Threats to Virtual Network Security

Pratishtha
GBTU at IPEC

ABSTRACT
Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Current drift of organizations is moving toward the technology "Cloud Computing". Cloud Computing directly refers to the virtual organizations. Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. Since, many local intrusion detection & audit practices are taking place; our virtual organization is under these threats. Privacy concern of information about each member between organization & member keeps the information private & centralized. With its innovative features, it raises the question of trust, privacy & security.
In this paper I would try to identify threats to security in cloud computing and how these threats can be dealt with. Moreover we will also discuss the latest solutions available and their relative advantages and drawbacks.

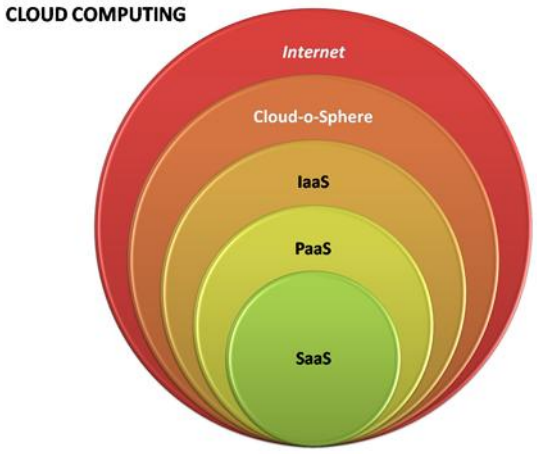
KEYWORDS
Cloud Computing, Security, Privacy, Confidentiality, Virtual, Network, Reliability, Cost

1. INTRODUCTION
In earlier days, internet was signified with a simple symbol of cloud, which represents the invisible ambiguities and smooth flow of information in and out from the cloud. The Cloud Computing is innovated from this cloud symbol. It provides a virtual space to the organizations and companies to store their database on their hardware and servers. A substantially growing business will requisite such kind of technology. For Cloud Computing, it should endow the features such as Dynamism, Abstraction and Resource Sharing. Dynamism means meeting the fluctuating demand of customers at instant, Abstraction is the absorption of data with the service provider which reduces the further complexities and Resource Sharing deals with the optimization of resource utilization. The architecture provided by the Cloud Computing is flexible also. This feature is required due to the sharing of application and other network hardware also. Flexibility architecture gives us an advantage during expansion and contraction of resources with tiny configuration changes. Focusing on the security aspects, Cloud Computing faces breaches. Since, the data of customers is stored with the third party; it is possible that any private information can be leaked.

a. FEATURES
Scalability of cloud computing provides the users a self service basis near real time and provisions for the resources to be fine-grain. [1][2]
Cost is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure. [3] Pricing on a utility computing basis is fine grained with usage based options and fewer IT skills are required for the implementation. [4]
Reliability is improved if multiple redundant sites are used, which makes well designed cloud computing suitable for business continuity and disaster recovery. [5]
Agility improves with users' ability to re-provision technological infrastructure resources.
Virtualization allows applications to be drifted from one physical server to another which in turn can increases utilization.
Maintenance is easier in this case due to one-time installment of applications which can be accessed from different places.
Security is the biggest challenge which can be improved by centralizing the data. Security complexity can be increased when data is distributed over a wider area and in multi-tenant systems that are being shared by unrelated users. Also user access to security audit logs can be made difficult.

b. DEPLOYMENT MODELS
The cloud model is composed of four deployment models: private cloud, community cloud, public cloud and hybrid cloud:
Public Cloud- It is the standard computing model, in which services provide makes a resource available to the general public. These services may be free or on pay-per-usage model. [4]
Community Cloud- It shares the infrastructure between the several organizations from a specific community with common concerns, whether managed internally or by a third-party and hosted internally or externally. [6]
Private Cloud- It is the infrastructure operated solely for a single organization, whether maintained internally or by a third-party and hosted internally or externally. [6]
Hybrid Cloud- It is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. [6]
However by 2011, some vendors are moving towards the OpEx model with full service management, overcoming some of the criticisms.

c. CLOUD STACKS
Cloud Services can be divided into three stacks:



1. IaaS (Infrastructure as a Service) - It is the most basic layer of the cloud stack and serves as a foundation for other two layers for their execution. The main function of this service is virtualization. It uses pay-for-what-you-use model. It can bring more capacity online as soon as required. As in Amazon EC2 (Elastic Compute Cloud), an application can be executed on a virtual system.
2. PaaS (Platform as a Service) - This service is a set of software and product development tools hosted on providers' infrastructure. Here developers create applications on the providers' platform over the internet. The users may use API, website portals or gateway software installed on customers' system. There are no standards for inter-

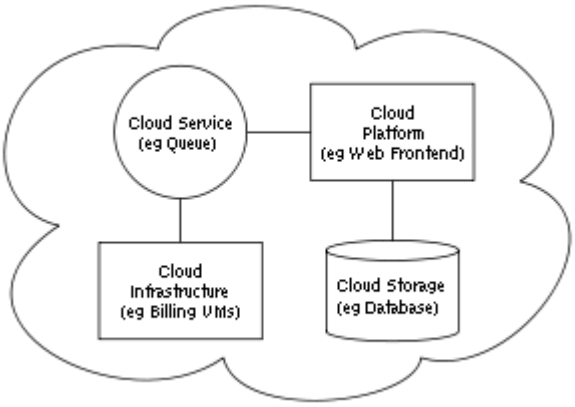
operability or data operability in the cloud. Some providers will not allow software created to be moved off the providers' platform. PaaS have layers viz. Cloud OS, Cloud Middleware

3. Saas (Software as a Service)- It is the top most layer of the cloud computing stack which is directly consumed by the end user. It delivers single application through the browser. Here customers do not put any investment in servers or software licensing. It works efficiently for all ERPs and HR apps.

There are few more stacks in cloud such as DaaS (Data as a Service), BaaS (business as a service) and MaaS (Management as a service). [7]

d. CLOUD ARCHITECTURE

It involves the delivery of cloud computing which has multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue. Elastic provision implies intelligence in the use of tight or loose coupling as applied to mechanisms such as these and others.



Cloud Computing is the summation of front end and back end. The inter-cloud is an interconnected global 'cloud of clouds' and an extension of the Internet 'network of networks' on which it is based.

Front end is the clients' terminal with interface accessing CCS (cloud computing servers). Back end is cloud (i.e. computers, severs or data storage systems). Each application in cloud has its dedicated layer. Networked computers communicate well with each other. For reliability, servers need to store data redundantly.

Applications built on Cloud Architectures run in-the-cloud where the physical location of the infrastructure is determined by the provider. They take advantage of simple APIs of internet-accessible services that scale on-reliability and scalability logic of the underlying services remains implemented and hidden inside-the-cloud. The usage of resources in Cloud Architecture is as needed, sometimes seasonal, thereby providing the highest utilization and optimum bang for the buck. [8]

e. SECURITY CHALLENGES

Despite the secure affirmation of the data by cloud providers, Cloud Computing is not that secured. Several Breaches and attacks happen in this service. Security in the cloud is intangible and less visible, which can make assured sense of security.

User control over cloud resources- Cloud users don't have control over the resources provided by the cloud. There is an immanent risk of data exposure to the third parties or cloud providers itself. From security perspective, isolation of data containers within the technical infrastructure of cloud computing can be a way to ensure that each user can access the data and controls it.

Data Secrecy and confidentiality- Encryption of the data is commonly used these days. It is a practice to secrecy and confidentiality of a data in a hostile environment. But technically, only end-users possess decryption keys.

New threats emerging from the new technology- Virtualization and grid technologies expose cloud infrastructures to emerging and high-impact threats against hypervisors and grid controllers. [9]

Access control and use of the data- The cloud architecture requires the adoption of identity and access management measure. When data are trusted to a third party for handling, precaution must be place to ensure uninterrupted and full control of the data owner over its data.

Application and platform security- Secure development lifecycle of the organizations may need to change to accommodate the cloud computing risk context.

Security models on cloud computing- Migrating onto a cloud may imply outsourcing some security activities to the cloud provider. This may cause confusion between cloud provider and user regarding individual responsibilities, accountability and readdress for failure to meet required standards. Means to clarify those issues can be contracts, but also the adoption of policies by the cloud provider which will clearly set forth obligations and responsibilities of all parties involved. [9]

Lack of reference security standards- The consequence of uncertainty regarding the security and quality levels to be ensured by the cloud providers, but also vendor dependency for cloud users given that every provider uses a proprietary set of access protocols and programming interfaces for their cloud services.

f. PRIVACY CHALLENGES

Cloud providers can store important data, files and records of cloud users. Given the volume or location of Cloud computing providers, it is difficult for companies and private users to keep at all times in control the information or data they entrust to cloud suppliers.

Sensitivity of entrusted information- Entrusting the information to a cloud increases the risk of uncontrolled dissemination of that information to competitors.

Localization of information and applicable law- The relation of certain data to a geographic location has never been more blurred than with the advent of cloud computing.

Users access rights to information- Users of the same cloud share the premises of the data processing and the data storage facilities, they are by nature exposed to the risk of information leakage, accidental or intentional disclosure of information.

Data transfers - If the data used by, or hosted on, the Cloud may change location regularly or may reside on multiple locations at the same time, it becomes complicated to watch over the data flows and, consequently, to determine the conditions that would legitimize such data transfers.

Externalization of privacy - Companies engaging in Cloud computing expect that the privacy commitments they have made towards their customers, employees or other third parties will continue to apply by the Cloud computer provider. This becomes particularly relevant if the Cloud provider operates in many jurisdictions in which the exercise of individual rights may be subject to different conditions.

Contractual rules with privacy implications- It is common for a Cloud provider to offer his facilities to users without individual contracts. Yet, it can be that certain Cloud providers suggest negotiating their agreements with clients and, thus, offering the possibility of tailored contracts. Whatever the opted contractual model is, certain contractual clauses can have direct implications in the privacy and protection of the entrusted information (e.g. defining who actually "controls" the data and who only "processes" the data).

g. TRUST CHALLENGES

The Security and Privacy challenges discussed above are also relevant to the general requirement upon Cloud suppliers to provide trustworthy services. If Cloud providers find adequate solutions to address the data privacy and security specificities of their business model, they will have met in a certain way the requirement of offering trusted services.

Yet, there are a few other challenges which, if tackled properly, would enhance users confidence in the application of Cloud computing and would build market trust in the Cloud service offerings.

Continuity and Provider Dependency - The increasing complexity of Cloud architectures and the resulting lack of transparency also increase the security risk. In many Cloud implementations, the centralized management and control introduces several so-called single points of failure. These could threaten the availability of Cloud users' data or computing capabilities indirectly, as a small incident in the Cloud could have an exponential impact.

Compliance with applicable regulations and good practices - If privacy is one regulatory area particularly relevant to Cloud computing, it is certainly not the only area. Once the applicable law to a Cloud service is determined, the provider will need to comply with other regulations than privacy.

Change in Cloud ownership and "Force Majeure" - The Cloud market is still immature and the situation of global economy may affect some of the Cloud industry players too in the coming months or year(s). Accordingly, users of the Cloud must be confident that the services externalized to the Cloud provider, including any important assets (personal data, confidential information) will not be disrupted as it was discussed above ("Continuity and Provider Dependency").

Trust enhancement through assurance mechanisms - By definition, the Cloud-computing concept cannot guarantee full, continuous and complete control of the Cloud users over their assets. For these reasons, the establishment of appropriate "checks and controls" to ascertain that Cloud providers meet their obligations becomes very relevant for Cloud users (for example, through adherence to generally-accepted standards).

h. DEALING WITH CHALLENGES

Federated ID: Inherent in a cloud computing environment is the need for workers to log into multiple applications and services. This presents a formidable security pitfall, as organizations may lose control over their ability to ensure strong authentication at the user level. To mitigate this risk, organizations need "single sign-on" capabilities.

Always-on Connectivity: When the majority of an organization's critical business data is stored in the cloud, network downtime can shut down business operations. Access to cloud services must be always available, even during maintenance, thus requiring high availability technologies and capabilities such as active/active clustering, dynamic server load balancing and ISP load balancing within the network infrastructure. Organizations should seek technologies that are built into their network solutions, rather than purchase them as standalone products to ensure effectiveness, ease of management and reduced network costs.

Multi-layer Inspection: The rise of the cloud computing environment and increased sophistication of threats has created a need for a proper layered defense comprised of perimeter protection and intrusion detection and prevention capabilities within the network. Rather than implementing first-generation firewalls to protect the cloud at the perimeter, we must use firewall that integrates advanced firewall and IPS capabilities for deep traffic inspection. This will allow organizations to inspect all levels of traffic, from basic Web browsing to peer-to-peer applications and encrypted Web traffic in the SSL tunnel. Additional IPS appliances should be implemented to protect networks from internal attacks that threaten access to the cloud.

Centralized Management: Human error is still the greatest network security threat facing both physical and virtual computing environments. As companies deploy additional network devices to secure their virtual networks, they exponentially increase this risk as device management, monitoring and configuration become more tedious and less organized. It is recommended companies use a single management console to manage, monitor and configure all devices – physical, virtual and third-party.

Virtual Desktop Protection: More and more organizations are deploying virtual desktops to realize the cost and administration benefits. However, these desktops are just as – if not more – vulnerable than their physical counterparts. To adequately protect virtual desktops, organizations should isolate them from other network segments and implement deep inspection at the network level to prevent both internal and external threats. Those organizations should deploy a multi-pronged approach to security by implementing IPS technology that prevents illegal internal access, protects the clients from malicious servers, as well as providing secure remote access capabilities through IPSec or SSL VPN that protects against unauthorized external access.

Besides the apparent challenges, Cloud computing can also lead to new opportunities in the fields of security, privacy and trust for the Cloud users:

• Re-parameterizes around the core internal and sensitive data by migrating public data and applications to the cloud. Outsourcing all publically available systems to specialized partners removes the need for maintaining a complex, vulnerable and expensive internal Internet Street. Instead, the renewed perimeter around the core data creates new opportunities for implementing fine-grained access controls

• Transfer the risks associated with cyber terrorism, denial-of-service and internet crime to the Service Provider. Future projections predict increasing importance of cyber terrorism and organized internet crime. Cloud users can easily outsource the specialized defense against these threats

• Outsource parts of the compliance efforts (e.g. PCI DSS) to the Cloud providers, and make the providers accountable for a predefined set of compliance rules

• Reduce the potential of human errors and rely on the increased autonomy of cloud platforms. Self-monitoring and self-healing systems will reduce human interventions for regular maintenance of the IT systems

• Use the disperse characteristics of the Cloud to build flexible and high performing contingency and disaster recovery capabilities On the other hand, the Cloud service providers can use other Cloud services for their own benefit, which generates the following opportunities for the Cloud service providers:

• Focus on the business offering by transferring the risks associated with identity management and verification to built-for-purpose Identity Providers, such as OpenID. There are currently already some initiatives to implement such model where, for example, telecom providers offer identity verification services to online booking agencies.

2. ADVANTAGE OF CLOUD COMPUTING

It can execute all the programs a normal computer can run.

Clients can access their applications and data from anywhere, any time.

Data won't be confined to a hard drive on a user's computer or even on a corporation's internal network.

Bring hardware costs down.

User needs just to buy a terminal which has just enough processing power to run the middleware.

Need not to buy a set of s/w licenses for every employee.

Client can utilize whole network if cloud computing system's back-end is Grid computing.

3. CONCLUSION

In this paper, I have described the cloud computing with its privacy, trust and security challenges with the way to deal with them. The ways allow mutually distrustful entities form different security domains to collaboratively detect both distributed attacks against their combined infrastructure and abuses of the trust relationships existing between their security domains. In dealing with security, privacy and trust challenges, there should be federated ID where only single sign-in facility should be provided. Always on connectivity allows organizations to access their data anytime and anywhere. Multi-layer inspection leads to checking of layers through generations of firewalls. For reducing human errors, organizations must have centralized

management. More and more organizations are working upon virtual desktop protection which gives benefit in the case of administration and cost. The need for migrating data into as much as core is required where any security breach is not possible. Also, flexibility and agility of cloud computing makes it popular in this modern era.

4. FUTURE SCOPE

The Cloud computing market is an evolving market. It is therefore expected, that best practices will increasingly address the regulatory and operational challenges of Cloud computing, as it was the case with other information services models (e.g. e-marketplaces). Such practices will be consolidated further as the Cloud market becomes bigger and as the service models offered by Cloud become clearer to users. In this perspective, in order to build a trusted model of services, Cloud providers would need to adapt their service models to the best practices and the levels of commercial "fairness" shaped by the stakeholders' community. With so many advantages of Cloud Computing, we can expect all the large and small organizations will go for this technology with the protected environment and new innovations within this Cloud

5. REFERENCES

[1] KIT Software Quality Department "Defining and Measuring Cloud Elasticity".

[2] Cloud Slam 2011 "Economies of Cloud Scale Infrastructure".

[3] CloudAve "Recession is good for Cloud Computing Microsoft Agrees".

[4] IDC "Defining 'Cloud Services' and 'Cloud Computing'"

[5] King, Rachael: Businessweek "Cloud Computing: Small companies take flight.

[6] National Institute of Science and Technology, "The NIST Definition of Cloud Computing"

[7] Techno-pulse "Cloud Computing for the beginners"

[8] Jinesh Varia "Amazon web-services- Cloud Architectures"

[9] Deloitte, "Cloud Computing"