A SURVEY PAPER ON ENSURING SECURITY IN CLOUD COMPUTING

Yogita gangboir[1], Praveen Shende[2], Tushar Kumar Vaidya[3]

[1,3]Department of Computer Science and Engineering, CSIT, Durg, (India)

[2]Assoistant Professor in Computer Science and Engg. Department, CSIT, Durg, (India)

ABSTRACT

Cloud computing means store the new technology around the world. It is the next generation of computer industry which plays a vital role in corporate business. Any type of users who want to do secure transmission of data or storage of data in any network. Cloud computing stores the data and share distributed resources in open environment thus it suffers from security problems. The objective of this paper is to ensure security on software as a service model for uploading and downloading data by end user in cloud computing.

Keywords: Cloud Computing, Infrastructure As A Service, Platform As A Service, Software As A Service, Security.

I. INTRODUCTION

Cloud computing is the new technology which provide different services and resources to users. In cloud computing users doesn't know how computation is done and storage is managed. There are three types of services – (Infrastructure as a service (IaaS), platform as a service (PaaS), software as a service(SaaS). The cloud service provider is responsible to manages a cloud and provide data storage services to different users. Cloud computing gives assurance to reduce all the operational and capital cost of the organizations and just focus on strategy of organization.

II. ABOUT CLOUD COMPUTING

For providing a secure cloud computing services, a major decision is to decide which type of cloud going to be implemented. There are four types of cloud deployment model – public, private, community and hybrid cloud.

2.1 Public Cloud

In public cloud model, it allows all users' access to the cloud via interfaces by using mainstream web browsers. It's work on pay-per-use model,. disadvantage of this model , it is less secure than other cloud models because This ensure to cloud users that all the applications and data accessed on the public cloud are not subjected to attackers. Therefore for trust and privacy concern it will not be good deal with Public clouds. Public cloud employs different techniques for resource optimization; since these services are transparent for end users and represent a potential threat to the security of the system. If a cloud provider runs several data centers, for instance, resources can be assigned in such a way that the load is uniformly distributed between all centers. Example of public cloud is Amazon web service (AWS), it is simple storage service which is form of IaaS type of cloud, and it offering the Google App Engine with provides a PaaS to its customers. The customer relationship management (CRM) solution Salesforce.com is the example of SaaS cloud service.

2.2 Private Cloud

In private cloud model, all the cloud services, applications and resources are managed by the organization itself. It is quite similar to intranet . private cloud model is secure than public cloud because of its specified internal exposure. The advantage of private cloud is that, the enterprise retains full control over data, security mechanism, and performance of the system.

2.3 Community Cloud

In community cloud model, is work on specific community of cloud consumer, it is similar to public cloud. Community Clouds are owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. The cloud infrastructure is provisioned for exclusive use of a specific community of consumers from organizations that have shared concerns.

2.4 Hybrid Cloud

In hybrid cloud model, it is the combination of power of the private and public models. Most of the organizations deploy their own cloud with their limited infrastructure to host their sensitive applications. When need for a big infrastructure and non-critical applications so it can be moved into the public cloud and critical applications could stay in their own internal cloud. It introduces the complexity of determining how to distribute applications across both a public and private cloud.

2.5 Architecture of Cloud Computing

Cloud computing is a traditional computing model, it is very important to understand the cloud's architecture. Because there is different definitions and architecture of cloud, all the enterprises is using different architecture. NIST (National Institute of Standards and Technology) summarizes the architecture of the cloud computing [4]. In this architecture there are five essentials characteristics, three service models and four deployment models.
Five essentials characteristics are:

- On-demand self-service- A consumer can unilaterally provision computing capabilities.
- Broad network access- Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
- Resource pooling- The provider's computing resources are pooled to serve multiple consumers, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- Rapid elasticity- Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.
- Measured service- Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service.

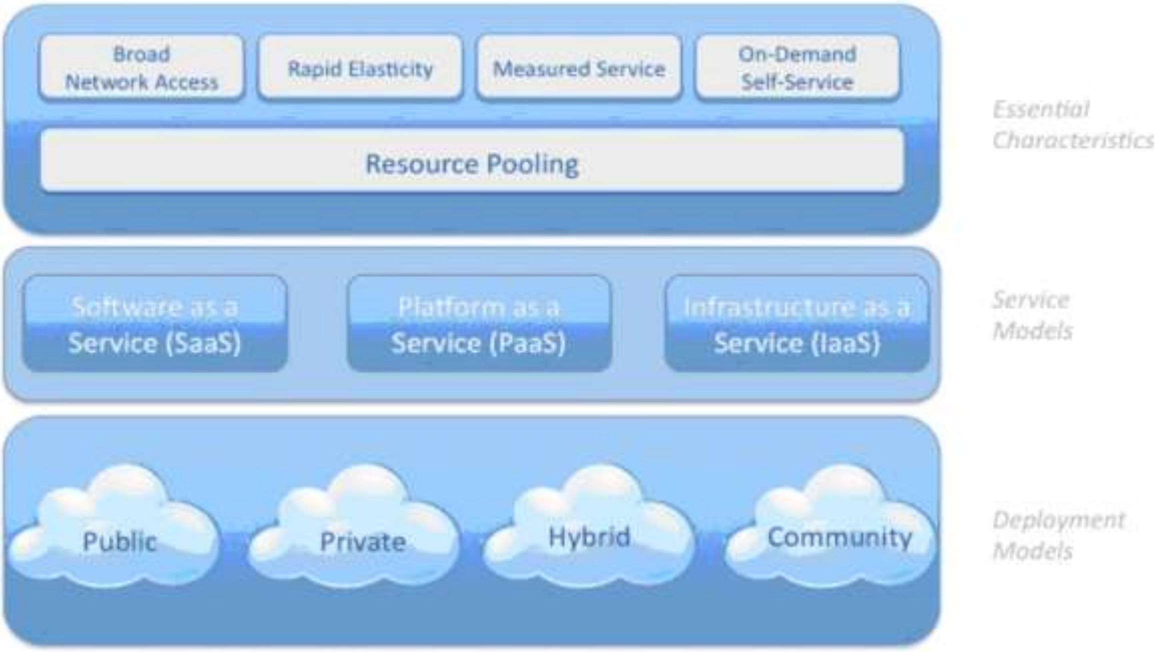


Figure 1: Architecture of Cloud Computing

Different services models are- Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (laaS).

- Software as a Service- In this service model consumer is only use to application provided by the cloud service provider running on the cloud infrastructure. In this Applications and computing resources as a web base application it act as an interface between application host and customer.
- Platform as a Service (PaaS) this model is consumer-created or acquired applications created by using different languages and supported by cloud provider. cloud infrastructure are does not control by the consumer, it has control with possible configured settings for application-hosting (e.g. Java runtime environment) and enables users to deploy their own applications within it.
- Infrastructure as a Service (IaaS) The consumer does not control or manage cloud infrastructure but has control over operating systems, storage, and deployed applications, and networking components (e.g., host firewalls). It is only cloud layer where the Cloud computing resources are only shared with contracted clients at a pay-per-use fee.

III. SECURITY CHALLENGES AND POLICY IN CLOUD COMPUTING

Cloud computing is a new computing model, regardless of the system's architecture or service's deployment is different from the traditional computing model[3].

3.1 Security Challenges In Cloud Computing Environment

- In the traditional model, it can be protect device user by dividing physical and logical security zones. It is difficult to clearly define the boundaries to protect the user devices.
- Security service challenge. Cloud service provider controlled all data, different services, networks and resources. So when security is something wrong, how to provide assurance that the service continues to be used, as well as the confidentiality of user data is particularly important.

- Protection. This is challenge to protect user data. It includes location of data stored, way of data storage, recovery of data, encryption and data integrity protection.
- In cloud computing model, many users dynamically changes and also services. So lead of user can not classify.
- The user's rights may be difficult to ensure because in cloud model, cloud service provider has many rights. So it becomes a problem that, how to balance the rights between the users and cloud service providers.
- Complexity of cloud computing. It is an important issue that how to ensure communications among the various subjects are security and integrity.
- Security benefits. There are definitely plenty of concerns regarding the inability to trust cloud computing due to its security issues. However, cloud computing comes with several benefits that address data security [9].

3.2 Policy in Cloud Computing

There are some security policy points [3]:

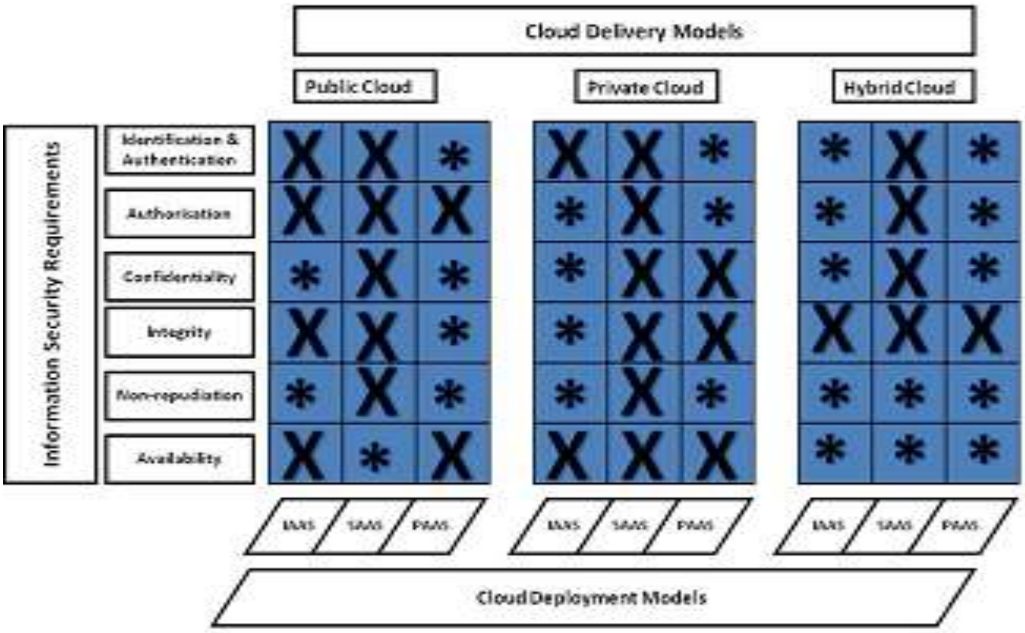
- Divided into multiple security domains in the cloud computing environment, different security domain operation must be mutual authentication, each security domain internal should have main map between global and local.
- Ensure that the user's connection and communications security with the SSL, VPN, PPTP, etc. Using license and allowing there are multiple authorizations among user, service owner and agents, to ensure user access to data securely.
- User data security assurance: according to the different user's requirements, different data storage protection should be provided. At the same time, the efficiency of data storage should be improving.
- Using a series of measure to solve the user dynamic requirements, including a complete single sign-on authentication, proxy, collaborative certification, and certification between security domains.
- Establishment of third-party monitoring mechanism to ensure that operation of cloud computing environment is safe and stable.
- The computing requested by service requestor, should carry out the safety tests, it can check whether they contain malicious requests to undermine the security rules.

IV. SECURITY REQUIREMENTS IN CLOUD COMPUTING

Cloud computing security should be guided in this manner to become an effective and secure technology solution. In Figure 2, cloud computing security requirements, is coupled with different cloud delivery model and deployment model. Here "X" denotes the mandatory requirements and an asterisk (*) denotes the optional requirements [9].

Different security requirements are:

- Authentication and Identification- It depending upon the type of cloud as well as the cloud delivery model. The specified users must be established first.
- Authorization –It ensures that referential integrity is maintained. It follows on in exerting control and privileges over process flows within Cloud computing. Authorization is maintained by the system administrator in a Private cloud.



	Public Cloud			Private Cloud			Hybrid Cloud		
	IAAS	SAAS	PAAS	IAAS	SAAS	PAAS	IAAS	SAAS	PAAS
Identification & Authentication	X	X	*	X	X	*	*	X	*
Authorisation	X	X	X	*	X	*	*	X	*
Confidentiality	*	X	*	*	X	X	*	X	*
Integrity	X	X	*	*	X	X	X	X	X
Non-repudiation	*	X	*	*	X	*	*	*	*
Availability	X	*	X	X	X	X	*	*	*

Figure 2: Cloud Computing Security Requirements

- Confidentiality- confidentiality plays an important role especially to maintain control over organizations' data situated across multiple distributed databases. It is a must when employing a Public cloud due to public clouds accessibility nature. Provide confidentiality of users' profiles and protecting their data, that is virtually accessed, allows for information security protocols to be enforced at various different layers of cloud applications.
- Integrity - The integrity is required when cloud domain mainly accessing the data. Therefore ACID (atomicity, consistency, isolation and durability) properties of the cloud's data should be robustly imposed across all Cloud deliver models.
- Non-repudiation - Non-repudiation can be obtained by applying the traditional e-commerce security protocols. Tokens are provisioning to data transmission within cloud applications.
- Availability – It is one of the most critical security requirements in Cloud model because it is a key decision factor when deciding among private, public or hybrid cloud vendors as well as in the delivery models.

V. RESULT

S. No.	Security Area	Current / possible solution
1	Authentication and Authorization	Open Authorization [8]
2	Availability	Data Dispersion
3	Data confidentiality	Attribute based Proxy Re-Encryption [6]
4	Virtual Machine Security	Reconfigurable distributed virtual machine[12]
5	Information Security	Risk Management Framework [16]

6	Network Security	Network Security for virtual machines [15]
7	Cloud standards	IEEE Cloud Computing Standard Study Group
8	Web application Security	Web Application Scanners
9	Backup	Agent less Method for data Backup and Recovery [1]

Table1 1: Current Solutions Available For Security Saas Service

VI. CONCLUSION

Cloud Computing is a new and growing paradigm where computing is considered as on-demand service. In this paper survey of cloud computing, we mainly described the different characteristics, service model and different security requirements. We also discussed about the security challenges & policies and some results in which some security area has different possible solutions.

REFERENCES

[1] Agentless Recovery. http://www.ibm.com/deceloperworks/cloud/liberary/cl-agentlessrecovery/[Accessed`; january 2013]

[2] Amazon EC2 Service http://aws.amazon.com/ec2

[3] Bhupesh Kumar Dewangan and Sanjay Kumar Baghel, "Survey on Ensuring Security Model of Cloud Computing", IJAIR, ISSN, 2278-7844.

[4] Bhupesh Kumar Dewangan and Praveen Shende, "Survey on User Behavior Trust Evaluation in Cloud Computing", International Journal of Science, Engineering and Technology Research (IJSETR), ISSN, 2278 – 7798 Volume 1, Issue 1, July 2012

[5] http://2012ieeetitles.blogpost.in/2012/07/a-secure-erasure-code-based-cloud.html.

[6] Jeong-Min et al, "Attribute based Proxy Re-Encryption for Data Confidentiality in Cloud Computing Environments", IEEE ACIS/JNU Int. Conference on Computers, Networks, Systems, and Industrial Engineering (CNSI 2011),Korea.

[7] "NIST Cloud Computing Standards Roadmap " NIST Special Publication 500-291, Version 2 (Supersedes Version 1.0, July 2011) .

[8] Pratap Murukutla, K.C. Shet, "Single Sign On for Cloud .In", International Conference on Computing Sciences,2012 IEEE DOI 10.1109/ICCS.2012.66.

[9] Ramgovind S, Eloff MM, Smith E, "The Management of Security in Cloud Computing",

[10] Rashmi,Dr.G.Sahoo and Dr. S. Mehfuz, "Securing Software as a Service Model of Cloud Computing: Issues and Solutions", International Journal on Cloud Computing: Services and Architecture (IJCCSA) , Vol.3, No.4, August 2013.

[11] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki and Sugata Sanyal, "A Survey on Security Issues in Cloud Computing".

[12] Song Fu, "Failure-aware resources management for high-availability computing clusters with distributed virtual machines", J parallel Distrib. Comput. 70(2010)384_393.

[13] Traian Andrei "Cloud Computing Challenges and Related Security Issues. A Survey Paper", http://www.cse.wustl.edu/~jain/cse571-09/ftp/cloud/index.html

[14] Vijay Sarathy, Purnendu Narayan and Rao Mikkilineni "Next generation Cloud Computing Architecture Enabling real-time dynamism for shared distributed physical infrastructure".

[15] Wu H, Ding Y, Winer C, Yao L, "Network Security for virtual machine in Cloud Computing", In 5th International conference on computer sciences and convergence information technology (ICCIT). IEEE Computer Society Washington, DC, USA, pp 18–21

[16] Xuan Zhang et al.(2010), "Information Security Risk Management Framework for the Cloud Computing Environments", 10th IEEE International Conference on Computer and Information Technology,Bradford, West Yorkshire,Uk.

Biographical Notes

Miss. Yogita Gangboir is presently pursuing M.Tech final year in Computer Science & Engineering Department from CSIT, Durg ,Chhattisgarh, India.

Mr. Praveen Shende working as Assistant Professor in Computer Science & Engineering Department, CSIT, Durg, Chhattisgarh, India.

Mr. Tushar Kumar Vaidya is presently pursuing M. Tech final year in Computer Science & Engineering Department from CSIT, Durg, Chhattisgarh, India.