Cloud Computing Services: A Survey

Anupama Prasanth
Lecturer
College of Computer Studies
AMA International University

ABSTRACT
Cloud computing is a new way of delivering computing resources, not a *new technology; a* term simply renames common technologies and techniques that we have come to know in IT. It is the most significant technique in the 21st century. This new technique conveys enormous impact to the society, especially the business world. The services of cloud computing sets the clients free from worrying about data processing problems, so that they can focus on their major businesses. This new economic model for computing is increasingly becoming popular and is seeing massive global investment. Despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are the major barriers for cloud adoption.
This paper mainly focuses on the three cloud service models, commonly referred to as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), its major threats and some guidance on situations where particular flavor of cloud model are best option for an organization. This also discusses with example some major cloud service providers in order to show that how cloud computing will make the business world simpler, more efficient and more specialized.

General Terms
Cloud Computing, Cloud Security, Cloud Service Models et. al.

Keywords
SaaS, PaaS, IaaS, Cloud Security Threats, Cloud Service Models, Cloud Computing.

1. INTRODUCTION
Recently, cloud computing has grown from being a promising business concept to one of the fastest growing buzz word in the distributed computing. It is a great network-tech breakthrough, which might bring us to the cloud society. Cloud computing represents an unusual way to architect and remotely manage computing resources and soon will reshape the IT industry as a revolution. In order to gain in the competitive business environment, businesses are increasingly looking for innovative ways to reduce costs while maximizing value. Recession-hit companies are more aware that simply by tapping into the cloud they can easily access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. It is the growing acceptance of innovative technologies that has seen cloud computing become the biggest buzzword in IT.
In order to truly understand how the Cloud can be of value to an organization, it is very important to understand what the Cloud really is, it's different models, its vendors and its security issues. Since the Cloud is a broad collection of services, organizations can choose where, when, and how they use Cloud Computing. However, cloud computing has been already changing the way that the business world runs; this is going to be discussed in this paper
This paper is organized as follows: In section 2, the basic concepts of cloud computing will be introduced along with its challenges and security concerns. In section 3, the paper explains the three main cloud service models, its threats and also discusses the area where these models make sense. Summary is concluded in the last section.

2. CLOUD COMPUTING
The term cloud computing has the feel of an IT buzzword. It is a newly born internet based computing technique and becoming a popular option for renting of computing and storage infrastructure services; for remote platform building and customization for business processes and for renting of business applications as a whole. This new technique integrates, optimizes and provides computing ability, aiming to simplify the clients computing jobs by the way of renting resources and services. Although many formal definitions have been proposed in both academia and industry, the generally accepted definition of Cloud Computing comes from the National Institute of Standards and Technology (NIST)[1]. The NIST definition runs to several hundred words and appears to include key common elements widely used in the cloud computing community. It essentially says that: *Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*[1]. This definition includes cloud architectures, security and deployment strategies [1]. What this means in plain terms is the ability for end users to utilize parts of bulk resources and that these resources can be acquired quickly and easily.
This technology, how it is defined in different levels of organizations is different. It is fully based on the way they utilize the facilities. For startups and technology companies defines the cloud as a drastic increase in capital efficiency. Because this provides a channel to start a new service with cheaper and easier than ever to scale it. But the same way for the large businesses, the cloud turns computing from a capital expense to an operating expense. Cloud computing provides computation, software, data access, and storage services and it do not require end-user knowledge of the physical location and configuration of the system that delivers the services. We can say it as the byproduct and consequence of remote computing sites provided by the Internet. This may take the form of web-based tools or applications that users can access and use through a web browser as if the programs were installed locally on their own computers
The following are the essential key characteristics of the cloud computing which make this technology highly attractive form of business in the future.

IT service-centric approach: Users of the cloud generally want to execute some application for a specific timely purpose; they don't want to get bogged down in the system and network administration of the environment. They would prefer to quickly and easily access a dedicated instance of an application or a service on demand.

On-demand self service based usage: This feature of cloud computing provides users the ability to upload, build, deploy, schedule, manage and report on their business services on demand. A customer is always in the driving seat regarding its present and future needs. He can avail computing resources such as CPU time, network storage, software use and so forth in a convenient fashion without resorting to human interaction with providers of these resources.

Consumption based billing and Measured services: Cloud computing is usage driven. Consumers pay for only the time they use the infrastructure for. It can be provided as much services as needed to the customer. Cloud computing provides with the specified number of user license for any type of the software and assign definite data space and network bandwidth which is suitable to that demands. This characteristic makes this service very well defined and predictable cost.

Location independent resource pooling and Broad network access: Cloud computing enable users to access systems using a web browser regardless of their location or what device they are using. And also it provides variety of services on the network with broader data spaces, multiple value added services, many new software, many advanced processing techniques and much more accessibility to a highly rich and capable network.

Rapid Scalability: This is very important feature of cloud computing, that any modification and enhancement in the services are very easy and fast which make this service very scalable and resilient. Users can easily add up required bandwidth, processing speed and data storage or number of license in very short time. Resource provisioning appears to be infinite to customers, the consumption can rapidly rise in order to meet peak requirement at any time.

2.1 Cloud Security Concerns

Cloud computing frees individuals and organizations from the expenditure and burden of installing, maintaining and upgrading software applications. It allows companies to focus on their core competencies, rather than investing in centralized computing facilities. Although cloud computing benefits are tremendous, security and privacy concerns are the primary obstacles to wide adoption. Cloud service providers (CSPs) are separate administrative entities, so moving to the commercial public cloud reduces the direct control over the systems that manage their confident data and valuable applications. CSPs' infrastructure and management capacities are much more powerful and reliable than those of personal computing devices; the cloud platform still faces both internal and external security and privacy threats. Apple's iPad subscriber privacy leak [14], Amazon S3's recent downtime [15], and Gmail's mass email deletions [16] are all such examples.

The critics of cloud computing points to the fact that users are fully depends on a high quality Internet connection. Even if most of our applications are locally installed, our reliance on the Internet is so great. The disruption caused by an Internet outage is highly significant. So a reliable Internet connection now become as requisite a utility service for business and personal activities as a constantly available phone network and electricity supply. Cloud computing has also a trust on external suppliers which may also raise potential business continuity, data protection and security risks.

The common security issues around cloud computing are mainly on Cloud infrastructure, platform and hosted code (storage and network vulnerabilities), Data (data integrity, data lock in, data reminisce, provenance, data confidentiality, user specific concerns), Access (cloud authentication, authorization, encrypted data communication, user identity management), and Compliance (security audit, data location, operation traceability). People who are using cloud computing services needs to take appropriate measures for ensuring safe web access, these include setting a strong password, ensuring antivirus, antispyware and firewall software are installed, and ensuring that their operating system and web browser(s) are always updated with the latest security patches.

Well-known security issues such as data loss, phishing and 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 [12] that require novel techniques to tackle with. For example, hackers are planning to use Cloud to organize botnet as Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start and attack [12].

3. CLOUD SERVICE MODELS

Although the term Cloud Computing is widely used, it is important to note that all Cloud Models are not the same. As such, it is critical that organizations don't apply a broad brush one-size fits all approach to security across all models. Cloud Models can be segmented into **Software as a Service (SaaS), Platform as a service (PaaS) and Integration as a Service (IaaS)**. When an organization is considering Cloud security it should consider both the differences and similarities between these three segments of Cloud Models.

3.1 Software as a Service (SaaS)

Software as a Service (SaaS)[2],[3],[8] is defined as "software that is deployed over the internet. With SaaS, a provider licenses an application to customers either as a service on demand, through a subscription, in a "pay-as-you-go" model, or (increasingly) at no charge when there is opportunity to generate revenue from streams other than the user, such as from advertisement or user list sales".

Consistent with the basic notion of cloud computing, SaaS[20] is a model whereby the customer licenses applications and provisions them to users on demand. The services run on the provider's infrastructure and are accessed through a public network connection. Applications may be made available through Internet as browser applications or they may be downloaded and synchronized with user devices. SaaS offers compelling benefits. It simplifies licensing. In fact, the customer doesn't need to acquire a software license at all. This is a task of the provider. There is also no need to calculate maximum capacity. It outsources the tedious task of application maintenance and upgrades and ties customer costs to usage, which lowers fixed costs and capital investment. It does so at the price of restricting customer flexibility in terms of configuration options and update schedule. This rapid growth indicates that SaaS will soon become commonplace within every organization and hence it is important that to understand what SaaS is, where it is suitable and security issues. The core technology of SaaS is centered on its multi-tenant architecture. Chong and Carraro (2006) characterized SaaS as "Software deployed as a hosted service and accessed over the Internet." In order to provide efficient and effective services to SaaS clients, the SaaS providers must design their application architecture as "scalable, multi-tenant-efficient, and configurable" (Chong and Carraro, 2006)[13].

3.1.1. Top threats in SaaS

Software-as-a-service is growing in popularly but not all IT decision-makers are taking the leap. "Security is the No. 1 reason preventing firms from moving to SaaS," Forrester analyst Liz Herbert writes in a recent report on software-as-a-service adoption[6],[9]. There are numerous security risks to look at before adopting software-as-a-service. Here are four problems to consider. [11], [9],[19]

3.1.1.1. Undeveloped Identity Management:

Identity and access management in the cloud is immature. Cloud providers themselves aren't always sophisticated about integrating their platforms with identity services that exist behind the enterprise firewall. There are some third-party technologies that let IT extend role-based access controls into the cloud with single sign-on.

3.1.1.2. Weak Cloud Standards:

SAS 70 is an auditing standard designed to show that service providers have sufficient control over data. The standards weren't crafted with cloud computing in mind, but it's become stand-in benchmark in the absence of cloud-specific standards.

3.1.1.3. Secrecy in Security and data centers:

Cloud vendors argue that they are more able to secure data than a typical customer, and that SaaS security is actually better than most people think. But some customers find this hard to believe because SaaS vendors tend to be rather secretive about their security processes. In particular, many cloud service providers release very few details about their data centers and operations, claiming it would compromise security. However customers and industry analysts are getting fed up with all the unanswered questions and hush-hush nondisclosure agreements

3.1.1.4. Risk in universally Accessibility:

The major benefit of software-as-a-service is that business applications can be accessed wherever there is Internet connectivity, which also poses new risks. Coupled with the proliferation of laptops and Smartphone, SaaS makes it even more important for IT shops to secure endpoints. If we put my e-mail on Gmail, an employee could log in from a coffee shop on an unsecured computer. It's one of the benefits of software-as-a-service, but it's also one of the downsides. That endpoint isn't necessarily secure.

3.2 Platform as a Service (PaaS)

Platform as a service' (PaaS) [10] is the delivery of a computing platform and solution stack as a service. It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers providing all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the Internet—with no software downloads or installation for developers, IT managers or end-users. Cloud platforms act as run-time environments which support a set of programming languages. They may offer additional services such as reusable components and libraries that are available as objects and application programming interfaces. Ideally, the platform will offer plug-ins into common development environments, such as Eclipse, to facilitate development, testing and deployment. Platforms are also expanding to real-world integration platform services including business process integration, and assured system-to-system messaging.

3.2.1 Top threats in PaaS

3.2.1.1. Default Application Configurations:

When running an application on a cloud infrastructure, the odds that the application is secure in its default configuration are probably zero. Thus, making changes to the default application installation will be the number one security threat.

3.2.1.2. SSL Protocol based attacks:

The second greatest threat to PaaS users will be SSL-based attacks. SSL is the underpinnings of most of the "security" utilized in the cloud and, for that matter, the Internet in general. The current focus of the hacking community on breaking SSL will become a major threat in the near future. In order to avoid this attack, the first measure is to make sure that the applications are not open to default attacks, understanding this and take all possible steps to mitigate attacks on SSL.

3.2.1.3. Insecure permission on cloud data:

The third major threat that PaaS users will need to address is insuring the proper permissions on data stored in the cloud. While this may seem like a given, many of the applications There exist a serious information leakage, because of the data's underlying permissions were not set correctly. From a security standpoint, this means that too much access had been granted.

3.3 Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS)[3] is a way of delivering Cloud Computing infrastructure – servers, storage, network and operating systems – as an on-demand service. Rather than purchasing servers, software, datacenter space or network equipment, clients instead buy those resources as a fully outsourced service on demand. Cloud consumers directly use IT infrastructures provided in the IaaS cloud. Virtualization is extensively used in IaaS cloud in order to integrate/decompose physical resources in an ad-hoc manner to meet growing or shrinking resource demand from cloud consumers. It is an evolution of virtual private server offerings and merely provides a mechanism to take advantage of hardware and other physical resources without any capital investment or physical administrative requirements. The benefits of services at this level are that there are very few limitations on the customer. There may be challenges including dedicated hardware but almost any software application can run in an IaaS context.

3.3.1 Top threats in IaaS

The most important threat you'll face when using an IaaS offering is dealing with vulnerabilities in underlying operating systems (OS's) and services[19].

3.3.1.1. Threats in underlying operating system and services:

The number one threats for the consumer of an IaaS offering are vulnerabilities in the underlying Operating system or services that are running on it[16]. At the current time, Linux variants and Windows based OSes are the main options you have in Public IaaS offerings. Both of these OSes and services that run on them have vulnerabilities. OS and service vulnerabilities are publicized through many outlets, and in many instances exploits are publicly available.

3.4 Service Models: An Overview

The most common way of representing cloud is the SPI (Software as a Service, Platform as a Service and Infrastructure as a Service) model. There are two primary

dimensions which constrain the offerings: The services differ according to their flexibility and degree of optimization. Software services are typically highly standardized and tuned for efficiency. However, they can only accommodate minimal customization and extensions. Infrastructure services can host almost any applications but are not able to leverage the benefits of economy of scope as easily. Platform services represent a middle ground. They provide flexible frameworks with only a few constraints and are able to accommodate some degree of optimization.

Infrastructure offerings can create a foundation for Platform offerings, and Platform offerings can do the same for Software offerings. Software offerings can be hosted through a Platform or can hop-scotch Platform and build delivery architecture on top of raw Infrastructure. Infrastructure can be replaced with traditional infrastructure by both Platform and Software layers that might directly depend on it. Software tends to cater to end users looking to satisfy some business, general process or even recreational need. Platform primarily interfaces with application developers and software companies, providing them the tools and run time to quickly build Software offerings. Infrastructure tend to focus on identifying value to network planners that need to organize specific lower level resources in support of Platform or Software offerings.

Table 1: Comparison between areas makes sense

Features	***SaaS***	***PaaS***	***IaaS***
Users	End users	Application developers	Network architects
Suitable areas	• Applications where there is significant interplay between the organization and the outside world. • Applications that have a significant need for web or mobile access. • Software that is only to be used for a short term need. • Software where demand spikes significantly.	• Situation where multiple developers will be working on a development project or where other external parties need to interact with the development process. • Developers wish to automate testing and deployment services.	• Can be applied where demand is very volatile. • For new organizations without the capital to invest in hardware • Organization which are growing rapidly and scaling hardware would be problematic • There is pressure on the organization to limit capital expenditure and to move to operating expenditure • For specific line of business, trial or temporary infrastructural needs

4. CONCLUSION

This paper outlined a survey in Cloud computing services, focusing on the SaaS, PaaS and IaaS service models, also articulate the areas where these models are best suited. This paper also analyzed a few threats of each of these models. However after all, all the stuff that cloud computing can offer is only a platform and some new ways for running services. No matter how well the platform is developed, if the services provided are not brilliant enough, it will surely end up with an eventually failure. Since this is a huge area, and there a lot of work to do, we hope this paper could be a useful starting point for identifying opportunities for further research.

5. ACKNOWLEDGEMENTS

We are heartily thankful to our colleagues, their encouragement, guidance and support from the initial to the final level enabled us to develop an understanding of the subject.

6. REFERENCES

[1] P. Mell and T. Grance, "Draft nist working definition of cloud computing - v15," *21. Aug 2009*, 2009.

[2] Amazon Elastic Compute Cloud web services, http://aws.amazon.com/ec2

[3] Zhao Wei; An Initial Review of Cloud Computing Services Research Development; International Conference on Multimedia Information Networking and Security; 2010.

[4] SalesForce Force.com Platform as a service, http://developer.force.com

[5] CRM Open source business software ;SugarCRM; http://www.sugarcrm.com

[6] PingIdentity. (2009, September). Open source federated Identity Management. Retreived September 16, 2009, from http://www.sourceid.org/content/primer.cfm

[7] Workday Wiki free encyclopedia; http://www.en.wikipedia.org/wiki/**Workday**,_Inc.

[8] Googe Apps and Google App Engine; apps.google.com; appengine.google.com

[9] Cloud Security Alliance. (2009, December). Security Guidance for critical Areas of Focus. Retrieval April 2010, from Cloud security Alliance: http://www.cloudsecurityalliance.org/

[10] Platform as Service; http://java.dzone.com/articles/what-platform-service-paas

[11] Danwei CHEN, Xiuli HUANG, Xunyi REN: Analysis of Cloud Computing and Cloud Security, In Computer Technology and Development; 2010.02

[12] Y. Chen, V. Paxson and R. Katz, "What's new about cloud computing security?" 2010.

[13] Chong, F. and Carraro G. "Architecture strategies for catching the long tail," a Microsoft white paper, available at

http://msdn2.microsoft.com/enus/architecture/aa479069(d=printer).aspx

[14] http://techcrunch.com/2010/06/15/ipad-breach-personal-data/

[15] (http://status.aws. amazon.com/s3-20080720.html

[16] www.techcrunch.com/2006/12/28/gmail-disaster-reports-of-mass-email-deletions

[17] http://www.systemexperts.com/assets/pdf/SystemExperts-IaaSThreatsInTheCloudPt1.pdf

[18] Microsoft; www.microsoft.com/windowsazure; www.microsoft.com/onlinehome.live.com

[19] Shubhashis Sengupta, Vikrant Kaulgud, Vibhu Sayanya Sharma; Cloud Computing Security- Trends and Research Directions ; IEEE World Congress on Services 2011. David C. Chou, Amy Y Chou; Software as a Service (SaaS) as an outsourcing model: An economic Analysis