Review on Security Issues in Cloud Computing

[1]A.Ravi Kiran, [2]R.Tamilkodi
[1]P.G Student, [2]Associate Professor,
[1,2]Department of computer applications, Godavari Institute of Engineering and Technology, Rajahmundry, India

***Abstract*—**Cloud computing is a structural design for providing computing service via the internet on demand and pay per use access to a group of shared assets namely networks, storage, servers, services and applications, without actually acquiring them. So it saves control the cost and time for organizations. several industries, such as banking, healthcare and education are moving towards the cloud appropriate to the efficiency of services provided by the pay-per-use model based on the assets such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. Cloud computing is a absolutely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.som and Microsoft etc. Some degree of control over the data may acquire various security issues and threats which include data leakage, insecure interface, sharing of resources, data accessibility and inside attacks. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and consistency. This paper shows what are all the issues we are facing in cloud storage.

***Keywords*--** Security Issues, Cloud Security, Cloud structural design, Data Protection, Cloud Platform, cloud storage.

I. INTRODUCTION

Cloud Computing is a scattered architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud service providers (CSP's) offer cloud platforms for their customers to utilize and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs (cloud service providers) and ISPs (Internet Service Providers) in cooperation services [1]. Cloud computing is a model that enables convenient, on-demand network access to a shared group of configurable computing resources such as networks, servers, storage, applications that can be speedily provisioned and released with minimal management effort or service provider's interaction[2].

Cloud providers offer three types of services [1] i.e. Software as a Service (SaaS), Platform as a Service (PaaS) ,and Infrastructure as a Service (IaaS). There are various reasons for organizations to move towards IT solutions that consist of cloud computing as they are just required to pay for the resources on consumption basis.

Clouds are the new trend in the development of the distributed systems, the precursor of cloud being the grid. The user does not need knowledge or capability to control the infrastructure of clouds; it provides only abstraction. It can be utilized as a service of an Internet with high scalability, higher throughput, quality of service and high computing authority. Cloud computing providers deliver common online industry applications which are accessed from servers through web browser [2].

While initially this idea was present only in the academic area, recently, it was transposed into industry by companies like Microsoft, Amazon, Google and Salesforce.com. This makes it possible for new startups to enter the market easier, since the cost of the infrastructure is greatly diminished[3]. This allows developers to focus on the business value rather on the starting budget. The clients of commercial clouds rent computing power or storage space (virtual space) dynamically[2]. With the utilize of this technology, users can access heavy applications via insubstantial portable devices such as mobile phones, PCs and PDAs.

II. PROPOSED METHODOLOGY

Cloud Computing mainly addresses the challenges of meeting the requirements of next generation private, public and hybrid. Cloud computing architectures, also challenges of allowing applications and development platforms to take advantage of the benefits of cloud computing. The research on cloud computing is still at an early stage. Many existing issues have not been fully addressed, while new challenges keep emerging from industry applications. To solve the this above challenges it introduces two secure system. Which generate better and efficient system for accessing massive data on Cloud.

1. SecCloud
2. SecCloud+

III. CLOUD COMPUTING MODELS

Generally cloud services can be divided into three categories[1]:

1. Software as a Service (SaaS).
2. Platform as a Service (PaaS).
3. Infrastructure as a Service (IaaS).

Software-as-a-Service (SaaS): Software as a service(SaaS) can be described as a process by which Application Service Provider (ASP) provide various software applications over the Internet. This makes the customer to get free of installing and operating the application on personal computer and also eliminates the wonderful load of software maintenance, continuing operation, protection and support [3]. SaaS features a complete application accessible as a service on demand. Examples of SaaS includes: Salesforce.com, Google Apps.

Platform as a Service (PaaS): Platform as a service (PaaS) is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end-users[4]. It provides an infrastructure with a high level of integration in order to implement and test cloud applications.

Infrastructure as a Service (IaaS): Infrastructure as a service (IaaS) refers to the sharing of hardware assets for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage additional readily accessible by applications and operating systems[3]. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner.Infrastructure, but he controls the operating systems, storage and deployed applications. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Examples of IaaS includes Amazon Elastic Cloud Computing (EC2), Amazon S3.

IV. CLOUD DEPLOYMENT MODELS

1. Private cloud
2. Public cloud,
3. Hybrid cloud and
4. Community cloud.

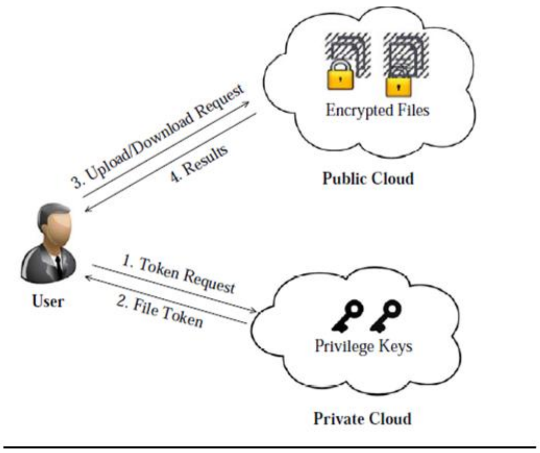


Figure 1: Cloud deployment model architecture

Private cloud: Private cloud can be owned and managed by the organization or a third party and exist at on premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security rules, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security. One of the greatest examples of a private cloud is Eucalyptus Systems [4].

Public Cloud: A cloud infrastructure is provided to a lot of clients and is managed by a third party and exist further than the company firewall [3]. Multiple enterprises can work on the infrastructure provided. These clouds are fully hosted and managed by the cloud provider and fully responsibilities of system, management, provisioning, and maintenance. Public cloud providers such as Google or Amazon offer an access control to their customers [6]. Examples of a public cloud include Microsoft Azure, Google App Engine.

Hybrid Cloud: A composition of two or more cloud and its deployment models, correlated in a way that data transfer takes place between them without distressing each other.

These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider [5]. A well-constructed hybrid cloud accepting customer payments. Drawback to the hybrid cloud is the complexity in effectively creating and governing such a result. These can be private, community or public clouds which are correlated by a proprietary or standard technology that provides portability of data and applications among the composing clouds. An example of a Hybrid Cloud includes Amazon Web Services (AWS).

Community Cloud: Infrastructure shared by a number of organizations for a shared cause and may be managed by them and rarely accessible cloud model. These clouds are normally based on an agreement among related business organizations such as banking or educational organizations [7,8]. A cloud environment operating according to this representation may exist locally or remotely. An example of a Community Cloud includes Facebook.

V. SECURITY ISSUES IN CLOUD

Cloud Computing is not a new technology instantly the existing technology reorganized in a new format thereby providing new mode of communication[3]. It suffers from all inherent issues the previous networking technologies suffered. Networking among two computers has always been plagued with security and privacy issuses [4].

The cloud computing suffers from the following drawbacks:

1. Data Security and Privacy
2. Compliance Issues
3. Funding
4. Lack of Standardization
5. Identity and Access Management.

A. Data security and privacy:

Data is stored in the cloud shared by multiple tenants. The private information is stored away from its owner, which increases its exposure[4]. This raises serious questions regarding the security of user's data. The privacy of cloud data cannot be guaranteed.

B. Compliance issues:

The cloud is an incorporation of many different facets such as various computing resources, cross-border locations, multiple tenants of the same computing resource, etc. Each different measurement provides different set of rules and regulations for the service provider to follow. Cloud data requests to be secured, the cloud service providers have to observe with regular audits.

C. Funding:

A cloud alone comprises of several components and services requiring sufficient funding. A cloud service provider has to set up bulky data centers to store data and provide other services such as IaaS, etc.

D. Identity and access management:

Data in the cloud is stored at various locations, that is, the location of data in the cloud is portable. The cloud user may or may not be aware of his data's location. The cloud being multi-tenant in environment, the cloud user may have to logon using different user credentials for different providers. A cloud needs to have a strong and sturdy identity and access management system in place so as to attract more transfers to the cloud

VI. SYSTEM DESIGN

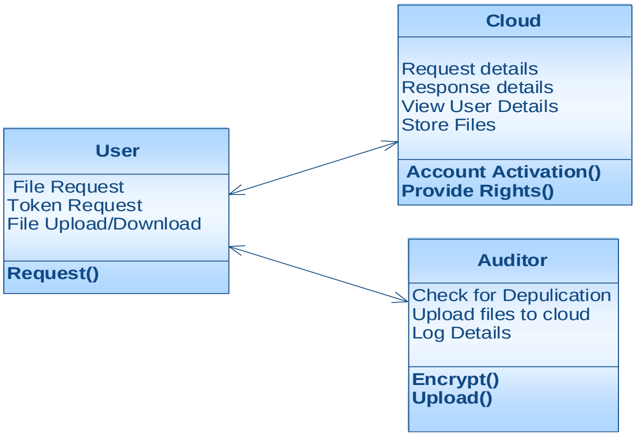


Figure 1: System design

VII. RESULT

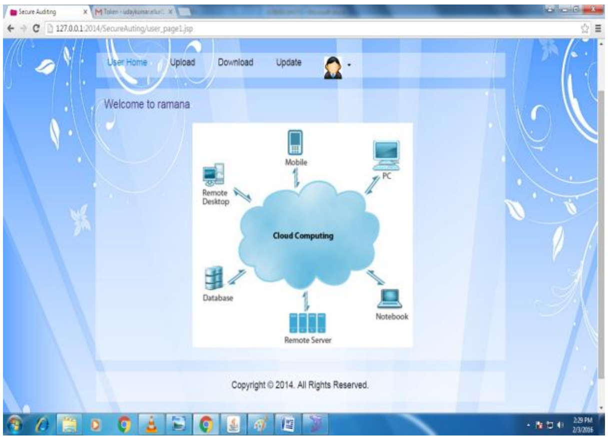
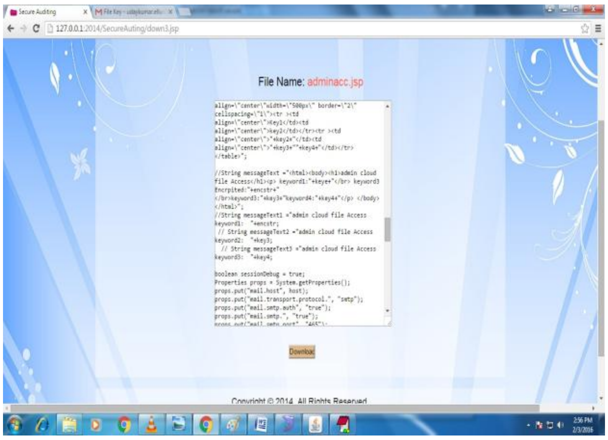


Figure 3: User home page.


Secure Auditing
File Key - udaykumar.eluri
127.0.0.1:2014/SecureAuting/down3.jsp
Download
Copyright © 2014. All Rights Reserved.

File Name: adminacc.jsp

```
align=\"center\"width=\"500px\" border=\"2\"
cellspacing=\"1\"><tr ><td
align=\"center\">Key1</td><td
align=\"center\">key2</td></tr><tr ><td
align=\"center\">"+key2+"</td><td
align=\"center\">"+key3+""+key4+"</td></tr>
</table>";

//String messageText ="<html><body><h1>admin cloud
file Access</h1><p> keyword1:"+keye+"</br> keyword3
Encrpited:"+encstr+"
</br>keyword3:"+key3+"keyword4:"+key4+"</p> </body>
</html>";
//String messageText1 ="admin cloud file Access
keyword1:  "+encstr;
 // String messageText2 ="admin cloud file Access
keyword2:  "+key3;
  // String messageText3 ="admin cloud file Access
keyword3:  "+key4;

boolean sessionDebug = true;
Properties props = System.getProperties();
props.put("mail.host", host);
props.put("mail.transport.protocol.", "smtp");
props.put("mail.smtp.auth", "true");
props.put("mail.smtp.", "true");
props.put("mail.smtp.port", "465");
```

Figure 4: Source of encrypted file.

CONCLUSION

One of the biggest security worries with the cloud computing representation is the sharing of resources. Cloud service providers require to inform their clients on the level of security that they provide on their cloud. In this paper, we first discussed various models of cloud computing, security issues. This paper has highlighted all these issues of cloud computing. We believe that proper to the complexity of the cloud, it will be complicated to achieve end-to-end security. New security techniques require to be developed and older security techniques required to be completely tweaked to be able to work with the clouds architecture. As the development of cloud computing technology is still at an early stage, and pave the way for additional research in this area. Cloud computing is clearly one of the most attractive technology areas of the current times due, at least in component to its cost-efficiency and flexibility. The surge in action and interest, there are significant, persistent concerns about cloud computing that are impeding the momentum and will finally compromise the vision of cloud computing as a new IT procurement model. Require of control is transparency in the cloud implementation. somewhat contrary to the original promise of cloud computing in which cloud implementation is not related. Because of today's supposed lack of control, larger companies are testing the waters with minor projects and less responsive data.

References

[1]. K. ValliMadhavi, R.Tamilkodi, R. Bala Dinakar,"Data StorageSecurity in Cloud Computing for Ensuring Effective and Flexible Distributed System", International Journal of Electronics Communication and Computer Engineering, 2012.

[2]. A.Kundu, C. D. Banerjee, P.Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[3]. Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C.,Kramer D. ,Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[4]. R.L.Grossman ,"The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202

[5]. B. R. Kandukuri, R.Paturi V, A.Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[6]. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.