Cloud Computing: Security Issues and Challenges

Nazia Majadi

Abstract— Cloud computing uses the internet and central remote servers to maintain data and applications. It allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. The appearance of cloud computing has made a tremendous impact on the Information Technology (IT) industry over the past few years. Recently IT industry needs Cloud computing services to provide best opportunities to real world. Cloud computing is in initial stages, with many issues still to be addressed. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment. The objective of this paper is to introduce a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types..

Index Terms— *Cloud Computing, Information Technology (IT), Information as a service (IaaS), Infrastructure, Platform as a service (PaaS), Scalability, Software as a service (SaaS).*

1 Introduction

According to the National Institute of Standards and Technology (NIST) definition [3] Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The name comes from the use of a cloud-shaped symbol [4] as an abstraction for the complex infrastructure it contains in system diagrams (see figure 1).

Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. In the last few years, cloud computing [6] received considerable attention, as a promising approach for delivering Information and Communication Technologies (ICT) services.

With the fast development of processing, storage technologies, the sensation of the Internet, and computing resources have become cheaper, more powerful and more universally available than ever before. This technological trend has enabled the realization of a new computing model called cloud computing. From the past few years, the cloud computing has made a tremendous impact on the Information Technology (IT) industry, where large companies such as Google,
IBM, Amazon and Microsoft struggle to provide more powerful, reliable and cost-efficient cloud platforms, and business enterprises seek to find new paradigm in their business models [16].

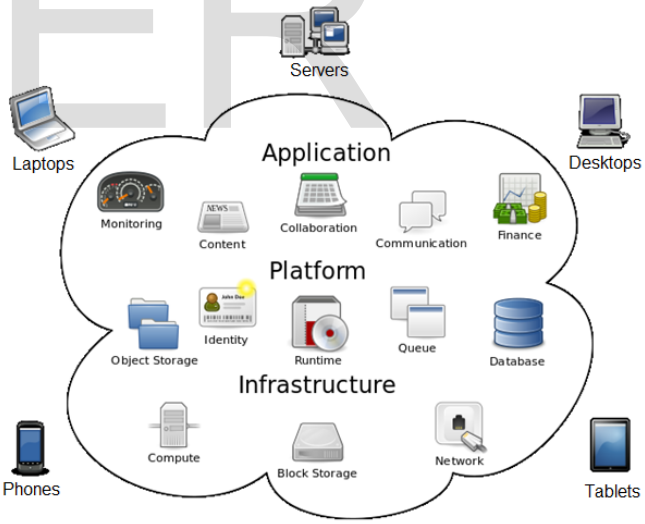

Figure 1: A logical diagram of Cloud Computing [4].

But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloud computing as depicted in figure 2.

From one point of view, security could improve due to centralization of data and increased security-focused re-

• *Nazia Majadi has completed her MSc in Computer Science and Engineering from Bangladesh University of Engineering and Technology in 2012. She is currently working as a Lecturer in the department of Computrer Science and Engineering, Military Institute of Science and Technology (MIST). E-mail: nazia_majadi@yahoo.com*

sources. On the other hand concerns persist about loss of control over certain sensitive data, and the lack of security for stored kernels entrusted to cloud providers. If those providers have not done good jobs securing their own environments, the consumers could be in trouble. Measuring the quality of cloud providers' approach to security is difficult because many cloud providers will not expose their infrastructure to customers. This work is a survey more specific to the different security issues and the associated challenges that has emanated in the cloud computing system.

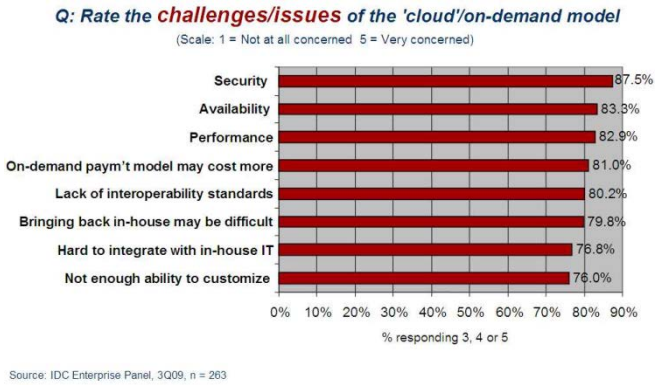

Figure 2: Results of IDC survey ranking security challenges, 2010 [1].

This paper is organized as follows. Section 2 highlights a brief review of literature on security issues in cloud computing. Security issues of cloud implementation and cloud computing deployment methods are described in Section 3. Section 4 deliberates on associated cloud computing challenges, and Section 5 presents the conclusion.

2 Related Work

Several studies have been carried out relating to security issues in cloud computing. Like, Gartner [7] identified seven security issues that need to be addressed before enterprises consider switching to the cloud computing model. They are as follows: (i) privileged user access - information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications first to test the water; (ii) regulatory compliance - clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by third party organizations that check levels of security and providers that don't (iii) data location – depending on contracts, some clients might never know what country or what jurisdiction their data is located (iv) data segregation - encrypted information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be deployed by the provider. (v) recovery - every provider should have a disaster recovery protocol to protect user data (vi) investigative support - if a client suspects faulty activity from the provider, it may not have many legal ways pursue an investigation (vii) long-term viability - refers to the ability to retract a contract and all data if the current provider is bought out by another firm. The Cloud Computing Use Case Discussion Group discusses the different Use Case scenarios and related requirements that may exist in the cloud model. They consider use cases from different perspectives including customers, developers and security engineers [8]. ENISA investigated the different security risks related to adopting cloud computing along with the affected assets, the risks likelihood, impacts, and vulnerabilities in the cloud computing may lead to such risks [10]. In 2009, Balachandra et al discussed the security SLA's specification and objectives related to data locations, segregation and data recovery [16]. In 2010, Bernd et al discussed the security vulnerabilities existing in the cloud platform. The authors grouped the possible vulnerabilities into technology-related, cloud characteristics-related, security controls related [13]. Subashini et al discuss the security challenges of the cloud service delivery model, focusing on the SaaS model [17]. Ragovind et al discussed the management of security in Cloud computing focusing on Gartner's list on cloud security issues and the findings from the International Data Corporation enterprise [15]. Morsy et al investigated cloud computing problems from the cloud architecture, cloud offered characteristics, cloud stakeholders, and cloud service delivery models perspectives in 2010[14]. A recent survey by Cloud Security Alliance (CSA)&IEEE indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers. It also details that cloud computing is shaping the future of IT but the absence of a compliance environment is having dramatic impact on cloud computing growth [13]. Although there are several studies those have been carried out relating to security issues in cloud computing, but this work presents a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing deployment types and the service delivery types.

3 Security Issues

3.1 Cloud Computing Model

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand as depicted in figure 3. The Cloud Computing model has three main deployment models which are:

3.1.1 Private Cloud

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 to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud [18].

3.1.2 Public Cloud

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. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization [11]. 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 not subjected to malicious attacks.

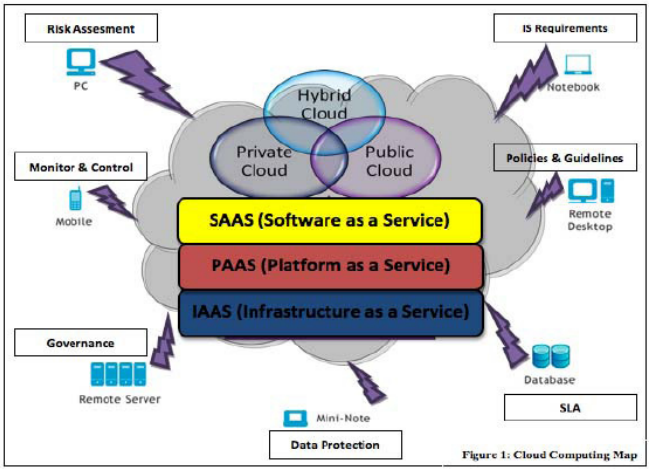

Figure 3: Cloud deployment model [1]

3.1.3 Hybrid Cloud

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 [14]. It provides virtual IT solutions through a mix of both public and private clouds. 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 architecture that allows interfaces with other management systems. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. 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.

3.2 Cloud Computing Services

Cloud computing services are available across the entire computing spectrum. The basic services of cloud have been considered as the following.

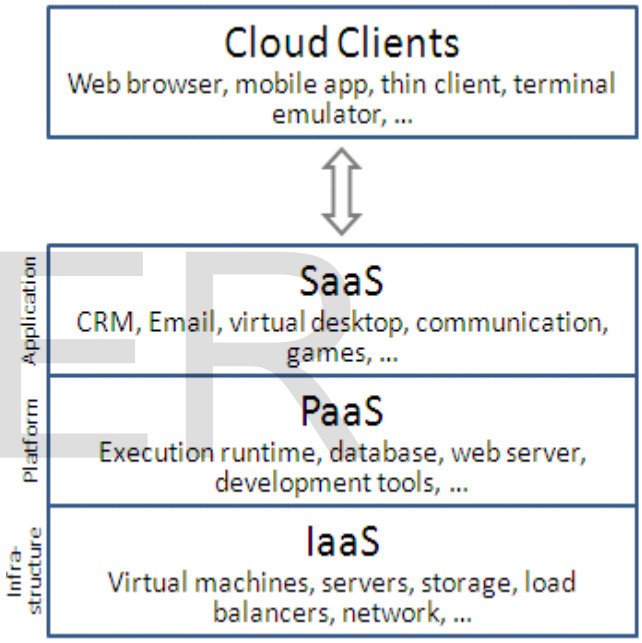

Figure 4: Basic three cloud computing services with cloud clients [4].

***Software as a service (SaaS)*:** SaaS reassign programs to millions of users all the way through browser. For user, this can save some cost on software and servers. For Service provider's, they only need to maintain one program, this can also saves space and cost. SaaS provider naturally hosts and manages a given application in their own or leased datacenters and makes it available to multiple tenants and users using the Web.

***Platform as a Service (PaaS)*:** PaaS is an application development and deployment platform provided as a service to developers over the Web. Middleman's equipment can be used to develop programs and transfer it to the end users through internet and servers. The cost and complexity of development and deployment of applica-

tions can be reduced to a great extent by developers by using this service. Thus the developers can reduce the cost of buying and reduce the complexity of managing the required Infrastructure. It provides all of the services essential to support the complete life cycle of building and delivering web applications and all the services entirely available from the Internet. This platform consists of infrastructure software, a database, middlware, and development tools.

***Infrastructure as a Service (IaaS)*:** IaaS is the delivery of associated software and hardware as a service. Hardware like server, storage and network, and associated software like operating systems, virtualization technology and file system. It is an evolution of traditional hosting to allow users to provide resources on demand and without require any long term commitment. Different PaaS services, the IaaS provider does very little management other than keep the data center operational and end-users must deploy and manage the software services themselves-just the way they would in their own data center [16].

4 Cloud Computing Challenges

The current adoption of cloud computing is associated with numerous challenges because users are still skeptical about its authenticity. The major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follows:

A. **Security:** It is clear that the security issue has played the most important role in hindering Cloud computing acceptance. There exists no doubt that putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with. For example, hackers can use Cloud to organize botnet as Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack [15].

B. **Costing Model:** Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication, i.e. the cost of transferring an organization's data to and from the public and community Cloud and the cost per unit of computing resource used is likely to be higher. This problem is particularly prominent if the consumer uses the hybrid cloud deployment model where the organization's data is distributed amongst a number of public/private (in-house IT infrastructure)/community clouds. Intuitively, on demand computing makes sense only for CPU intensive jobs [15].

C. **Charging Model:** The elastic resource pool has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions of static computing. Moreover, an instantiated virtual machine has become the unit of cost analysis rather than the underlying physical server. For SaaS cloud providers, the cost of developing multitenancy within their offering can be very substantial. These include: redesign and redevelopment of the software that was originally used for single-tenancy, cost of providing new features that allow for intensive customization, performance and security enhancement for concurrent user access, and dealing with complexities induced by the above changes. Therefore, a strategic and viable charging model for SaaS provider is crucial for the profitability and sustainability of SaaS cloud providers [15].

D. **Service Level Agreement (SLA):** Although cloud consumers do not have control over the underlying computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources when consumers have migrated their core business functions onto their entrusted cloud. Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers. The very first issue is the definition of SLA specifications in such a way that has an appropriate level of granularity, namely the tradeoffs between expressiveness and complicatedness, so that they can cover most of the consumer expectations and is relatively simple to be weighted, verified, evaluated, and enforced by the resource allocation mechanism on the cloud. In addition, different cloud offerings (IaaS, PaaS, and SaaS) will need to define different SLA metaspecifications. This also raises a number of implementation problems for the cloud providers. Furthermore, advanced SLA mechanisms need to constantly incorporate user feedback and customization features into the SLA evaluation framework [18].

E. **Cloud Interoperability Issue:** Currently, each cloud offering has its own way on how cloud clients/applications/users interact with the cloud, leading to the "Hazy Cloud" phenomenon. This severely hinders the development of cloud ecosystems by forcing vendor locking, which prohibits the ability of users to choose from alternative vendors/offering simultaneously in order to optimize resources at different levels within an or-

ganization. More importantly, proprietary cloud APIs makes it very difficult to integrate cloud services with an organization's own existing legacy systems (e.g. an on-premise data centre for highly interactive modeling applications in a pharmaceutical company).The primary goal of interoperability is to realize the seamless fluid data across clouds and between cloud and local applications. There are a number of levels that interoperability is essential for cloud computing. First, to optimize the IT asset and computing resources, an organization often needs to keep in-house IT assets and capabilities associated with their core competencies while outsourcing marginal functions and activities (e.g. the human resource system) on to the cloud. Second, more often than not, for the purpose of optimization, an organization may need to outsource a number of marginal functions to cloud services offered by different vendors. Standardization appears to be a good solution to address the interoperability issue. However, as cloud computing just starts to take off, the interoperability problem has not appeared on the pressing agenda of major industry cloud vendors [15].

5 Conclusion

Cloud Computing emerged as a major technology to provide services over the Internet in easy and efficient way. The main reason for possible success of cloud computing and vast interest from organizations throughout the world is due to the broad category of services provided with cloud. The cloud computing is making the utility computing into a reality. The current technology does not provide all the requirements needed by the cloud computing. There are many challenges to be addressed by the researchers for making cloud computing work well in reality. Some of the challenges like security issues are very much required for the customers to use the services provided by the cloud. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

References

[1] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." *Platform Computing*, pp6, 2010.

[2] Arnold S., "Cloud computing and the issue of privacy." *KM World*, pp14-22. Available: www.kmworld.com [Aug. 19, 2009].

[3] Available from: *http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf*. Last visited on the 12th November, 2012.

[4]Available from: *http://en.wikipedia.org/wiki/Cloud_computing*. Last visited on the 15th November, 2012.

[5] Balachandra R. K., Ramakrishna P. V. and Rakshit A., "Cloud Security Issues." In PROC '09 IEEE International Conference on Services Computing, 2009, pp 517-520.

[6] Bechtolsheim A. (2008). Cloud Computing and Cloud Networking. *Talk at UC Berkeley.*

[7] Brodkin J., "Gartner: Seven cloud-computing security risks." *Infoworld*, Available: <http://www.infoworld.com/d/security-central/gartner-seven cloudcomputingsecurity-risks-853?page=0,1> [Dec. 13, 2012].

[8] Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010.

[9] Cloud Security Alliance (CSA). Available: http://www.cloudsecurityalliance.org [Jan. 11, 2013].

[10]ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security." Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud computingrisk-assessment [Jul. 10, 2010].

[11] Gens F., "New IDC IT Cloud Services Survey: Top Benefits and Challenges", *IDC eXchange*, Available: <http://blogs.idc.com/ie/?p=730> [last visited on Jan. 9, 2013].

[12] Global Netoptex Incorporated. "Demystifying the cloud. Important opportunities, crucial choices." pp4-14. Available: http://www.gni.com [last visited on Dec. 13, 2012].

[13] Grobauer B., Walloschek T. and Stöcker E., "Understanding Cloud Computing Vulnerabilities," *IEEE Security and Privacy*, vol. 99, 2010.

[14] Morsy M. A., Grundy J. and Müller I., "An Analysis of the Cloud Computing Security Problem" In PROC APSEC 2010 Cloud Workshop. 2010.

[15] Ramgovind S., Eloff M. M., Smith E., "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010.

[16] Reddy V. K, Rao B. T., Reddy L. S. S, and Kiran P.S. (2011). Research Issues in Cloud Computing. *Global Journal of Computer Science and Technology*. 11 (11), p59-64.

[17] Subashini S., and Kavitha V., "A survey on security issues in service delivery models of cloud computing." *J Network Comput Appl* doi:10.1016/j.jnca.2010.07.006. Jul., 2010.

[18] Weinhardt C., Anandasivam A., Blau B., and Stosser J., "Business Models in the Service World." *IT Professional*, vol. 11, pp. 28-33, 2009.