - where IT services are mounted on top of large-scale conglomerated and virtualized infrastructure within enterprise firewall and consumed in "per transaction" basis.[3].

There is a growing body of work dealing with various cloud computing security issues. Authors have mostly discussed about singular aspects of cloud security such as vulnerabilities in platform layer (virtualization, network, or common software stacks); vulnerabilities with co-located user data and multi- tenancy; access control; identity management and so on.

We observe that data, platform, user access and physical security issues; although accentuated in cloud computing; are generally applicable in other enterprise computing scenario as well. For example, hypervisor related threats such as cross channel attacks will be present in any virtualized environment not specific to cloud. Two of the great virtues of cloud computing are service abstraction and location transparency. However, from security point of view these two points in conjunction with third-party control of data can create challenging security implications [3].

In the system architecture, there is a central entity to index or manage the distributed data storage entities. It is effective to simplify the design and maintenance of the system by a central managed architecture, but the central entity may become a bottleneck if the visiting to it is very frequent. Although systems in practice have used some technique as backup recovery to avoid the probably disaster from the central bottle neck, the flaw come from the architecture has not resolved essentially [1]. On Other side, Security and privacy are two prime barriers to adoption of the cloud computing [2]. Cloud computing, which is considered to be the next big trend of information age by many people, offers great benefits including: low up front IT investments, pay-for-use model allows for reduced operating expenses, reduced complexity, etc. However organizations or companies have to upload their data or programs to the cloud, obviously security and privacy will be two significant barriers to Adoption [2].

2 RELATED WORK ABOUT CLOUD COMPUTING SECURITY

2.1 Security Concerned Cloud Computing

2.1.1 Current Security model of the cloud computing

In order to archive security in cloud computing system, some technologies have been used to build the security mechanism for cloud computing. The cloud computing security can be provided as security services. Security messages and secured messages can be transported. Even the mechanism for the cloud computing security has many merits now, but there are still some disadvantages. For example, there is short of the mechanism on the hardware to support the trusted computing in cloud computing system. The creation and protection of certificates are not secure enough for cloud computing environments. The performance is reduced apparently when the cryptographic computing are processed. There are also lack of some

mechanisms to register and classify the participants carefully, such as the tracing and monitoring for them [4].

2.1.2 The challenge for the security in cloud computing

In cloud computing environment, many users participate in the CLOUD and they join or leave CLOUD dynamically. Other resources in the cloud computing environments are the same too. Users, resources, and the CLOUD should establish the trustful relationship among themselves. And they will be able to deal with the changing dynamically. The CLOUD includes distributed users and resource from distributed local systems or organizes, which have different security policies. According to this reason, how to build a suitable relationship among them is a challenge. In fact, the requirements for the security in cloud computing environment have some aspects, including confidentiality, multiple security policy, dynamic of the services, the trust among the entities, dynamically building trust domains [4].

2.2 The main security problem of cloud computing

1) Attacks:- The network attack is still the biggest challenge of network security. As more and more packages, customers, and enterprises migrate their data into the cloud computing, cloud computing will appear more and more network attacks and fraud. According to a Survey, Security experts said that cloud computing will be the focus of hackers within five years.

2) Data Security:- "Data of Cloud" is stored in different physical locations, in the absence of
Corresponding technical and regulatory constraints, data security is difficult to get protection.

3) Safety standards:- There were not the security model and standards for cloud computing architecture, the confidentiality, integrity and availability of data in the cloud service will be borne by the ultimate consumers of cloud computing, not by the cloud service providers, the rapid development of cloud computing is Promoted by several major IT giants, although they are taking the money in the IT field, after all cloud computing is a new thing, and structural standard between the different cloud computing service provider is not perfect.

4) Private information not Safer:-

Cloud users store data in the cloud, but they can not ensure if their private information is sold out by cloud service providers or not. How to select the Trusted Cloud Computing service provider? For example, in March of 2009, the famous Google has admitted that it leaked private customer information accidentally.

3 Model and Problem Work

Now a day cloud computing make everything flexible and easier but there is another aspect that is what about security? Is cloud computing in current scenario is providing confidentiality, integrity and being regulated by compliance like Data Protection Act. Through cloud computing the resource are centralized, so the exposure factor proportionally increase which results in risk. So it is necessary to put a countermeasure to mitigate the potential risk. According to the survey, some company says that due to cloud computing it become easier for bad guys to focus their effort and breach hundred of thousand of record [1]. There is no security rating system in place for cloud computing, so business users can't rely on third party security mechanism. Risk factor with cloud computing are high because level of security provided by cloud provider are not same.

General Framework

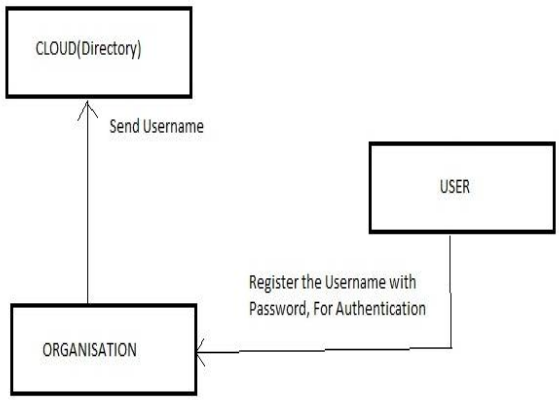

Figure 1

After classification of data, three entity is considered, first one is cloud provider itself, second is organization whose data resides at cloud and last one is employee or anonymous user who request for access of cloud data.
Now the above figure gives overview of Registration phase, in which if a user (either employee or anonymous) want to access the data then user have to register itself (if he is already registered need not require further registration), after registering itself then the transaction will become secure and the process become authenticated.
In this Process the user registered itself for accessing data, organization will provide username and password for authentication. At the same time organization sends the username to cloud provider.

II. Authentication Overview

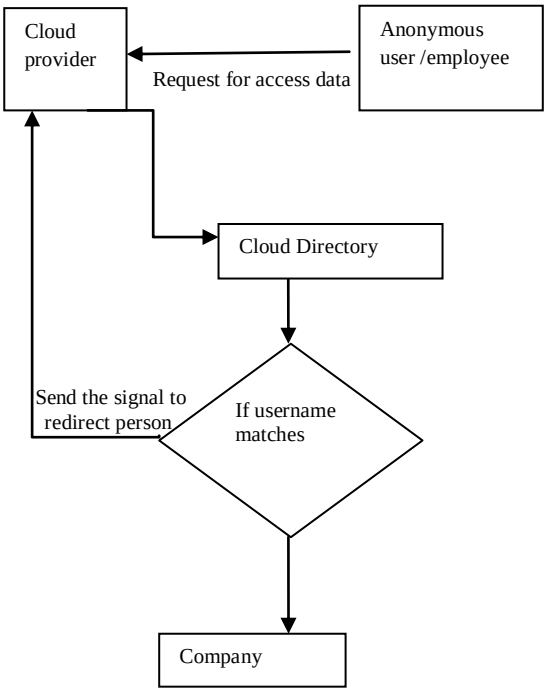

FIGURE 2

Now when user sends request along with username to access the data to cloud provider, the cloud provider first check in which ring requested data belong. If authentication is required, it first check the username in its own directory for existence, if the username does not exist it ask the user to register itself. If the username matches it redirect the request to company for authentication. The above Figure 2 represents the overall working environment of cloud computing model.

There are several steps of working over here, after registering as authentic user.

Step I Anonymous user send request for accessing data to the Cloud.

Step II The active Cloud check out in its directory for the status of the User.

Step III If the user name exists and verified than the process link up is create and the user redirects to the company.

Step IV If the Username doesn't match than the link is break and sign of unauthorised access will show.

The following figure 3 shows the modified general framework for a cloud computing platform.

III. Modified Framework

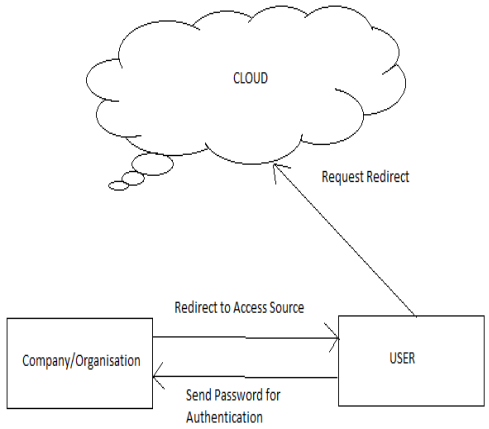

FIGURE 3

Now the user sends password for authentication, and after authentication it redirect the request to cloud provider to access resource. Only after the confirmation of Company or cloud provider. Such kind of working style can save user from many kind of security attacks, hence this kind of platforms which are fully enriched by key management process are safe to access data.

4 Conclusion

This technique provides a new way to authenticate in different approaches. It provides availability of data by overcoming many existing problem like denial of services, data leakage. As additional it also provides more flexibility and capability to meet the new demand of today's complex and diverse network.

5 References

1. A cloud computing platform based on P2P, Ke Xu et al, 2009

2. An improved trusted cloud computing platform model based on DAA and Privacy CA scheme, Wang Han-zhang et al, 2010

3. Cloud Computing Security - Trends and Research Directions, Shubhashis Sengupta etal, 2011

4. The Security of Cloud Computing System enabled by Trusted Computing Technology, Zhidong Shen et al, 2010

5. Security Issues and Countermeasures in Cloud Computing, Wang Jun-jie et al, 2011

6. Data security in the world of cloud computing, John harauz et al, 2010

7. Cloud computing security management, Sameera Abdulrahman et al, 2009

8. Inforamtion security risk management framework for cloud

computing environments, Xuan Zhang et al, 2010
9. A layered security approach for cloud computing infrastructure, Mehnet Yeldiz et al, 2010

ABOUT THE AUTHORS

Ashish Negi is currently working as an Associate Professor in Department of Computer Science & Engineering at G.B. Pant Engineering College, Pauri Garhwal
Uttarakhand-246149,India,PH-+91 1368 228030
E-mail: ashish.ne@gmail.com

Preeti Dimri is currently working as an Associate Professor in Department of Computer Science & Engineering at G.B. Pant Engineering College, Pauri Garhwal
Uttarakhand-246149,India,PH-+91 1368 228030
E-mail: pdimri1@gmail.com

Praveen Tiwari is currently Pursuing Master of Technology in Computer Science & Engineering, at G.B. Pant Engineering College, Pauri Garhwal,
Uttarakhand-246149,India,PH-+91 1368 228030
E-mail: tiwari_prav@rediffmail.com