A study on Cloud computing and emerging IT platforms: Security and challenges

Author: Rebeka Tanij Tania, B.Sc., M.S. (CSE, University of Dhaka)
PhD Student, Islamic Institute of Technology (IUT)
Assistant Professor, BGMEA University of Fashion & Technology

rebeka@buft.edu.bd, Mobile No. +8801712854323

Abstract: The cloud computing exhibits, remarkable potential to provide cost effective, easy to manage, elastic, and powerful resources on the fly, over the Internet. The cloud computing rises the capabilities of the hardware resources by optimal and shared utilization. It reduces cost and complexity of service provider by means of capital and operational cost. 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. Another aim is to identify security challenges for adopting cloud computing and solutions from real world for the challenge that do not have proper mitigation strategies identified through literature review.

Keywords: Software as a Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service(IaaS), private cloud, public cloud.

1. INTRODUCTION:

Cloud computing has experienced a great deal of interest in both academia and industry in recent years. With an estimated industry size of $131B, there is little doubt that it is both a successful technology and business model. By combining technologies such as virtualization, web APIs, and fast networks, cloud technology enables the provisioning and rental of computer infrastructure over the Internet. Similarly, by offering business advantages such as elasticity, the ability to defer capital expenditures, and the ability to outsource IT administration costs, cloud businesses provide many customers a valuable service. Cloud computing services can be broadly classified into three categories based on the level of abstraction of computing resources they provide. At the highest level are Software-as-a-Service (SaaS) clouds, which provide complete software applications; Platform-as-a-Service (PaaS) clouds, which provide language runtimes and support libraries; and, finally, Infrastructure-as-a-Service (IaaS) clouds, which provide generic computing infrastructure resources such as virtual machines and key-value object storage[1][2]. Cloud computing infrastructure can be public, meaning that it is shared among multiple, mutually distrustful tenants, or it can be private, meaning that all resources are reserved for one tenant exclusively. Public clouds serve a much larger market and thus are generally available at a lower cost. However, the multitenant nature of public clouds means that they face many more security challenges than private clouds do. In this article, the cloud services, security issues and cloud models are presented.

2.BACKGROUND ANALYSIS:

History of Cloud Computing surprisingly began almost 50 years ago. The father of this idea is considered to be John McCarthy, a professor at

MIT University in US, who first in 1961 presented the idea of sharing the same computer technology as being the same as for example sharing electricity. Electrical power needs many households/firms that possess a variety of electrical appliances but do not possess power plant. One power plant serves many customers and using the electricity example, power plant=service provider, distribution network=internet and the households/firms =computers. Since that time, Cloud computing has evolved through a number of phases which include grid and utility computing, application service provision (ASP), and Software as a Service (SaaS). One of the first milestones was the arrival of Salesforce.com in 1999, which pioneered the concept of delivering enterprise applications via a simple website. The next development was Amazon Web Services in 2002, which provided a suite of cloud-based services including storage, computation and even human intelligence. Another big milestone came in 2009 as Google and others started to offer browser-based enterprise applications, though services such as Google Apps [3].

Architecture

Basis information about the architecture is provided in this chapter, together with the explanations of relevant terms such as virtualization, Front/Back end or Middleware [4].

Virtualization is best described as essentially designating one computer to do the job of multiple computers by sharing the resources of that single computer across multiple environments. Virtual servers and virtual desktops allow you to host multiple operating systems and multiple applications locally and in remote locations, freeing your business from physical and geographical limitations. [5]

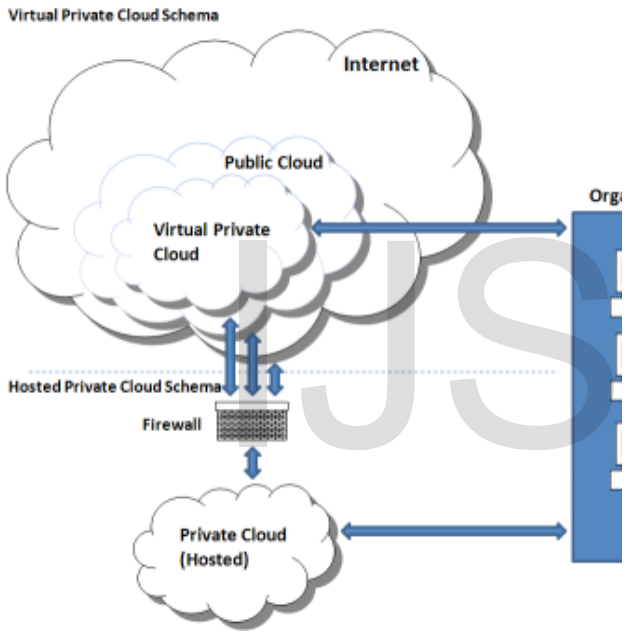
The Cloud Computing architecture can be divided into two sections, the front end and the back end, connected together through a network, usually Internet. The **Front End** includes the client's computer and the application required to access the cloud computing system. Not all cloud computing systems have the same user interface. Services like Web-based e-mail programs leverage existing Web browsers like Internet Explorer or Firefox. Other systems have unique applications that provide network access to clients.

The **Back End** of the system is represented by various computers, servers and data storage systems that create the "cloud" of computing services. Practically, Cloud Computing system could include any program, from data processing to video games and each application will have its own server.

A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called protocols and uses a special kind of software called **Middleware**. Middleware allows networked computers to communicate with each other. [6]

Public Cloud (external cloud) is a model where services are available from a provider over the Internet, such as applications and storage. There are free Public Cloud Services available, as well as

pay-per-usage or other monetized models. **Private Cloud** (Internal Cloud/Corporate Cloud) is computing architecture providing hosted services to a limited number of people behind a company's protective firewall and it sometimes attracts criticism as firms still have to buy, build, and manage some resources and thus do not benefit from lower up-front capital costs and less hands-on management, the core concept of Cloud Computing. [7]



Private/Public cloud

Source:http://www.technologyevaluation.com/login.aspx?returnURL=http://www.technologyevaluation.com%2fresearch%2farticles%2fi-want-my-private-cloud-21964%2f

3. CORE CLOUD COMPUTING TECHNOLOGIES

There are three main categories in CC, Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS). All of them are described below in more details.

- **Infrastructure as a Service** is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. [8]
- **Software as a Service** is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. It is becoming an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture become increasingly available. [9]
- **Platform as a Service** is an outgrowth of Software as a Service (SaaS). It is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

4. SECURITY IMPACT OF CLOUD COMPUTING

In past few years, cloud computing has grown to one of the fastest growing segments of IT industry. But this growth need cloud security to be intact. Below mentioned are few most important issues of cloud computing.

4.1 Privacy

Cloud computing utilizes virtual computing technology. In this, user's personal data is kept on various virtual data center which may cross international boundaries. This is where data privacy protection may face controversy of various legal systems. There might be few chances that un-legitimate user may leak hidden information, which in turns compromises privacy of data.

4.2 Security

Where is your data more secure, on your local hard driver or on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security. However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored. Industrious hackers can invade virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft.

4.3 Reliability

Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.

4.4 Open Standard

In cloud computing, open standards are critical to grow. Many CSP provides well documented APIs which are unique to their implementation and thus difficult to interoperable. Towards the progress, there are many open standards are under development; OGF's Open Cloud Computing Interface is one of them. The Open Cloud Consortium (OCC) is working to develop consensus on early cloud computing standards and practices.

4.5 Long-Term Viability

It should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application.

4.6 Freedom

In cloud computing, users are not permitted to physically possess storage of data, leaving data storage and control the data. Customers will contend that this is pretty fundamental and affords them the ability to retain their own copies of data

in a form that retains their freedom of choice and protects them against certain issues out of their control whilst realizing the tremendous benefits cloud computing can bring.

4.7 Compliance

Numerous regulations pertain to the storage and use of data require regular reporting and audit trails, cloud providers must enable their customers to comply appropriately with these regulations. Managing Compliance and Security for Cloud Computing, provides insight on how a top-down view of all IT resources within a cloud-based location can deliver a stronger management and enforcement of compliance policies. In addition to the requirements to which customers are subject, the data centers maintained by cloud providers may also be subject to compliance requirements.

5. CLOUD COMPUTING MODELS

5.1 Public Cloud

Public cloud makes use of standard cloud computing model and makes resources available to public over an Internet. Public cloud services may be offered on pay-per-usage basis or may be free. Benefits of public cloud:

1. Due to pay-per-usage, no wastage of resources.
2. Inexpensive setup as setup cost is managed by provider.
3. Easily accessible, etc.

5.2 Private Cloud

Private cloud is a cloud infrastructure operated for single organization [2]. It may be managed internally or by third party and hosted internally or externally. This kind of setup can grow business if security issues are handled carefully. It has significant footprint in terms of equipment setup and environmental controls. It costs additional capital expenditure as assets have to be refreshed periodically. Private cloud is also referred as internal cloud or corporate cloud.

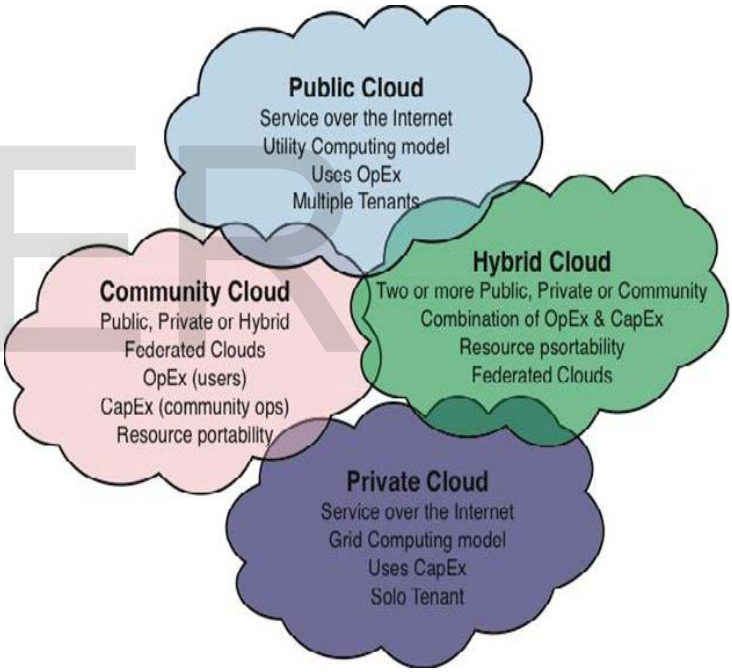


Figure: 2 Cloud computing models

5.3 Community Cloud

Community cloud is multi-tenant infrastructure shared amongst several organizations from specific group with common concerns. Concerns might be related to regulatory compliance, performance

requirements, etc. [3]. The goal of community cloud is to have participating organizations realize the benefits of public cloud with the added level of privacy which is usually associated with private cloud. It can be on-premises or off-premises and can be governed by participating organizations or by third party managed service provider (MSP).

5.4 Hybrid Cloud

Hybrid cloud is integrated cloud service utilizing both private and public clouds to perform distinct functions within organization [4]. In practice, an enterprise cloud implement hybrid cloud hosing to host their e-commerce website within a private cloud, where it is secure and scalable, but their brochure site is in public cloud, where it is more cost effective.

6. CLOUD VULNERABILITY:

Cloud computing is in constant development; as the field matures, additional cloud-specific vulnerabilities certainly will emerge, while others will become less of an issue. Using a precise definition of what constitutes vulnerability from the Open

Group's risk taxonomy and the four indicators of cloud-specific vulnerabilities we identify here offers a precision and clarity level often lacking in current discourse about cloud computing security.

Control challenges typically highlight situations in which successful security controls are ineffective in a cloud setting. Thus, these challenges are of special interest for further cloud computing security research. Indeed, many current efforts such as the development of security metrics and certification schemes, and the move toward full-featured virtualized network components directly address control challenges by enabling the use of such tried-and tested controls for cloud computing.

A particular vulnerability can be considered specific to cloud computing if it meets any of the following criteria [10]:

- it is intrinsic to or prevalent in a core technology of cloud computing, such as virtualization, service oriented architecture, and cryptography
- it has its root cause in one of essential cloud characteristics, such as elasticity, resource pooling, and pay-as-you-go model • it is caused by cloud innovations making existing (tried and tested) security controls hard or impossible to implement; for example, management procedures that were created initially for a fixed hardware structure do not port correctly to virtual machines [11]
- it is prevalent in established state-of-the-art cloud services

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

[4] F. Frankova, Service Level Agreements: Web Services and Security, ser. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, vol. 4607.

[5] "Service Level Agreement and Master Service Agreement", http://www.softlayer.com/sla.html, accessed on April 05, 2009.

[6] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, On Technical Security Issues in Cloud Computing. IEEE, 2009.

[7] Cloud security alliance: Security guidance for critical areas of focus in cloud computing v2.1," Dec 2009.

[8] E. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus Open-Source Cloud- Computing System," Cluster Computing and the Grid, IEEE International Symposium on, vol. 0, pp. 124–131, 2009.

[9] T. Garfinkel and M. Rosenblum, "When virtual is harder than real:security challenges in virtual machine based computing environments," Proceedings of the 10th conference on Hot Topics in Operating Systems –Volume 10, 2005

[10] Kamal Dahbur, Bassil Mohammad, Ahmed BisherTarakji, A Survey of risks, threats, and vulnerabilities in cloud computing, ACM 978-1-4503- 0474-0/04/2011

[11] Vaquero, Luis Rodero-Merino Juan Caceres et. al "A break in clouds : Towards a cloud definition." ACM SIGOMM Computer Communication Review Archive, Volume 39, Issue 1 (January 2009).