Research Paper Computer Science

Cloud Computing – How Insecure Is The World Up There

Astha Goyal Department of Computer Science, Keshav Mahavidyalaya, University of Delhi

Rochana Chaturvedi Department of Computer Science, Keshav Mahavidyalaya, University of Delhi

ABSTRACT

Cloud computing is one of the emergent technology that creates a virtual workspace for its users. This concept of virtualization has reached to a point where it will provide infrastructural and technological benefits to its users. There are companies who own the cloud computing infrastructure and they lease these services to end users. End users benefit from these services by saving upfront investment on IT infrastructure. Despite having a huge potential, organisations are still reluctant to adopt it completely due to security issues and challenges associated with it. As this technology is getting popular day by day, concerns about the security issues are being voiced up. It is difficult for any organization to share its confidential information on the cloud or on the resource which is owned by some other organization. Reliability is a major concern. Understanding the vulnerabilities of cloud computing will help organizations make the necessary shift towards cloud computing. The main aim of this paper is to provide a detailed analysis of security issues and challenges in cloud computing.

KEYWORDS Cloud Computing, Security, Threats of Cloud Computing.

I.Introduction

With the technological advancements today, cloud computing has evolved as a new concept of creating a virtual workspace which provides hardware and software support to the organizations around the globe. Cloud computing is a distribution technology that provides its users a computational environment that aims to be secure, quick, flexible, scalable, convenient and efficient. It is a cost effective delivery platform for providing IT services over the internet. This technology provides an on-demand network access to a shared pool of configurable computing resources like servers, data stores, networks, applications and services that can be easily provided and released to the demanding users as depicted in figure 1

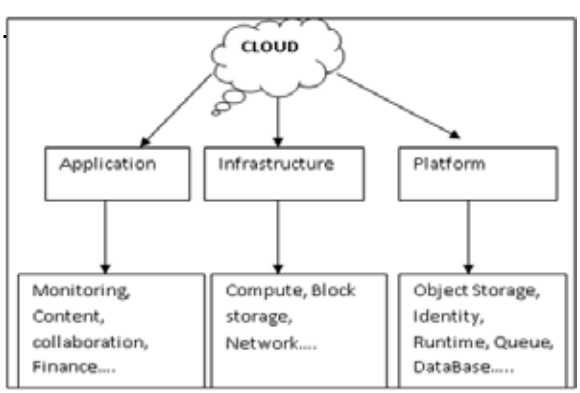


Fig.1:Cloud Computing Services

Cloud computing mostly involves accessing online software applications and storing and processing data. This approach is generally used by organizations to scale their capabilities dynamically without any infrastructural investment or purchase of licensed software. This involves usage of network servers that are remotely located and users can access these servers via internet for the various services provided by cloud rather than doing that on the personal computer of a local server. This technology is adopted by many organizations nowadays to increase their server powers but there are also some critical barriers to this adoption- Information security being the most significant one apart from others like compliance, privacy and legal matters.

When an organization opts for cloud computing technology they also opt for the information security risks associated with it. Security issues in cloud computing play a major role in slowing down its acceptance. As more and more confidential data of companies and individuals are getting uploaded on the cloud, concerns are beginning to grow about reliability of the environment.

Cloud computing security can be seen as sub-domain of network, computer and data security. The data of an organization will be placed over the cloud through a network hence network security; it will placed through computer system and stored in servers hence computer security; and last but not the least, information security where it may jeopardize confidentiality of an organization. In following section, we briefly describe the various Cloud Computing Models and in the section 3 we shall look into the security issues hindering the adoption of this technology.

II. Cloud Computing Models

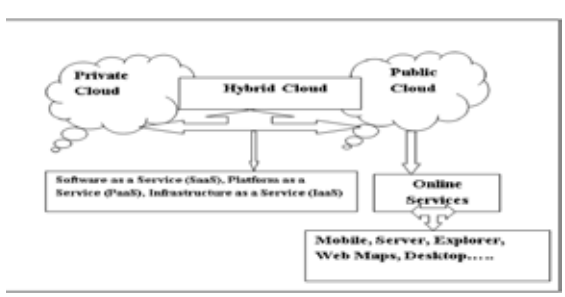


Fig. 2: Cloud Computing Deployment Models

2.1 Cloud Computing Deployment Models

There are four classifications on how a cloud service can be deoplyed. The cloud deployment models show how the network, platform, software, database and other infrastructure are provided as services to the users as depicted in figure 2.

There are four types of deployment models- Public, Private, Hybrid and Community.

2.1.1 Private Cloud: Private cloud is used to describe offerings that emulate cloud computing on private networks [1]. This model is similar to the intranet technology; wherein the entire infrastructure of the cloud seems to be private. The cloud infrastructure is set up within an

organization's datacentre with the scalable resources and applications provided by the cloud vendors. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself. This model is much more secure than the public cloud because it has limited exposure. Only designated stakeholders may have access to operate on a specific private cloud.

2.1.2 Public Cloud: "In this model resources are dynamically provided 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" [2]. The public clouds are maintained by the third party cloud service providers. Public clouds are less secure as they have high level of exposure which places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attack.

2.1.3 Community Cloud: The cloud infrastructure is shared by several organizations that have similar polices, objectives, aims and concerns. The communal concerns are security, compliance, jurisdiction, mission, policy considerations etc. whether managed internally or by a third party and hosted internally or externally. Security seems to be maintained at certain level since people with different requirements might not be interested in the information stored by organizations with same interest.

2.1.4 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" [3]. This model is a composition of two models mentioned above (private and public). In simple terms, the model works on owning a private cloud that is linked to public cloud for some extra services. Organizations can set up their private clouds which can be linked to one or more external cloud services, centrally managed by third party vendors. This model provides high level of security for data and applications as they exist on private cloud and scale up of capabilities because extra services can also be consumed from public clouds. This model reaps in benefits of both private and public clouds. This method overcomes the disadvantage of public cloud structure and limitations of private clouds. It has an open architecture that allows interfaces with other management systems.

2.2 Cloud Computing Service Delivery Models

Next level of security consideration deals with cloud computing service delivery models. These models depict how different services i.e. software, platform, infrastructure can be provided to the cloud clients.

The three main cloud service models are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS).

2.2.1 Software as a Service: "Software as a service is a distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the internet". [4] The capability provided to the customer is to use the provider's application running on a cloud infrastructure. These applications may be accessed from various client devices through an interface such as web browser. SaaS is also often associated with a pay-as-you-go subscription-licensing model. This model is mostly used to provide business software functionality at a low cost that allows customers to obtain the same benefits as of commercially licensed, internally operated software. It provides features like elasticity, emulator, virtual desktop etc. The architecture of SaaS supports multiple users at the same time and hence provides concurrent user system called Multi-Tenancy. SaaS applications are accessed over the internet using web browsers hence browser security is a point of concern here. The cloud users do not manage the cloud platform and infrastructure on which the application is running hence the burden of the security lies with the cloud provider.

2.2.2 Platform as a Service: Platform-as-a-Service (PaaS) is a set of software and development tools hosted on the provider's servers. It is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc. [3]. In this model, cloud providers provide a computing platform like operating system, database or web server to its users. The resources will be scaled automatically to match the user demand. This model offers a developing environment to its users where they can develop their applications completely (from planning to design to develop to test to maintain) without knowing the underlying architecture. Users can deploy their own developed applications onto the cloud infrastructure without installing any platform or tools on their local machines. Since this creates a kind of virtual machine for the user, it must be protected against malicious attacks such as cloud malware. This model offers greater extensibility and a greater customer control because of low degree of abstraction. Hence, it actually maintains the integrity of applications and reinforces accurate authentication checks during the data transfer.

2.2.3 Infrastructure as a Service: Infrastructure as a Service is a basic cloud service model where cloud providers deliver computers as physical or as virtual machines. Apart from machines, they also provide servers, storage, load balancers etc. IaaS is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee.[5] This model acts as a great support system for the organisations as it minimizes the need of initial investments in setting up the hardware components like servers, networking devices and processing powers. In this model, infrastructure services can be used without bothering about underlying hardware complexities as the hardware is completely abstracted. IaaS only provides basic security (perimeter firewall, load balancing, etc.) and applications moving into the cloud will need higher levels of security provided at the host.

Before we start discussing about various security aspects of cloud computing we need to understand the dependencies and relationships amongst these cloud service models. Cloud computing service model is presented in figure 3. According to which SaaS and PaaS, both are hosted above the IaaS layer. Thus, any security breach in IaaS service model will automatically impact the above two service models, and vice versa. PaaS offers a platform for the software development life cycle i.e. SaaS applications, this increases the security dependency between them. Because of these dependencies, any attack to any cloud service model can affect the security of the upper layers. Each model has its own inherent security loopholes but this relational dependency may also be a source of risk.

III. Security Issues In Cloud Computing

With the development in technology market, experts are worried about the security needs for cloud computing. "There's no more debate," says Rajat Bhargava, co founder of JumpCloud, a cloud security start-up. "When you don't own the network, it's open to the rest of the world, and you don't control the layers of the stack, the cloud- by definition- is more insecure than storing data on premises."[6]

Security issues in cloud computing is one of the major hindrance in its adoption. Many companies are trying to resolve these issues but none of them has been 100% successful. Without any second thoughts, putting your own data, running your software on someone else's resources appears to be

daunting. Well-known security issues such as data loss, phishing, botnet are some of the serious threats to organization's data and software. Most of the security issues stem from consumers loss of control, loss of trust and multi-tenancy. The pooled resources in cloud computing has introduced new security challenges which needs to be tackled by some novel technology.

Security issues can be broadly divided into two categories: issues faced by cloud service providers and issues faced by cloud service consumers. The provider must ensure that their infrastructure is secure and their clients' data and applications are protected. Users must take measures to fortify their applications and use strong password and authentication measures.

3.1 Threats and Challenges in Cloud Computing:
For securing any system, first step is to identify the possible threats and challenges, so that appropriate countermeasures can be implemented. The architectural design and characteristics of cloud computing technique itself imposes a number of security benefits such as data and process segmentation, centralization of security, redundancy and high availability. On the other hand, there are many traditional risks associated with it, due to shared approach of software, platform and infrastructure. In general, security is a term that relates the aspects of confidentiality, integrity and availability. These three are the building blocks of designing a secure system. Now we will discuss these with respect to cloud computing design.

3.1.1 Confidentiality
Confidentiality or data privacy means only authenticated users or systems must be authorized to access the data and other resources. It is the right of any person to control the disclosure of personal information. In cloud computing technique this is the biggest challenge due to sharing of cloud resources among large number of parties, devices and applications. This multi-tenancy of same resources provided by the cloud provider at different levels (network, host, application) increses the risks. The users are isolated at the virtual level but the basic hardware for all is same. The approach is very similar to multitasking in OS where processes share common processing resources such as CPU. Same as in multitasking, this model also hinders confidentiality and privacy of information system of an organization and becomes a very serious threat for the cloud users.

Confidentiality of data can be directly correlated to user authentication. Protecting a user's account is a superset of problem that includes access to objects including memory, devices, software etc. Hence a well-formed electronic authentication process is required here that can establish confidence in user identities that are electronically presented to an information system.

Software confidentiality is as important as data confidentiality for a good secure system. This means that specific applications or software will maintain and handle user's data in secure manner. This enrols one more factor 'Trust' in cloud environment. Software platform provided to the user must be certified and only the authorized users can access that software. Unauthorized access is possible only through lack of strong identification or application vulnerability. Thus cloud provider is ultimately responsible to provide a secure cloud that should ensure user's privacy.

3.1.2 Integrity
Integrity means that resources can be modified only by authorized people in authorized ways maintaining the specified standards. Integrity of information system refers to data, software and hardware integrity. Data integrity means protecting data from unauthorized deletion, modification or fabrication. And as discussed earlier same can be achieved by preventing unauthorized access. Due to increased number of access points in cloud environment, authorization is very crucial. Similarly, Software integrity means protection of software from unauthorized deletion, modification or theft. Cloud providers implement a set of software interfaces to manage cloud services. Hardware integrity or network integrity is an additional issue addressed by cloud providers, as they need to protect the underlying hardware from any sort of fabrication or modification from the unauthorized users.

3.1.3 Availability
Availability means that a system or resources are available to the end users as and when they require. This refers to data, software, hardware or other cloud resources being available to authorized persons upon demand. Depending on the user requirement, system should be made available to them. The system should have the ability to continue operations even in the possibility of security breach or overload. From the organization's point of view, time is money, thus they'll move to the cloud only if the uninterrupted and smooth conduct of operations is guaranteed. It is thus responsibility of the cloud provider to guarantee that information and corresponding systems for processing information are available to their multitude of clients upon demand without breaking down.

3.2 Security Issues at various levels
3.2.1 Software-as-a-Service Security Issues:
SaaS provides various software or application services on user demand like conferencing software, or business applications. SaaS users have less control over security of information system among the three cloud service models.

- Appli cation security: Applications are delivered to the user via internet through a web browser. However, flaws in web applications may lead security issues for SaaS applications. Attackers can perform malicious attacks using the web and can steal the data. SaaS security challenges are same as of any web application technology, but traditional security systems are not sufficient to overcome the problem here and hence new technologies are required. Cloud computing technology makes it easy to access applications over the internet via web browser from any device. However, it also exposes additional security risks. The top threats in this area are information stealing mobile malware, insecure network vulnerabilities in device's OS or proximity hacking.
- Multi-tenancy: SaaS applications can be grouped into different models as per the following characteristics: scalability, configurability and multi-tenancy. In the first model, each customer owns the instance of software as per his customized requirement. Security issues are not so bad in this model. In second model, different instances of applications are provided for each customer but all of them use the same application code. Some configurations will be changed to meet their needs but on the same platform. In the third model multitenancy is added, which means that single instance serves all customers. This approach enables efficient use of resources but limits the scalability. Data from multiple sites is likely to be stored in the same database hence this involves high risk of data leakage. Good security policies are required to ensure separation of data of various customers.
- Data security: It is the most common concern in any technology. In SaaS, user's data is processed in plaintext and stored in the database of the cloud. The database resource provider is the one responsible for the security of the data while processing or even storing. Also, they need to maintain backup of the data to facilitate recovery in case of any disaster, but it introduces security aspects also. In the world of SaaS, various compliance issues such as data privacy, segregation and security must be enforced by the cloud provider.

3.2.2 PaaS Security Issues:
This model facilitates deployment of applications on the cloud without spending money in buying the underlying software and hardware architecture. PaaS security depends on secure and reliable network and web browser. This requires two level of security: Security of the runtime engine i.e. PaaS platform and the security of consumer applications deployed on this platform. Same as SaaS, PaaS also brings various security is-

sues described as follows:

- Third party relationships: PaaS model offers third party web services components along with traditional programming languages. This combines more than one source element into a single integrated unit and hence inherit security issues of those as well. PaaS have to depend on security of web-hosted development tools and third party services.
- Software Development life Cycle: Developers face an add-on complexity of developing secure applications that can be hosted on cloud. "The speed at which applications will change in the cloud will affect both the software development life cycle and security"[7]. PaaS applications should be upgraded frequently, to ensure that application development processes are flexible enough to cater changes. However, developers also need to understand changes in PaaS components and related security aspects.
- Underlying infrastructure security: Since developers do not have access to underlying hardware layer, providers are solely responsible for security at this level. Developers can ensure the security of their application, but they do not have the assurance of the development tools provided under PaaS model.

3.2.7 IaaS Security issues:IaaS model provides a shared pool of hardware resources like servers, storage, networks and other computing resources. This creates virtual systems for the users which are accessed through internet. Users can run any software with full control and management on the allocated resources. With Iaas, users have better control over the security. The users can control the software running in their virtual machines and hence solely responsible to configure security policies correctly. However, the underlying infrastructure is controlled by cloud providers. They must take substantial efforts to secure their systems in order to minimize the threats. Some of the security issues associated with IaaS are:

- Virtualization: This allows user to create, share, and run virtual machines, which serves as a platform to run a variety of applications. This also introduces new opportunities for attackers. Virtualized environments are more prone to all types of attacks for normal infrastructure as they have two boundaries to be protected: physical and virtual.
- Shared resources: Virtual machines on the same server share CPU, memory, I/O and other resources. This decreases the security of each virtual machine wherein for example using covert channels, two VM's can communicate with each other bypassing all the rules defined by the security module. Thus, a malicious VM can monitor shared resources without being noticed and the attacker will get information of other virtual machines.
- Virtual Networks: Due to the concept of resource, pooling different tenants will share network components provided by cloud. These virtual networks increase the VM's connectivity, thus allowing attackers to launch cross attacks. The most secure way to handle this is by hooking each VM with its host by dedicated physical channels. However, virtual networks are mostly used to link VMs to communicate directly and efficiently.

3.3 Cloud Security Controls

Cloud security is effective if it is implemented completely. For this, we can recognize the possible issues that can arise with security management. Some predefined security measures are being taken care of by security management people. These controls are used to safeguard the weaknesses of the system to reduce security breach. [8]

3.3.1 Deterrent Controls:

Deterrent means to defend. These controls are like warning signs used to reduce attacks on cloud environment by defending mechanism. The warning signals use a message to inform the potential attackers about the adverse effects of the security breach. Hence, it is like threatening the thief for the theft. This control actually discourages a threat to happen.

3.3.2 Preventive Controls:

As the name says this category of controls prevents security breach to happen. Deterrent Controls can be considered as subset of preventive controls. Preventive controls provide strength to the system against malicious attacks. This controls security breach up to a certain level but cannot eliminate it. Some of the preventive measures are authentication, authorization, access control, identification of cloud users etc.

3.3.3 Detective Controls:

Detective controls are based on detection and reaction policy wherein they first detect the incident and then react appropriately. A detective control will first signal the preventive or corrective control to address the issue and then security monitoring team takes necessary steps. This model is based on the intrusion detection and prevention of attacks on cloud resources and supporting network channels.

3.3.4 Corrective Controls:

Corrective controls come into effect during or after an incident hence reducing the consequences of an attack. This limits the damage caused to cloud infrastructure due to security breach. For example restoring system backups after the attack is one of the corrective controls that will rebuild a compromised system.

IV. Conclusion

Cloud computing is the latest technology which is at its peak of acceptance these days and presents a good number of benefits to its users; however as discussed in this paper it also raises security problems which is slowing down its acceptance. In this paper, we have discussed various levels of security including storage security, middleware security, data security, network security and application security. Storage, virtualization and networks are the biggest threat to secure system. Each cloud service model be it SaaS, PaaS or IaaS and each deployment model be it private, public, community or hybrid cloud has its own concerns with respect to security. The main goal of any cloud service provider is to provide secure environment for the data that is not controlled by the owner of data. Hence, we have discussed various security control measures which if followed by cloud providers can solve the problem to an extent. Bottom up approach can be followed where we need to work on smaller problem to tackle the larger problem of cloud security. Once the smaller problems are handled the entire security of cloud computing can be handled. In our opinion, this is the best approach to solve security issues. Secure co-processors and Hadoop systems can be used to enhance security. With this growing era of technology, many new technologies are emerging at a rapid rate, with new advancements and with the potential of making human life easy. However, before opting for any naive technology one must carefully evaluate all security threats and its challenges.

REFERENCES

[1] S. Arnold (2009, Jul.). "Cloud computing and the issue of privacy." KM World, pp14-22. Available: www.kmworld.com [Aug. 19, 2009]. | [2] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." Platform Computing, pp6, 2010. | [3] Global Netoptex Incorporated. "Demystifying the cloud. Important opportunities, crucial choices." pp4-14. Available: http://www.gni.com [Dec. 13, 2009]. | [4] S. Subashini, and V. Kavitha. (2010) "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. | [5] J. Brodkin. (2008, Jun.). "Gartner: Seven cloud-computing security risks." Infoworld, Available: <http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurity-risks-853?page=0,1> [Mar. 13, 2009]. | [6] Electronic References. Retrieved from: http://www.techtimes.com/articles/8449/20140615/cloud-computing-is-the-future-but-not-if-security-problems-persist.htm. | [7] Morsy MA, Grundy J, Müller I (2010) An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 Cloud Workshop. Sydney, Australia: APSEC. OpenURL. | [8] Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 2010. 179-80. Print. |