TOP THREATS IN CLOUD COMPUTING

Pooja Sharma[1], Rajkumar Singh Rathore[2]

[1]PG Scholar, Masters of Technology ,
Galgotias College of Engineering and Technology, Greater Noida (India)
[2] Assistant Professor , Department of Computer Science & Engineering
Galgotias College of Engineering & Technology, Greater Noida (India)

ABSTRACT

*The purpose of this document, "Top Threats to Cloud Computing", is to provide needed context to assist organizations in making educated risk management decisions regarding their cloud adoption strategies. Many believe that Cloud is reshaping the entire IT industry as a revolution. Today rapid development in web technologies such as blogging, social networking, online media sharing etc. has moving bulk of data onto internet servers. Because of this there arises a need for companies to adopt utility or cloud computing. In this paper, we aim to point out the challenges and security issues in cloud computing as today, security and privacy concerns may represent the biggest hazards to moving services to external clouds. This paper outlines the brief description of cloud delivery and deployment models, cloud security advantages and disadvantages and then detailed discussion of issues and security threats relating to its implementation, datalocation and storage, management, virtualization etc in the Cloud. The aim is to provide some useful security related information for organizations having their data on clouds or for those preparing to migrate to the cloud to take advantage of this latest computing paradigm.***

Keywords: Cloud computing; Security; Public cloud; Private cloud; Hybrid cloud; policies; Security challenges; Cloud security model

I. INTRODUCTİON

Cloud computing has recently emerged as a buzz word in the distributed computing community. Many believe that Cloud is going to reshape the IT industry as a revolution. It is a business model that has inherited the benefit of other technologies such as distributed, pervasive, ubiquitous, utility computing and virtualization [4]. So, what is cloud computing? How these computing services providing ease for organizations to manage and save its data to the cloud? What are the issues and challenges for both cloud providers and its consumers?Here we start with first what is cloud computing:

Definition: Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., 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 everything about a cloud regarding to its architectures, security and deployment strategies. In particular, five essential elements of cloud computing areclearly mentioned:

- *On-demand self-service*: A consumer with an instantaneous need at a particular timeslot can avail computing resources (such as CPU time, network storage, software use, and so forth) in an automatic (i.e. convenient, self-serve) fashion.
- *Broad network access*: These computing resources are delivered over the network (e.g. Internet) and used by various client applications with heterogeneous platforms (such as mobile phones, laptops, and PDAs) situated at a consumer's site.
- *Resource pooling*: A cloud service provider's computing resources are 'pooled' together in an effort to serve multiple consumers using either the *multi-tenancy* or the *virtualization* model, "with different physical and virtual resourcesdynamically assigned and reassigned according to consumerdemand".
- *Rapid elasticit*y: For consumers, computing resources become immediate rather than persistent: there are no up-front commitment and contract as they can use them to scale up whenever they want, and release them once they finish to scale down.
- *Measured Service*: Although computing resources are pooled and shared by multiple consumers (i.e. multi-tenancy), the cloud infrastructure is able to use appropriate mechanisms to measure the usage of these resources for each individual consumer through its metering capabilities.
- Enterprises are now beginning to develop and deploy management software to deal with scaled Cloud environments [2]. They all are also developing their standards and policies for dealing with types of Clouds.
- The rest of this paper is organized as follows. Section 2 outlines the Cloud delivery and deployment approaches. Then, Sections 3rd and 4th discuss, in brief, the advantages and disadvantages of Cloud security and the inherent issues and challenges. The last section consists of the conclusion.

II. CLOUD COMPUTING

2.1 Delivery Models

As shown in *Fig. 1*, the Cloud model consists of, three types of services: Software Services, Platform Services and Infrastructure services. These services are related to three delivery models of Cloud, defined as follows:

- *Software as a service (SaaS)*: allows the users to utilize various applications from the cloud rather than using applications on their own computer. Normally it refers to prebuilt pieces of software or complete applications like an email system, database processing, human resource management, etcwhich are provided as services.
- *Platform as a service (PaaS)*: operates at a lower level than the SaaS. It is responsible for the management of the storage space, bandwidth allocation and computing resources available for the applications. This model refers to application development toolkits and deployment tools e.g. application servers, portal servers and middleware and consumers use these to build and deploy their own applications.
- *Infrastructure as a service (IaaS)*: This refers to infrastructure-centric IT resources such as visualized servers, storage, network devices, operating systems, etc as well as hardware services to enable Cloud platforms and software to operate. It dynamically scales bandwidth allocation and server resources for the cloud. This service allows the cloud to operate during high traffic/demanding situations as resources are dynamically increased as they are needed [2].

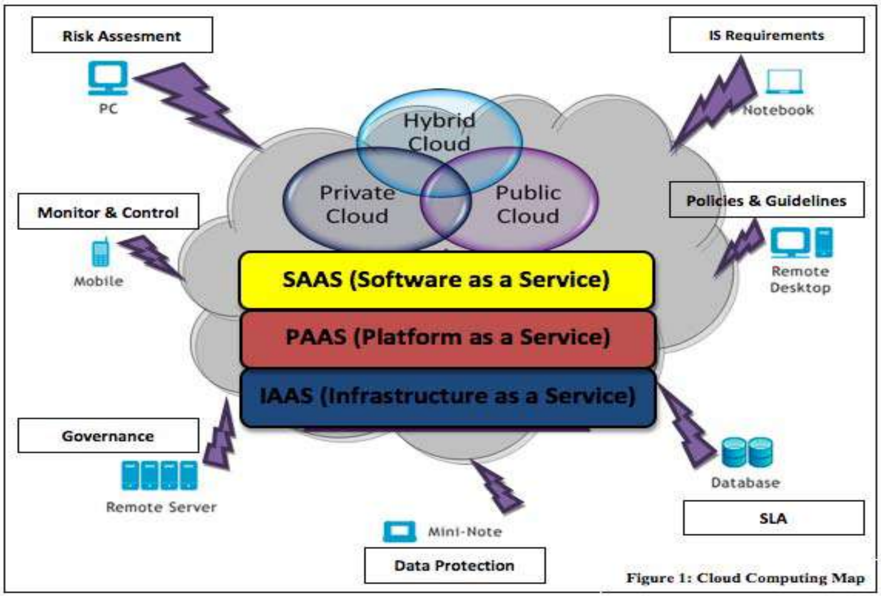

Figure1. Cloud Computing Map [5]

2.2 Deployment Approaches

There are three main types of cloud deployment models - public, private and hybrid clouds[10].

- *Public Clouds* – are the most common type of cloud. This is where multiple customers can access web applications and services over the internet. It's typically based on a pay-per-use model. Each individual customer has their own resources which are dynamically provisioned by a third party vendor. This third party vendor hosts the cloud for multiple customers from multiple data centers (see Figure 2), manages all the security and provides the hardware and infrastructure for the cloud to operate. The customer has no control or insight into how the cloud is managed or what infrastructure is available. Technically there may be little or no difference between public and private cloud architecture, however, security consideration may be substantially different for services (applications, storage, and other resources) that are made available by a service provider for a public audience and when communication is effected over a non-trusted network[11]. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attack [5].

- *Private Clouds* – emulate the concept of cloud computing on a private network. They allow users to have the benefits of cloud computing without some of the pitfalls. A private cloud is setup within an organisation's internal enterprise datacenter. Private clouds grant complete control over how data is managed and what security measures are in place. This can lead to users having more confidence and control. In this Cloud users can easily share and use the scalable resources and virtual applications (that are pooled together) provided by the cloud vendor. Utilization on the private cloud can be much more secure because of its specified internal exposure. The major issue with this deployment model is that the users have large expenditures as they have to buy the infrastructure to run the cloud and also have to manage the cloud themselves.

- *Hybrid Clouds* – Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models [11]. It provides virtual IT solutions through a mix of both public and private clouds (provisioned as a same unit) within the same network. Hybrid Clouds provide more secure control of the data and applications. For example, an organisation could hold sensitive information on their private cloud and use the public cloud for handling large traffic and demanding situations.

To summarise, in the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand [5]. Security considerations are the measure issue in deciding which type of cloud to deploy from an enterprise architectural point of view. Hence, there is a need of taking into account the information security differences of each model discussed above.

III CLOUD THREATS

There has been much debate about what is "in scope" for this research. We expect this debate to continue and for future versions of "Top Threats to Cloud Computing" to reflect the consensus emerging from those debates. While many issues, such as provider financial stability, create significant risks to customers, we have tried to focus on issues we feel are either unique to or greatly amplified by the key characteristics of Cloud Computing and its shared, on-demand nature. We identify the following threats
in our initial document:

1. Abuse and Nefarious Use of Cloud Computing
2. Insecure Application Programming Interfaces
3. Malicious Insiders
4. Shared Technology Vulnerabilities
5. Data Loss/Leakage
6. Account, Service & Traffic Hijacking
7. Unknown Risk Profile

1) Abuse and Nefarious Use of Cloud Computing

Description

IaaS providers offer their customers the illusion of unlimited compute, network, and storage capacity — often coupled with a 'frictionless' registration process where anyone with a valid credit card can register and immediately begin using cloud services. Some providers even offer free limited trial periods. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. PaaS providers have traditionally suffered most from this kind of attacks; however, recent evidence shows that hackers have begun to target IaaS vendors as well. Future areas of concern include password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables, and CAPTCHA solving farms.

Examples

IaaS offerings have hosted the Zeus botnet, InfoStealer trojan horses, and downloads for Microsoft Office and Adobe PDF exploits. Additionally, botnets have used IaaS servers for command and control functions. Spam continues to be a problem — as a defensive measure, entire blocks of IaaS network addresses have been publicly blacklist.

Remediation

- Stricter initial registration and validation processes.
- Enhanced credit card fraud monitoring and coordination.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one's own network blocks.

Impact

Criminals continue to leverage new technologies to improve their reach, avoid detection, and improve the effectiveness of their activities. Cloud Computing providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited.

2) Insecure Interfaces and APIs

Description

Cloud Computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and both accidental and malicious attempts to circumvent policy. Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to thirdparties in order to enable their agency.

Examples

Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring and logging capabilities,
unknown service or API dependencies.

Remediation

- Analyze the security model of cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Understand the dependency chain associated with the API.

Impact

While most providers strive to ensure security is well integrated into their service models, it is critical for consumers of those services to understand the security implications associated with the usage, management, orchestration and monitoring of cloud services. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.

3) Malicious Insiders

Description

The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance. To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary — ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The level of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection.

Examples

No public examples are available at this time.

Remediation

- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Specify human resource requirements as part of legal contracts.
- Require transparency into overall information security and management practices, as well as compliance reporting.
- Determine security breach notification processes.

Impact

The impact that malicious insiders can have on an organization is considerable, given their level of access and ability to infiltrate organizations and assets. Brand damage, financial impact, and productivity losses are just some of the ways a malicious insider can affect an operation. As organizations adopt cloud services, the human element takes on an even more profound importance. It is critical therefore that consumers of cloud services understand what providers are doing to detect and defend against the malicious insider threat.

4) Shared Technology Issues

Description

IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (*e.g.*, CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. To address this gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Still, even hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform. A defense in depth strategy is recommended, and should include compute, storage, and network security enforcement and monitoring. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider. Customers should not have access to any other tenant's actual or residual data, network traffic, etc.

Examples

- Joanna Rutkowska's Red and Blue Pill exploits
- Kortchinksy's CloudBurst presentations.

Remediation

- Implement security best practices for installation/configuration.
- Monitor environment for unauthorized changes/activity.
- Promote strong authentication and access control for administrative access and operations.

- Enforce service level agreements for patching and vulnerability remediation.
- Conduct vulnerability scanning and configuration audits.

Impact

Attacks have surfaced in recent years that target the shared technology inside Cloud Computing environments. Disk partitions, CPU caches, GPUs, and other shared elements were never designed for strong compartmentalization. As a result, attackers focus on how to impact the operations of other cloud customers, and how to gain unauthorized access to data.

5) Data Loss or Leakage

Description

There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data. The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment.

Examples

Insufficient authentication, authorization, and audit (AAA) controls; inconsistent use of encryption and software keys; operational failures; persistence and remanence challenges: disposal challenges; risk of association; jurisdiction and political issues; data center reliability; and disaster recovery.

Remediation

- Implement strong API access control.
- Encrypt and protect integrity of data in transit.
- Analyzes data protection at both design and run time.
- Implement strong key generation, storage and management, and destruction practices.
- Contractually demand providers wipe persistent media before it is released into the pool.
- Contractually specify provider backup and retention strategies.

Impact

Data loss or leakage can have a devastating impact on a business. Beyond the damage to one’s brand and reputation, a loss could significantly impact employee, partner, and customer morale and trust. Loss of core intellectual property could have competitive and financial implications. Worse still, depending upon the data that is lost or leaked, there might be compliance violations and legal ramifications.

6) Account or Service Hijacking

Description

Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

Examples

No public examples are available at this time.

Remediation

- Prohibit the sharing of account credentials between users and services.
- Leverage strong two-factor authentication techniques where possible.
- Employ proactive monitoring to detect unauthorized activity.
- Understand cloud provider security policies and SLAs.

Impact

Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Organizations should be aware of these techniques as well as common defense in depth protection strategies to contain the damage (and possible litigation) resulting from a breach.

7) Unknown Risk Profile

Description

One of the tenets of Cloud Computing is the reduction of hardware and software ownership and maintenance to allow companies to focus on their core business strengths. This has clear financial and operational benefits, which must be weighed carefully against the contradictory security concerns — complicated by the fact that cloud deployments are driven by anticipated benefits, by groups who may lose track of the security ramifications. Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts, and security design, are all important factors for estimating your company’s security posture. Information about who is sharing your infrastructure may be pertinent, in addition to network intrusion logs, redirection attempts and/or successes, and other logs. Security by obscurity may be low effort, but it can result in unknown exposures. It may also impair the in-depth analysis required highly controlled or regulated operational areas.

Examples

- IRS asked Amazon EC2 to perform a C&A; Amazon refused.
  http://news.qualys.com/newsblog/forrester cloud-computingqa. html
- Heartland Data Breach: Heartland’s payment processing systems were using known-vulnerable software and actually infected, but Heartland was “willing to do only the bare minimum and comply with state laws instead of taking the extra effort to notify every single customer, regardless of law, about whether their data has been stolen.”
  http://www.pcworld.com/article/158038/heartland_has_no_heart_for_violated_customers.html

Remediation

- Disclosure of applicable logs and data.
- Partial/full disclosure of infrastructure details (*e.g.*, patch levels, firewalls, etc.).
- Monitoring and alerting on necessary information

Impact

When adopting a cloud service, the features and functionality may be well advertised, but what about details or compliance of the internal security procedures, configuration hardening, patching, auditing, and logging? How are your data and related logs stored and who has access to them? What information if any will the vendor disclose in the event of a security incident? Often such questions are not clearly answered or are overlooked, leaving customers with an unknown risk profile that may include serious threats.

IV CONCLUSION

In this paper, we explored the security issues and challenges at various domains of cloud computing. We reviewed the present ongoing security issues to make the customers aware of the problem that will arise in cloud computing paradigm. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. However, one must be very careful to understand the security risks and challenges posed during utilization of these cloud computing technologies. Hence our concern is to provide a collective review of all these present issues in a single paper to provide ease to the cloud customers.

REFERENCES

[1] Tharam Dillon, Chen Wu and Elizabeth Chang, “Cloud computing : issues and challenges,” IEEE, 2010 [24th IEEE International Conference on Advanced Information Networking and Applications].

[2] ZaighamMahmood, “Data location and security issues in cloud computing,” IEEE, 2011 [International conference on Emerging Intelligent Data and Web Technologies].

[3] Sara Hamounda, “Security and privacy in cloud computing,” IEEE, 2012 [International Conference on Cloud Computing, Technologies, Applications & Management].

[4] Mervat Bamiah, Sarfraz Bohri, Suriayati Chuprat, Muhammad Nawaz Brohi, “Cloud implementation security challenges,” IEEE, 2012 [International Conference on Cloud ComputingTechnologies, Applications& Management].

[5] Ramgovind S, Eloff MM and Smith E, “The management of security in cloud computing,” IEEE, 2010.

[6] GurudattKulkarni, JayantGhambhir, TejswiniPatil, Amruta Dongare, “A security aspects in cloud computing,” IEEE, 2012.

[7] AkhilBehl, KanikaBehl, “An analysis of cloud computing Security Issues,” IEEE, 2012.

[8] Hsin-Yi Tsai, Melanie Siebenhaar, Andre Miede, Yu-Lu Huang, Ralf Steinmetz, “Threat as a service? Virtualization’s impact on cloud security,” IEEE, January/February 2012.

[9] Xiangyang Lou, Lin Yang, Linru Ma, Shanming Chu, Hao Dai, “Virtualization security risks and solutions of cloud computing via divide-conquer strategy,” IEEE, 2011 [Third International conference on Multimedia Information Networking and Security].

[10] Sean Carlin, Kevin Curran, “Cloud Computing Security,” International Journal of Ambient Computing and Intelligence, pp. 14-19, January-March 2011.

[11] Google. (2014). Cloud computing – Wikipedia. [online]. Available:http://en.wikipedia.org/wiki/Cloud_computing.