Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

A Study and Survey of Security and Privacy issues in Cloud Computing

Sultan Ahmad
Department of Computer Science and Engineering
Glocal University
Saharanpur(U.P), India

Dr. M. Mazhar Afzal
Department of Computer Science and Engineering
Glocal University
Saharanpur(U.P), India

***Abstract*—The Cloud Computing, an emerging IT model that changed the way the individual and also organizations approach information technologies. It has some important characteristics such as on-demand self service, broad network access, resource pooling, rapid elasticity and measured services that enable organization to become agile. These characteristics of cloud computing has associated with some open issues like security, scalability, availability and interoperability. The privacy and security issues mostly come in cloud deployment and delivery models are major issues in modern cloud computing world. In this paper, issues of security and privacy in development and delivery are observed and analyzed. The new challenges to the cloud services and parameters of concern are explored because prevention is better than cure.**

Keywords—Cloud Computing; Data Security; Security and privacy; Service model;

I. INTRODUCTION

Cloud computing has become bone of IT industries in present decade. Industry has moved beyond the initial phases of cloud computing and now entered in consolidation phase. This is now realistic and practical acceptance of all models of clouds. It is a model in IT sector which is widely available. It provides a convenient network access to share pool of computing resources likes servers, storage, and application with minimal efforts in the minute of our fingertips. That is why Cloud Computing is now become very important and popular point of discussion for organizations and individuals, and found to be the subject of keen interest. Cloud adoption is now become a part of business strategies globally. All sectors of enterprises, research institutes, financial institutes, government agencies and education sectors are adopting cloud computing. The new emerging trends and technologies likes mobility, Big Data analysis and social media are the key reasons that enforces organization to move towards Cloud Computing.

Cloud computing provides great facilities to customers and business organizations to use applications without installation of additional resources, and access the data across the globe through internet. It made IT industries very easy in sharing IT resources likes Software resources, hardware resources, operating systems etc. over the internet by using Cloud Service models, Cloud storages and Cloud Providers. The famous public cloud service providers are Microsoft's Azure, Amazon's EC2 (Elastic Compute Cloud) and Google's suite of apps (Gmail, Google Docs, and Google Calendar etc.), Salesforce.com, IBM blue cloud etc. The IDC survey explains the best benefit of cloud computing with respect to speed and easiness in deployment [1].

Besides the great advantages of Cloud Computing, the security and privacy issues related to this are great concerns in adopting cloud computing. After several years of existence, still it needs a sufficient level of trust regarding security and privacy requirements. The Security has been identified as the top obstacle for cloud users. Some important security issues remain a topic of concern for both the cloud providers and the cloud customers. As per a survey by Microsoft and the United Nation's National Institute of Standards and Technology(NIST), which is a road map for security in Cloud Computing model is still the ICT executive's main concerns [1, 2]. In this study, we model the security and privacy problems and concerns and further classify them. These issues indicate that more research and innovation are required, specially on the part of cloud providers. In this context, a brief study is focused on 1) Cloud computing architecture, 2) Security and Privacy issues in cloud computing, 3) The techniques and strategies regarding security issues and finally 4) Conclusion and future work.

II. CLOUD COMPUTING AND ITS ARCHITECTURE

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. servers, storage, networks, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [2]. Cloud computing is built on virtualization, distributed computing, utility computing and service-oriented architecture. Cloud model enables consumers to hire IT resources as a service from a provider's cloud infrastructure [3]. In general, a cloud system and its customers practicing the client-server model. The customer request over network to compute systems and cloud provider perform operations in response to the request. The IT resources that make up a cloud infrastructure are deployed in data centers.

A. Essential Characteristics of Cloud Computing

As explained in the National Institute of Standards and Technology's definition, cloud model is composed of five essential characteristics, as shown in the table.1, below [2].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

TABLE 1. CLOUD COMPUTING ESSENTIAL CHARACTERISTICS

Characteristics	Specifications
On-demand self-service	A consumer can unilateral provision computing capabilities, such as server time and network storage, which are needed automatically without requiring human interaction with each service provider.
A broad network access	Capabilities are available over the network and accessed through standard mechanisms and promote use by heterogeneous thin or think client platforms (e.g., mobile phone, tablets, laptops, and workstations).
Resource pooling	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources.
Rapid elasticity	Capabilities can be elastically provisioned and released. In some cases, automatically to scale rapidly outward and inward as to commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
Measured service	The cloud system automatically controls and optimizes resource use by leveraging a metering capability at some level of abstraction and appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). The resources usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

B. Cloud Computing Deployment and Service model

The NIST[2] defines, cloud computing system as three services, and four deployment models respectively as depicted in figure 1.The cloud computing could have different forms, as per the need and situations. It is vital to decide which type of cloud to be selected.

Public Cloud is accessible and provisioned for open use by general public. The cloud infrastructure may be owned, managed and operated by any type of organization likes business, academic, or government or a combination of these. Its infrastructure locates on the premises of the cloud provider. In this model, there may be multiple tenants(consumers) who share common cloud resources. It can be free, subscription-based or provided with pay-per-use model respectively.

Private Cloud services is provided for exclusive use by a single organization which may have multiple consumers (business units, sub organizations). It can be either managed by organization itself, or by a third party or combination of them. The cloud services in this model are dedicated to cloud consumers only. That why it provides greater degree of privacy and control over cloud infrastructure, applications and data usage and other resources. The on-premise and externally-hosted are the two variants of private cloud. It is mainly adopted by large organizations.

Community Cloud is provisioned for exclusive use by community; those have shared interest and concerns. For example, mission, security requirements, policy and compliance considerations are communities that may share common goals or concerns. The organization participating in the community specially share the cost of the community cloud service. It may exist on or off premises. It offers a higher level of control and protection against external threats than a public cloud.

Hybrid Cloud which combines two or more individual clouds. The combination may be of public, private or community clouds. There may be many possible compositions of hybrid clouds. Hybrid cloud has different properties in terms of parameters, such as performance, cost, security etc. In a hybrid cloud environment, the component clouds are combined through the use of open or proprietary technology, such as interoperable standards, architectures, protocols, data formats, application programming interfaces (APIs), and so on. These uses of many technologies make possible data and application portability. The structure of hybrid cloud may change over time as component clouds join and leave the cloud system.

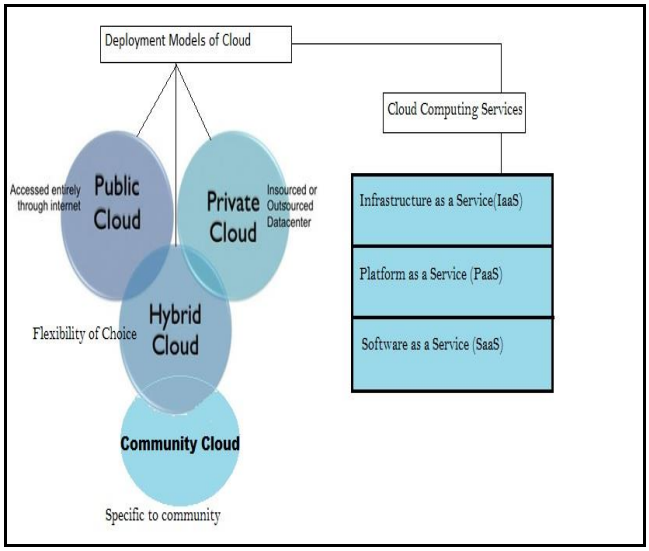

Fig. 1. Cloud Computing Deployment and Service Models

The Cloud Service model are classified by NIST in three cloud computing models. These three models are generally referred together as the SPI model. The selection of service models based on the cloud consumer requirement as they are of different capabilities and business objectives.

Software as a Service(SaaS): In this model, a cloud provider hosts an application centrally in the cloud and offers it to multiple cloud consumers for use as a service. The consumers do not own or manage any aspect of the cloud infrastructure. In SaaS, a given version of an application, with a specific configuration (hardware and software) typically provides service to multiple consumers by partitioning their individual sessions and data. SaaS applications execute in the cloud and usually do not need installation on consumer's devices. This enables a consumer to access the application on demand from any location and use it through a web browser on a variety of end-point devices. In this model, the cloud customer/consumers do not need to manage operating

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

systems, cloud infrastructure, networks, servers and storage. Some famous SaaS providers are Microsoft, Google etc.

Platform as a Service(PaaS): This model offers a cloud service generally includes compute, storage, and network resources along with platform software including an OS, a database, a programming framework, middleware, and tools to develop, test, deploy, and manage applications. PaaS enables application developers to design and develop cloud-based applications using the programming languages, the class libraries, and the tools supported by the cloud provider. PaaS offerings typically enable consumers to build highly-scalable cloud applications that can support a large number of end users. The elasticity and scalability are facilitated transparently by the cloud infrastructure. PaaS helps application testers to test the applications in various cloud-based environments. PaaS also enables application developers to publish or update the applications on the underlying cloud infrastructure. Further, PaaS enables application administrators to configure, monitor, and tune the cloud applications. Some of the PaaS providers are Google's App Engine and Force.com.

Infrastructure as a Service (IaaS): In this model, consumers hire IT resources, such as compute systems, storage capacity, and network bandwidth from a cloud service provider. The underlying cloud infrastructure is deployed and managed by the cloud service provider. Consumers can deploy and configure software, such as operating system (OS), database, and applications on the cloud resources. Typically, the users of IaaS are IT system administrators. IaaS can even be implemented internally by an organization, with internal IT managing the resources and services. IaaS pricing can be subscription-based or based on resource usage. Some IaaS providers are Amazon and GoGrid.

III. SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING

The security and privacy-related challenges in cloud computing are utmost important. There are numerous security issues for cloud computing as it encompasses a lot of IT technologies like networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management[4]. That is why, all security issues related to these systems and technologies are directly applicable to the cloud computing hierarchy. The privacy and security are two inherent issues in cloud computing environment due to their nature, which involve storing of unencrypted data on a machine owned and operated by someone other than the original owner of the data. This illustrated in the figure 2.

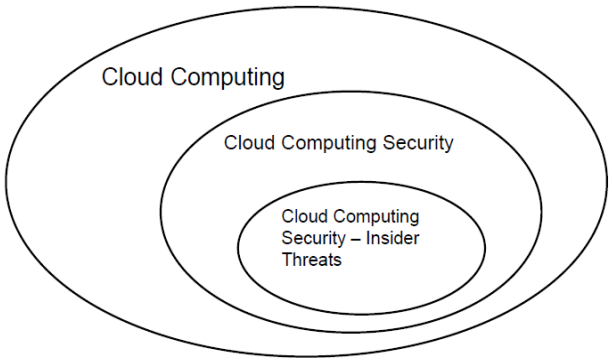

Fig. 2. Cloud Computing Security Framework

The Cloud Computing Security can be divided into mainly two categories: Data Security and Network Security.

Data Security means protecting data from unauthorized access, disclosure, use, disruption, modification, inspection, recording, or destruction from the unauthorized users. The Confidentiality, Integrity and Availability are the three key attributes of the Data Security. Beside these, the Authentication, Authorization and Auditing (AAA) are the other three aspects of Data Security. The challenges of data, and network securities of cloud computing environment are listed [5] in below table.

TABLE 2. CHALLENGES OF CLOUD COMPUTING IN DATA SECURITY AND NETWORK SECURITY

Relation	Security Issues	Affected Cloud Service
Data Security	Data Locality	SaaS, PaaS and IaaS
	Data Integrity	SaaS, PaaS and IaaS
	Data Segregation	SaaS, PaaS and IaaS
	Data Access	SaaS, PaaS and IaaS
	Data Confidentiality Issues	SaaS, PaaS and IaaS
	Data Breaches	SaaS and PaaS
	Reliability of Data Storage	SaaS and IaaS
	Data Center Operation	SaaS, PaaS and IaaS
	Data Sanitization	SaaS, PaaS and IaaS
Network Security	Application Vulnerabilities	SaaS, PaaS and IaaS
	Host and Network Intrusion	PaaS
	DoS(Denial of Service)	SaaS and PaaS
	Man In The Middle	SaaS, PaaS and IaaS
	IP Spoofing	SaaS and PaaS
	Port Scanning	SaaS and PaaS
	Packet Sniffing	PaaS

The security gradation can be done on security challenges related to each of these cloud models such as SaaS, PaaS, IaaS. The most integrated model, SaaS provides the greatest level of security as the cloud service provider is responsible for security measures. The PaaS, and IaaS, offer degrees of flexibility for clients to develop their own software, leave more gaps in security unless the user takes security measures into user's hands[6]. The more flexibility extends; the more additional security requirements are sought for cloud customers.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

The specific security and privacy challenges in cloud computing strategies require the development of advanced security technologies to tackle the issues which are tabulated in the table 3.

TABLE 3. SUMMARY OF SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING

No.	Issues	Sub Issues	Explanation of issue in Existing Literature Reference. No.
1	Loss of Control	Data loss and data breach	[7], [8]
		Data Storage and Transmission under multiple regional regulation	[9]
		Cheap data and Data Analysis	[10]
2	Virtualization related issues	New Access Context	[11]
		Attacks against Hypervisor	[11]
		VM Hijacking	[12]
		VM Hopping	[13], [14]
		VM Escape	[14]
		VM Mobility	[13]
		Dormant VMs	[11]
3	Multi-Tenancy related Issues		[15]
4	Lack of Transparency		[16]
5	Management Issues		[17]

IV. THE PROBABLE SOLUTIONS ON SECURITY AND PRIVACY ISSUES

The issues given in the table 3, can be categorized in view of their orientation. The loss of control, virtualization related issues and multi-tenancy related issues are technically-oriented. The lack of transparency and management issues are management-oriented. After review of these issues and their solutions across the literature survey, it is found that there are numerous solutions in respect of loss of control, virtualization and multi-tenancy related issues. These solutions are very much correlated in nature and need to be implemented in integrated way. But there is a lack of advanced solutions to deal with security and privacy issues with respect to the management prospective. The lack of transparency and management issues are to be resolved by further research investigations. The customer training is highly recommended in full understanding of when cloud services should be used needs to be a part of basic employee training in many jobs that involve managing information.

V. CONCLUSION

The issues and challenges currently inherent to the cloud indicate that there is more innovation needed specifically in cloud provider side. It has still having more room for improvement and innovations. Further in view of new demand of today's complex and diverse network, cloud security and issues should be addressed in continuous way. This will help companies to achieve more efficient use of ICT and accelerate the adoption of innovations and cloud computing.

REFERENCES

[1] F. Gens, "New IDC IT cloud services survey: top benefits and challenges," 2009; http://blogs.idc.com/ie/?p=730

[2] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011; http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[3] Abu Sarwar Zamani, Md Mobin Akhtar and Sultan Ahmad, "Emerging Cloud Computing Paradigm" International Journal of Computer Science, paper id 'IJCSI-2011-8-4-164' published in IJCSI Volume 8, Issue 4, July 2011, Mauritius.

[4] Krutz RL, Vines RD. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing; 2010 Aug 9.

[5] Subashini S, Kavitha V., " A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications. 2011 Jan 31; 34(1):1.

[6] Beulah S, Dhanaseelan FR., "Survey on security issues and existing solutions in cloud storage", Indian Journal of Science and Technology. 2016 Apr 14; 9(13):1–8.

[7] D. Sheppard, "Is loss of control the biggest hurdle to cloud computing?" 2014; http://www.itworldcanada.com/blog/isloss-of-control-the-biggest-hurdle-to-cloud-computing/95131.

[8] Top Threats Working Group,"The notorious nine: cloud computing top threats in 2013," 2013;https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.

[9] A. Murphy, "Storing data in the cloud raises compliance challenges," 2012; http://www.forbes.com/sites/ciocentral/2012/01/19/storing-data-in-the-cloud-raises-compliance-challenges/.

[10] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcingcomputation without outsourcing control," in Proceedingsf the 2009 ACM Workshop on Cloud Computing Security, Chicago, IL, 2009, pp. 85-90.

[11] Virtualization Special Interest Group and PCI Security Standards Council, "PCI DSS Virtualization Guidelines," 2011; https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf.

[12] A. Jasti, P. Shah, R. Nagaraj, and R. Pendse, "Security in multi-tenancy cloud," in Proceedings of 2010 IEEE International Carnahan Conference on Security Technology (ICCST), San Jose, CA, 2010, pp. 35-41.

[13] D. Hyde, "A survey on the security of virtual machines," 2009; http://www.cs.wustl.edu/~jain/cse571-09/ftp/vmsec.pdf

[14] K. Owens, "Securing virtual compute infrastructure in the cloud," Savvis Inc., Town and Country, MO, 2009.

[15] H. Aljahdali, P. Townend, and J. Xu, "Enhancing multi-tenancy security in the cloud IaaS model over public deployment," in Proceedings of 2013 IEEE 7th International Symposium on Service Oriented System Engineering (SOSE), Redwood City, CA, 2013, pp. 385-390.

[16] W. Pauley, "Cloud provider transparency: an empirical evaluation," IEEE Security & Privacy, vol. 8, no. 6, pp. 32-39,2010.

[17] S. Luo, Z. Lin, X. Chen, Z. Yang, and J. Chen, "Virtualization security for cloud computing service," in Proceedings of 2011 International Conference on Cloud and Service Computing(CSC), Hong Kong, 2011, pp. 174-179.