An Analysis of Cloud Computing and its Security Issues

Anuj Garg
Department of Computer Science and Engineering
Advanced Institute of Technology and Management, Palwal, Haryana, India

Dr. Deepti Sharma
Department of Computer Science and Engineering
Advanced Institute of Technology and Management, Palwal, Haryana, India

Abstract- Cloud computing is a versatile technology for providing computing services by the internet on demand and pay per use access to a pool of shared resources like networks, servers, services, storage and applications, without acquiring physically . Cloud computing begins from the development of parallel computing, distributed computing, shared computing and grid computing. Although the technology and its application are not new, the rising awareness and implementations of cloud services and its underlying technologies cause the need for security requirements being up to date. Cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability. In this paper, we explore the different concepts involved in cloud computing, vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud Computing and its environment as well as to identify and relate vulnerabilities and threats with possible solutions.

Keywords – Cloud Computing, SaaS, Paas, IaaS, Security Requirements, Issues, Vulnerabilities, Threats, Countermeasures

I. INTRODUCTION

The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Applications such as e-mail, web conferencing, customer relationship management (CRM), all run in cloud. Cloud Computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application. The importance of Cloud Computing is increasing. A study by Gartner [1] considered Cloud Computing as the first among the top 10 most important technologies and with a better prospect in successive years by companies and organizations. It appears as computational paradigms as distribution architecture and its main aim is to provide quick, secure, convenient data storage and net computing services, with all computing resources considered as services and delivered over the Internet [2, 3]. The cloud enhances collaboration, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction by optimized and efficient computing [4-6]. Because Cloud Computing represents are new computing model, there is a great chance of uncertainty about how security at all levels like network, host, application, and data levels can be chase and how applications security is moved towards Cloud Computing [7]. Security concerns related to risk areas like external data storage, dependency on the internet, lack of control, multi-tenancy (user) and integration with internal security. Compared to old technologies, the cloud has many specific features, such as its large scale and cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form [9]. In general cloud providers offer three types of services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). We present here a categorization of security issues for these Cloud Computing services focused in the

Identifying the main vulnerabilities and the most important threats in environment. A threat is a potential attack that can be a cause of misusing of information or resources, and the term vulnerability refers to the flaws in a system that allows an attack to be successful. Here we describe the relationship between vulnerabilities and threats. The remainder of the paper is organized as Section 2 presents the analysis of Cloud Computing. Next, in Section 3 we define the most important security aspects for each layer of the Cloud model. Finally, we provide some conclusions.

II. Overview of Cloud Computing

A. Definition

Cloud computing is becoming a great deal of attention, both in publications and among users. Cloud computing is a service based on subscription where you can receive networked storage space and computer resources. It allows consumers and businesses to use applications without installation and access their personal files at any computer by internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you can use a service over the Internet, at another location, to store your information or use its applications. Doing this may give rise to certain privacy implications.

Examples:

Examples of cloud computing services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere a network connection is available.
1. A simple example of cloud computing is Yahoo mail, Gmail, or Hotmail and many more. You do not need software or a server to use them. All a consumer would need is just an internet connection and you can start sending emails. The server and email management software is all on the cloud and is totally managed by the cloud service provider like Yeah, Google etc.
2. When you store your photos online instead of on your home computer, or use webmail or a social networking site, you are using a "cloud computing" service.

B. Basic Concepts

There are certain models and services working for making the cloud computing feasible and accessible to end users. Following are the models for cloud computing:
Deployment Models
Service Models
Deployment Models for Clouds

These models define the various types of access to the cloud as how the cloud is located? Cloud may have any of these four types of access: Public, Private, Hybrid and Community.

Public Cloud

The Public Cloud makes services and systems to be easily accessible to the public. This cloud may be less secure due to its openness for example- email. This cloud can be accessed by any of the subscriber with an internet connection and access to the cloud space.

Private Cloud

The Private Cloud makes services and systems to be accessible within an organization. This cloud offers increased security because of private nature.
This type of cloud is established for a specific group or organization and can limits access to that group.

Community Cloud

The Community Cloud makes services and systems to be accessible by group of organizations .this cloud is shared among two or more organizations that have similar cloud requirements.

Hybrid Cloud

The Hybrid Cloud is a combination of public and private cloud. Although, the most critical activities are performed using private cloud while the less critical activities are performed by public cloud.
Service Models for Clouds

Service Models are the reference models for the Cloud Computing. These models can be categorized into following three basic service models as
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)

Software as a Service (SaaS)

In a cloud computing SaaS is software that is owned, delivered and managed by one or more providers and that is offered in a pay-per-use manner [18]. SaaS in simple terms can be defined as "Software deployed as a hosted service and accessed over the Internet" [19] .SaaS can provide scalability and shifts burdens from subscribers to providers, resulting in a large number of opportunities for more efficiency and performance. The typical user of a SaaS offering usually has neither knowledge nor control about the underlying infrastructure [20].

Platform as a Service (PaaS)

This type of cloud computing provides development and deployment environment as a service. The consumer can use the mediator's equipment for the development of his own programs and deliver them to the users through Internet and servers. The consumer can control the applications that run, but cannot control the operating system, hardware or network on which they are running.

Infrastructure as a Service (IaaS)

In this Physical infrastructure is abstracted to provide computing, storage, and networking as a service for avoiding the expenses and requirement for dedicated systems. Infrastructure as a service delivers a platform virtualization outsourced service.

Benefits

Cloud Computing have various advantages. Some of them are as follows:

- Application can be accessed as utilities, over the Internet.
- Applications can be configured and manipulated at anytime and anywhere.
- There is no need to install a specific piece of software to manipulate or access cloud applications.
- Cloud Computing provides online development and deployment tools and runtime environment by Platform as a Service model.
- Cloud Computing provides on-demand self-service. The resources can be used without direct interaction with the cloud service providers.
- Cloud Computing is very cost effective as it just requires an Internet connection.
- Cloud Computing provides load balancing so that it is more reliable.

III. SECURITY CONSIDERATION IN CLOUD COMPUTING

In this section security consideration in cloud computing will be discussed. Some important keywords are secure Cloud systems, Cloud security, delivery models security, SPI security, SaaS security, Paas security, IaaS security, Cloud threats, and Cloud vulnerabilities. The cloud model provides three types of services [11, 15, 16].Before discussing the security challenges in Cloud Computing,

We have to understand the relationships and dependencies between these cloud service models [4]. PaaS and SaaS both are hosted on top of IaaS so that any flaws in IaaS will affect the security of both PaaS and SaaS services. As a matter of these deep dependencies, any attack to any cloud service layer may compromise the upper layers.

A. Security issues in SaaS

SaaS provides application services on demand such as email, conferencing software, and business applications such as ERP, CRM, and SCM [17].The users of SaaS may have less control over security among the three delivery models in the cloud computing. The SaaS applications may raise some security concerns.

Security of Applications

The applications are mainly delivered via the Internet through a Web browser [10, 12]. However, vulnerabilities for the SaaS applications are created as a result of flaws in web applications. Attackers are using the web to compromise user's computers. There may be more security issues, but it is a good start for securing web applications.

Multi-tenancy Applications

SaaS applications can be defined as maturity models that are specified by these characteristics: scalability, configurability, and multi-tenancy [17]. According to the first maturity model, each customer has his own customized software instance. This model also has some drawbacks, but security issues are not as bad as in the other models. In the second maturity model, each customer has different instances of the applications but all instances use the same application code. In the third model multi-tenancy is added, so all customers are served by single instance, but the risk of data leakage between these tenants is high.

Security of Data

Security of data is a common for any technology, but it becomes a major challenge when SaaS users have to rely on their providers for proper security [10, 11].

B. Security issues in PaaS

PaaS provides facilitates for the deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers [11]. Like SaaS and IaaS, PaaS also depends on a secure, reliable network and secure web browser. PaaS application security comprises two software layers: Security of the PaaS platform itself, and Security of customer applications deployed on a PaaS platform [8].

Relationships to Third-party

PaaS does not only provide traditional programming languages, but also does third-party web services components. So that PaaS users have to depend on both the security of web-hosted development tools and third-party services.

System Development Life Cycle

The speed at which applications will change in the cloud will affect both the System Development Life Cycle (SDLC) and security [10, 14]. So that Developers should keep in mind that PaaS applications must be upgraded frequently.

Security of infrastructure

Because of developers do not have access to the layers, so providers are fully responsible for the security of underlying infrastructure.

C. Security issues in IaaS

Infrastructure as a service provides a pool of resources like servers, storage, networks, and other computing resources in the form of virtualized systems, which are accessed through the Internet [14].In IaaS, users of cloud have better control over the security compared to the other models but there should not be any security hole in the virtual machine monitor [11].

D. Security and Privacy

Security and Privacy of information is the biggest challenge to cloud computing. Security and privacy issues can be overcome by employing encryption, security hardware and security applications.

IV.CONCLUSION

Cloud computing is dramatically changing the horizon of information technology and ultimately turns the utility computing into a reality. Cloud Computing is a relatively new concept that presents a good number of benefits. It is a combination of several key technologies that have evolved and matured over the years. It also has a potential for cost savings to the enterprises but the security risk are also enormous. Since Cloud Computing is a combination of many technologies, so that it inherits their security issues too.

In our paper, we have presented an overview or analysis of cloud computing and focused on the various types of models for cloud. We also discuss some benefits of cloud computing. In the next section we describe the security issues in SPI model of cloud with some subsections .we believe our paper will provide a better understanding of the cloud computing and different security issues, thereby bolstering further research in this arena.

REFERENCES

[1] Gartner Inc Gartner identifies the Top 10 strategic technologies for 2011: http://www.gartner.com/it/page.jsp?id=1454221. Accessed: 15-Jul-2011

[2] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: A Statistics Aspect of Users. In: First International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg, pp 347–358

[3] Zhang S, Zhang S, Chen X, Huo X (2010) Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. IEEE Computer Society, Washington, DC, USA, pp 93–97

[4] Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0.. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[5] Marinos A, Briscoe G (2009) Community Cloud Computing. In: 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Springer-Verlag Berlin, Heidelberg

[6] Centre for the Protection of National Infrastructure (2010) Information Security Briefing 01/2010 Cloud Computing. Available:http://www.cpni.gov.uk/Documents/Publications/2010/2010007ISB_cloud_computing.pdf

[7] Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysis in the migration to cloud environments. Future Internet 4(2):469–487

[8] Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O'Reilly Media, Inc., Sebastopol, CA

[9] Li W, Ping L (2009) Trust model to enhance Security and interoperability of Cloud environment. In: Proceedings of the 1st International conference on Cloud Computing. Springer Berlin Heidelberg, Beijing, China, pp 69–79

[10] Rittinghouse JW, Ransome JF (2009) Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security, CRC Press

[11] Subashini S, Kavitha V (2011) A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 34(1):1–11

[12] Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) On technical Security issues in Cloud Computing. In: IEEE International conference on Cloud Computing (CLOUD'09). 116, 116, pp 109–116

[13] Onwubiko C (2010) Security issues to Cloud Computing. In: Antonopoulos N, Gillam L (ed) Cloud Computing: principles, systems & applications. 2010, Springer-Verlag

[14] Morsy MA, Grundy J, Müller I (2010) An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 Cloud Workshop. APSEC, Sydney, Australia

[15] Mell P, Grance T (2011) The NIST definition of Cloud Computing. NIST, Special Publication 800–145, Gaithersburg, MD

[16] Zhang Q, Cheng L, Boutaba R (2010) Cloud Computing: state-of-the-art and research challenges. Journal of Internet Services Applications 1(1):7–18

[17] Ju J, Wang Y, Fu J, Wu J, Lin Z (2010) Research on Key Technology in SaaS.

[18] Mertz SA, Eschinger C, Eid T, Pring B (2007) Dataquest Insight: SaaS Demand Set to Outpace Enterprise Application Software Market

[19] Growth. Gartner RAS Core Research Note, 3 August 2007 Moxie Marlinspike, "New Tricks for Defeating SSL In Practice," 2009.

[20] Frederick Chong and Gianpaolo Carraro, "Architecture Strategies for Catching the Long Tail," Microsoft Corporation, April 2006..

[21] P. Kumswat, Ki. Attakitmongcol and A. Striaew, "A New Approach for Optimization in Image Watermarking by Using Genetic Algorithms", *IEEE Transactions on Signal Processing*, Vol. 53, No. 12, pp. 4707-4719, December, 2005.

[22] H. Daren, L. Jifuen,H. Jiwu, and L. Hongmei, "A DWT-Based Image Watermarking Algorithm", in *Proceedings of the IEEE International Conference on Multimedia and Expo*, pp. 429-432, 2001.

[23] C. Hsu and J. Wu, "Multi-resolution Watermarking for Digital Images", *IEEE Transactions on Circuits and Systems- II*, Vol. 45, No. 8, pp. 1097-1101, August 1998.

[24] R. Mehul, "Discrete Wavelet Transform Based Multiple Watermarking Scheme", in *Proceedings of the 2003 IEEE TENCON*, pp. 935-938, 2003.