IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

A Review on the Security Issues in Cloud Computing Models

Er. Ubeeka Jain[1], Ritika Trivedi[2]

Department of Computer Science & Engineering, RIEIT RailMajra[1]

Abstract: As predicted, computing has become the fastest growing services in recent years and has acquired a new dimension in the form of cloud computing. It is greatly influenced by merging of internet with computing, sharing of resources and combining the advancements in technologies that paved to various cloud offerings. The fundamental guidelines of cloud computing model are computing, storage, Security & programming as an administrator. But the size of computation & demand for higher computation is growing very rapidly which is causing an uneven and heavy workload on cloud resources. Due to this rapidly increase of data, there is the need of security as per the increasing demand. But due to this increasing cloud demand, security of cloud data has become a problem for the future. So, here we are discussing about the security issues in the cloud data, service and deployment models.

Keywords: Cloud Computing, Cloud Security Issues, Cloud Service model, Cloud Deployment model.

I. INTRODUCTION

Cloud computing is a newly emerging technique which provides online computing resources and storage. In the cloud computing environments we have to deal with different fundamentals like virtualization, interoperability, scalability and the quality of service and the delivery models of the cloud system [1]. By providing all these fundamentals, the main goal of cloud computing is to make a better use of distributed resources, achieving higher throughput and supporting the capability of solving large scale problems [2].

Therefore, in order to achieve these goals and to handle such large resources pool different techniques are required for optimizing and improving the effectiveness of services and providing a satisfactory level of performance for users. Many researches and studies have been carried out recently about cloud computing challenges and issues such as scheduling problem [3][4], cloud security [5] and performance etc.

One of the most important issues in the field of cloud computing is huge data and its security. Many Non-Industry representatives, government and non-profit organisations noticed various security issues in services rendered by cloud computing. CSA identified 16 issues out of which information management and data security particularly data manipulation, data confidentiality, integrity and availability are the areas that need research (Cloud Security Alliance 2009) [6].

In this paper, we are presenting a brief overview on the various security issues of data storage, cloud deployment model and cloud service model.

Rest of the paper is organized as follows: Section II describes the characteristics of cloud computing; Section III presenting various security issues in cloud environment and Section IV concludes the paper.

II. CHARACTERISTICS OF CLOUD COMPUTING

A. Broad Network Access

Capabilities available in cloud can be accessed by wide variety of devices. Tablets, smart phones, Laptops and desktop can be used to access the resources. Devices used for accessing may have thin/thick client platforms.

B. Rapid Elasticity

Cloud computing provide the great elasticity capabilities by providing the unlimited resources. Users can demand the resources offered at the time of required and same amy be released once the requirement is over. Even though, providers also have the limited resources but for consumers it appears as unlimited resources are offered.

C. Measured service

Being the utility model, services consumed by the consumers must be measured for the billing purpose. Cloud systems provide the capability to measure the quantity of resources used. Majority of the services offered are measuring the resources such as Virtual machine, Memory, storage, number and type of CPU accessed and the duration of their usage. This measurement helps in generating the bill as per the usage reported. Measured services must be transparent for both the user and the provider to avoid any kind of contention, later on.

D. Agility

Cloud computing is much sought in the business circle due to its agility. In traditional based system procuring the resources require a lengthy procedure of getting the requirement approved, inviting the quotation, selecting the best quotation, ordering and delivering. In case of cloud computing resources can be demanded at any time and the same will be available to the users. users in hours instead of in week and month in case of traditional system. This rapid provisioning of the resources is knows as agility and it reduces downtime and helpful in improving the customers satisfaction and growing business advantage [7].

E. Resource Pooling

Cloud computing works on distributed model where resources are distributed throughout the data center. In case of excessive need of resources, they can be pooled with different physical and virtual resources to serve

multiple consumers. These resources are assigned and reassigned according to customer demand. Locations, from where resources are pooled are not known to the consumer, user can only specify location at higher level of abstraction (e.g. country, state or data center). Examples of resources that can be pooled include storage, processing, memory and network bandwidth.

III. CLOUD SECURITY ISSUES

Though security issues ranked as one of the top challenges in the adoption of cloud it is still vague which issues are particular to cloud computing. Applications running on or being developed for cloud computing platforms pose various security and privacy challenges depending on the underlying delivery and deployment models. The demand for cloud computing has forced the development of new market offerings, representing various cloud service and delivery models. These models significantly expand the range of available options, and task organizations with dilemmas over which cloud computing model is developed.

A. Security Issues in Cloud Delivery Model

The three key cloud delivery models are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In SaaS, the cloud providers enable and provide application software as on-demand services. Because clients acquire and use software components from different providers, crucial issues include securely composing them and ensuring that information handled by these composed services need to be well protected.

PaaS enables programming an environment that involves a broad collection of application infrastructure services such as database services, business process management and application platform. The programming environments used have an impact on the application framework. It poses constraints on which services the application can request from an Operating System. For example, a PaaS environment might limit access to well-defined parts of the file system, thus requiring a fine-grained authorization service.

In IaaS, the cloud provider supplies a set of virtualized infrastructural components such as Virtual Machines (VMs) and storage on which customers can build and run applications. The application will eventually reside on the VM and the virtual operating system. Issues such as trusting the VM image, hardening hosts, and securing inter-host communication are critical areas in IaaS [8].

B. Security Issues in Cloud Deployment Model

The Figure 1 depicts the security issues that fall under the various layers of cloud framework.

Cloud deployment models include public, private, community, and hybrid clouds. Public clouds are external or publicly available cloud environments that are accessible to multiple tenants, whereas private clouds are typically tailored environments with dedicated virtualized resources for particular organizations. Similarly, community clouds are tailored for particular group of customers. The analysis of cloud computing models has shown that public cloud deployment model stay dominant and keep expanding further. Private and Hybrid deployment models are going to stay for years ahead but their market share is going to continuously drop.

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. The organization and designated users have access to operate on a specific Private cloud [9].

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are subjected to malicious attacks [10].

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network [11]. Hybrid cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open framework that allows interfaces with other management systems. It can also describe configurations combining virtual and physical, collocated assets for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter.

C. Security of Data Deployed in Cloud

Data in the cloud refers to data while it is being transmitted, stored or processed by a Cloud Service Provider (CSP) [12]. The organization should apply the same data classification used when the data is resident within the organization and therefore apply necessary cryptographic security requirements to data stored, transmitted or processed by a CSP. Cryptographic security controls cannot be replaced by CSP Service Level Agreements. Once data is safely transmitted to a CSP, it should be stored, transmitted and processed in a secure way [13].

The emergence of cloud computing has made critical customer and enterprise data to be handled by third-party cloud providers. The environment provides a multi-tenant shared computing and storage environments which highlights the need to turn towards encryption to secure the customers and enterprise data. Storage, movement, and processing of digital information are commonly discussed in terms of "Data at Rest," "Data in Transit," and "Data in Use."

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

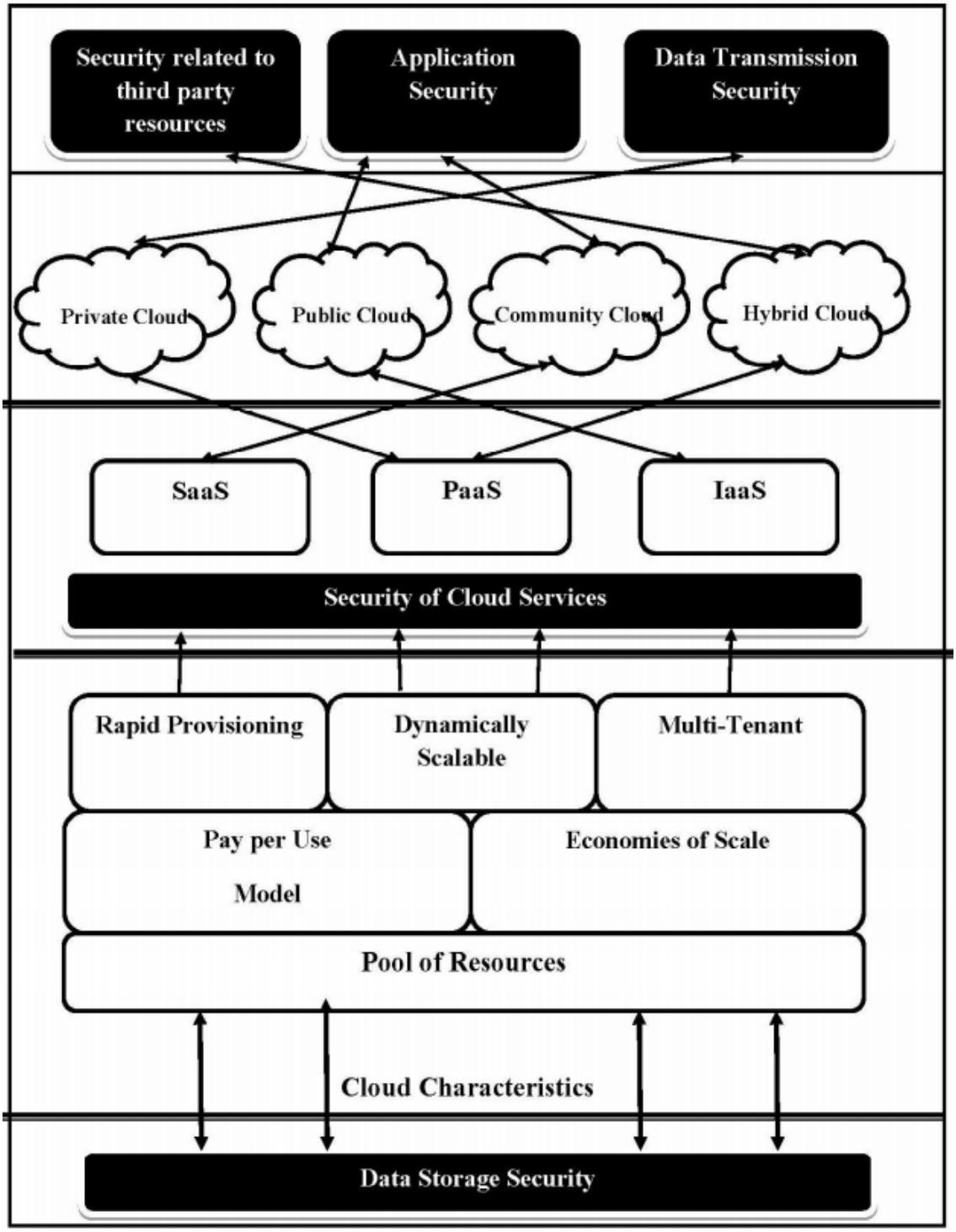

Figure 1.1 Security issues under various layers of cloud computing

Encryption is one of the most effective and primary data protection techniques available today (Cloud Security Alliance 2009) [6]. For encryption to be useful, encryption keys must be properly managed and protected. The application of encryption mechanisms can similarly be considered for each of the three states. When enterprises and individuals move their data and applications to the cloud, protection of their confidential information such as company secrets and sensitive information in transit, at rest, and in use is critical. When cryptography is used to protect valued data, the risk is transferred from the content to the keys. Once encryption has occurred, protection of cryptographic keying material need to be secured. Furthermore, the emergence of cloud delivery of security services means that encryption capabilities cannot only be used to secure data in the cloud, but can also be offered through the cloud to enable organizations of all kinds to more easily protect sensitive data [14].

It is clear that encryption is essential to cloud computing. Various questions arise and the one among that target who provides these encryption controls. The cloud customer's are expected to encrypt the data before moving it to a

DOI 10.17148/IJARCCE.2015.41119

public cloud. If the customer cannot do these themselves, then encryption should be outsourced to a security service offered by the cloud provider or vendors who offer specialized encryption for cloud environments. Protocols such as SSL or IPSec are used for transmitting data over the internet. The functional high-level description prefers to protect data by presenting encrypted data in a way that enables it to be processed. It discusses about the ability to perform operations on ciphertext without the need to decrypt it. Clearly such a solution is extremely desirable for cloud computing. Understanding the security and privacy risks of various cloud computing models and developing efficient and effective solutions are critical for its success. Although clouds allow customers to avoid start-up costs, reduce operating costs, and increase their agility by immediately acquiring services and infrastructural resources when needed, their unique architectural features also raise various security and privacy concerns [15][16].

IV. CONCLUSION

Cloud Computing has attracted several enterprises due to various benefits that it offers in the form of greater resiliency, faster deployment, low costs or pay per usage, on demand security control and detection of system tampering. The major issue identified in cloud computing is its security attribute, which affects its growth. In this paper, we have presented a brief overview on the various security issues of data storage, cloud deployment model and cloud service model. These issues also shown in figure 1. So, there is the need more advancement in the concepts of cloud computing to make it make it more useful in the future technology.

REFERENCES

[1]. Rimal, Bhaskar Prasad, Eunmi Choi, and Ian Lumb. "A taxonomy and survey of cloud computing systems."In INC, IMS and IDC,.NCM'09. Fifth International Joint Conference on, pp. 44-51. IEEE, 2009.

[2]. Jadeja, Yashpalsinh, and KiritModi. "Cloud computing-concepts, architecture and challenges."In Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on, pp. 877880. IEEE, 2012.

[3]. S. Sotiriadis, N. Bessis, and N. Antonopoulos. "Towards inter-cloud schedulers: A survey of meta-scheduling approaches." In P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2011 International Conference on, pp. 59-66. IEEE, 2011.

[4]. Dutta, Kushal, Ramendu Bikash Guin, Sayan Chakrabarti, Sourav Banerjee, and Utpal Biswas. "A smart job scheduling system for cloud computing service providers and users: modeling and simulation." In Recent Advances in Information Technology (RAIT), 2012 1st International Conference on, pp. 346-351.IEEE, 2012.

[5]. Kandukuri, Balachandra Reddy, V. Ramakrishna Paturi, and Atanu Rakshit. "Cloud security issues." In *Services Computing, 2009. SCC'09. IEEE International Conference on*, pp. 517-520. IEEE, 2009.

[6]. Cloud Security Alliance 2009, https://cloudsecurityalliance.orn/ csaguide.pdf

[7]. Adabi, Sahar, Ali Movaghar, and Amir Masoud Rahmani. "Bi-Ievel fuzzy based advanced reservation of Cloud workflow applications on distributed Grid resources." The Journal of Supercomputing 67.1 (2014): 175-218.

[8]. Subashini, Subashini, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." *Journal of network and computer applications* 34, no. 1 (2011): 1-11.

[9]. Yarter, Lawrence C. "Private cloud delivery model for supplying centralized analytics services." *IBM Journal of Research and Development* 56, no. 6 (2012): 10-1.

[10]. Foster, Ian, Yong Zhao, Ioan Raicu, and Shiyong Lu. "Cloud computing and grid computing 360-degree compared." In *Grid Computing Environments Workshop, 2008. GCE'08*, pp. 1-10. Ieee, 2008.

[11]. Idziorek, Joseph, and Mark Tannian. "Security analysis of public cloud computing." *International Journal of Communication Networks and Distributed Systems* 9, no. 1-2 (2012): 4-20.

[12]. Kaufman, Lori M. "Data security in the world of cloud computing." *Security & Privacy, IEEE* 7, no. 4 (2009): 61-64.

[13]. Abadi, Daniel J., Samuel R. Madden, and Nabil Hachem. "Column-stores vs. row-stores: how different are they really?." In *Proceedings of the 2008 ACM SIGMOD international conference on Management of data*, pp. 967-980. ACM, 2008.

[14]. Gartner Hype Curve 2014, www.gartnercom/technology/ research/ hype-cycles/.

[15]. Ren, Kui, Cong Wang, and Qian Wang. "Security challenges for the public cloud." *IEEE Internet Computing* 1 (2012): 69-73.

[16]. Sakr, Salam, An Liu, Daniel M. Batista, and Mohammad Alomari. "A survey of large scale data management approaches in cloud environments."*Communications Surveys & Tutorials, IEEE* 13, no. 3 (2011): 311-336.

DOI 10.17148/IJARCCE.2015.41119