IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 3, Mar 2014, 101-106

SECURITY THREATS TO CLOUD COMPUTING

LEKSHMY D. KUMAR[1] & B. R. SHANKAR[2]

[1]M.Tech Student, Department of Mathematical and Computational Sciences, NITK,
Mangalore, Karnataka, India

[2]Associate Professor, Department of Mathematical and Computational Sciences, NITK,
Mangalore, Karnataka, India

ABSTRACT

Cloud Computing is a model for delivering information technology services in which resources are retrieved from The Internet through web based tools and applications, rather than direct connection to the server and resources are provided as long as connected to the web. Cloud Computing has become a viable business and technological proposition because of the significant reduction in both infrastructure and operational costs that it offers when compared to traditional IT services. As cloud computing is increasing its popularity, concerns are being raised about the security issues associated with the adoption of the new model.

Data Security is one of the most critical aspects in a cloud computing environment due to the sensitivity and importance of information stored in the cloud. Data resides in resources not in the purview of data owner or one which could be accessed by cloud administrators depending on implementation. This paper discuss about the various data security threats and challenges that are to be considered and counter measures to be taken by organization before moving their information into the cloud.

KEYWORDS: Security, Privacy, Compliance, Data Breach, Vulnerability, Policy

INTRODUCTION

Cloud Computing is an emerging technological development that leverages the Internet to provide unparalleled distributed computing service based on service oriented architecture and virtualisation. Cloud Computing is a subscription based service where you can obtain networked storage space and computer resources. The cloud makes it possible to access information anytime from anywhere.

Cloud computing is named so because the information which is being accessed is available in the cloud and the user need not be in a specific place to access the information. You only need to buy the amount of storage space, computing resource, software etc that you will use, a business can purchase more resources or reduce their subscription as their business grows or as they find they need less storage space.

CLOUD COMPUTING FRAMEWORK

According to IEEE “Cloud Computing is a paradigm in which information are permanently stored in servers on the Internet and cached temporarily on clients that include desktops, entertainment centers, table computers, notebooks, wall computers, hand-held devices, sensors, monitors etc.”

ESSENTIAL CHARACTERISTICS

On-Demand Self-Service: This means that cloud services can be used as and when required without prior subscription. A consumer can unilaterally upgrade/degrade computing capabilities, such as server time, data storage and network storage, automatically as and when needed without requiring human interaction with each service provider.

Ubiquitous Network Access: The cloud offers infinite network access to vast infrastructure and computing resources such as storage facility, memory, processor, hosting etc. The available resources can be accessed over the Internet through standard mechanisms.

Resource Pooling: The cloud uses shared pool of resources which is located at various parts of world, making the cloud location-independent. The providers serve multiple clients, customers or tenants with different physical and virtual resources dynamically assigned and reassigned according to the customer demand.

Rapid Elasticity: The computing capabilities can be elastically assigned and released, in some cases automatically, with demand. But to the consumer, the capabilities available for provisioning often appear to be unlimited and can be changed in any quantity at any time.

Measured Service: The cloud services are controlled and monitored by the cloud service provider. Measured service is crucial for billing, resource optimization, access control, capacity planning and others. This also provides transparency for both the provider and the consumer of the utilized service.

SERVICE MODELS

Software as a Service(SaaS): Cloud based applications or software run on distant computers in the cloud that are owned and operated by others and that connect to user's computers via Internet usually by a web browser.

Platform as a Service(PaaS): Platform as a Service provides a cloud based environment with everything required to support the complete life cycle of building and delivering web based(cloud) applications, without the cost and complexity of buying and managing the underlying hardware, software, provisioning and hosting.

Infrastructure as a Service(IaaS): Infrastructure as a Service provides companies with computing resources including servers, networking, storage and data centre space on a pay-per-use basis.

DEPLOYMENT MODELS

Private Cloud: Private cloud is owned and operated by a single company that controls the way virtualised resources and automated services are customised and used by various lines of business and constituent groups.

Community Cloud: Community cloud is a multi-tenant infrastructure that is shared among several organizations from a specific group with common computing concerns.

Public Cloud: Public clouds are owned and operated by companies that use them to offer rapid access to affordable computing resources to other organizations or individuals.

Hybrid Cloud: Hybrid cloud uses a private cloud foundation combined with strategic use of public cloud services. A cloud computing environment in which an organization provides and manages some resources in-house and has others provided externally.

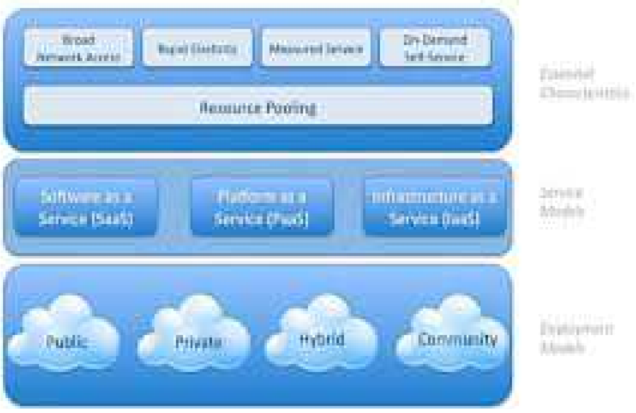

Figure 1: Cloud Computing Framework

RISKS TO CLOUD COMPUTING

In cloud computing the service provider provides resources such as software, platform and infrastructure. The user information/data also resides in the cloud. The risk with this type of service is that the data can be abused, stolen, distributed, compromised or harmed. There is no guarantee that the user's data will not be sold to its competitor. Other risks include privacy, data protection, ownership, location and lack of reliable audit standard to data security procedure of most cloud service providers.

Privacy Issues

Privacy is difficult to achieve using traditional information security systems, and so is one of the challenging area of Cloud Computing. Cloud computing has significant implications for the privacy of personal information as well as maintaining the confidentiality of business and government information. In public cloud various sensitive information are given to the hands of a third party service provider whose cloud infrastructure may not have proper regulations and could propagate through geographical borders that impact both legal and regulatory requirements of the information being propagated or stored. Cloud users must be aware of the contract they sign with service provider and should be informed about the service provider's privacy and security guidelines and practices.

Data Ownership and Content Disclosure Issues

Another issue which is to be considered before migrating to cloud is data ownership of the information residing on the cloud. Once the data is put to the cloud, not only the privacy is lost, the data ownership and the right of data content disclosure is also lost. Cloud users must protectively mark(TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED, PROTECT) their information and explicitly specify the ownership of information in the service contract.

Data Confidentiality

The confidentiality of a system is guaranteed if it prevents unauthorized gathering of information. Cryptographic techniques and access controls based on strong authentication are normally used to protect confidentiality. The data in a cloud computing system is very often in motion due to the system’s dynamic and open nature. A cloud provider must be able to store this data on a server of its own choice in order to optimize its infrastructure capacity and ensure the necessary performance. These processes are usually outside the customer’s sphere of influence and can lead to confidentiality problems, for instance, if the data crosses territorial borders or is stored on a less secure system.

Data Location

Another major concern about cloud computing is the data location. Cloud computing offers high degree of data mobility. After the data is handed over to the cloud provider, the data owner have no control over the location of data in the cloud. Where does the data reside that has been created by data owners? The countries legal protection will not be applicable to the data once it is moved outside the country. A foreign government may be able to access the data.

If that country has laws that you are comfortable with, data may be physically stored in database with other company's data. To achieve regulatory compliance in the cloud, it requires effort from both users and cloud provider, the users know about the information requirements and can communicate that clearly to the cloud provider and the cloud provider is transparent and willing to provide regulatory rules required to protect the assets.

Data Breaches

A malicious hacker can extract private cryptographic keys if the multi-tenant service provider database is not designed properly, a single flaw in one client's application could allow to get not just client's data but every other client’s data as well. You can encrypt the data to reduce the impact but if the encryption key is lost, your data will be lost.

Control Issues

Cloud especially public cloud is highly uncontrollable. In order to control cloud services and practices use of legal, regulatory, compliance and certification practices are recommended which is quite difficult to maintain. The location-independency makes it more difficult to achieve regulatory security compliance.

Service Traffic Hijacking

If an attacker gain access to user's credentials, the attacker can monitor user activities, manipulate user data and can return falsified information and can redirect client to illegitimate sites. The user's account will become new base for the attacker. To prevent this protect the credentials, avoid sharing of credentials between users and services.

Insecure Interfaces and APIs

Administrators rely on interfaces for cloud provisioning, management, orchestration and monitoring and APIs are integral to security and availability of general cloud services. Organizations and Third parties build on these interfaces injecting add-on services. This increase risk as organization may be required to exchange the credentials to the third party. An organization must properly understand the implications associated with cloud provisioning, management, orchestration and monitoring.

Denial of Service

The organizations are dependent on 24/7 availability of one or more services. A cloud provider uses virtual machines that run on physical hosts which are shared resources. These resources which include networking systems can be overloaded in certain situations. If one customer is target of attack it is possible that unrelated customer is also affected by the same attack. The cloud provider must protect customers from such attacks. The customer must be aware of the potential and take steps to provide assurances that their services are not adversely affected.

Shared Technology Vulnerability

Vulnerability is prominent factor of risk. It is the probability that an asset will be unable to resist the actions of a threat agent. Shared technology delivers the services in a highly scalable fashion. But in some cases, underlying components were not designed to offer strong isolation capabilities for a multi-tenant deployment. Cloud providers must have in-depth defense strategy that includes computer, storage and network security enforcement and monitoring. Strong compartmentalization should be used to ensure that individual customers do not impact other tenants on the shared infrastructure.

Regulatory and Legislative Issues

A company is responsible for any accounting or financial wrongdoings, even if these are the result of third party, cloud service provider. If the company fails, it is the responsibility of the service provider to ensure regulatory and legislative compliance. A cloud service provider stores the data in various geographical locations to reduce costs and improve reliability. There should be guidance on what corporate institutions can put in the cloud and what not. The easiest way is to look for providers who are already compliant themselves.

Forensic Evidence Issues

In cloud when a crime occurs what information can be legally accepted as forensic evidence? If information is gathered from a public cloud how authentic is that compared with when similar information is gathered from private cloud.? With pretrial discovery and e-discovery, as cloud provider is the data custodian and user is the lawful data owner, who should provide pretrial evidence to the court and who is responsible to discovery and litigation subjects.?

Since copies of information is stored in the cloud, which is the authentic copy of information that is admissible in a court of law.? Different cloud deployment model provides different level of security, privacy so it is mandatory that cloud users must evaluate the security, privacy, legal and regulatory requirements of their information before choosing a cloud model and cloud service provider.

Auditing Issues

Auditing is done so as to evaluate policies, practices, operations and technical controls of an organization to assess compliance, detection, protection and security forensics. Regular security audits are required. Proactive audits are required to assess whether the security controls and procedures prevent this protect the credentials, avoid sharing of credentials between are functioning properly and whether they are adequate to secure the organization's assets. Similarly reactive audits are done when an incident occurs. Auditing security requirements are difficult and challenging in cloud environment. One method is the cloud provider makes the customers aware of the audit process and different levels of audit coverage. By this approach the trust between cloud service provider and customer can be achieved.

Business Continuity and Disaster Recovery Issues

Cloud computing is dynamic and provides ubiquitous on-demand network access to a wide range of shared pool of resources. Information in the cloud could be unavailable due to natural disaster or deliberate attacks. Users must be concerned about the information stored in the cloud. Cloud providers rent infrastructure from other cloud providers. If one service provider is down there is high chance that other service provider suffers same losses affecting wider range of cloud users. So the cloud users must understand the disaster recovery procedures. Moreover user must be aware of the service provider's business continuity plans and whether recovery is built as an abstraction to all layers of its services.

Security Policy Issues

Another major concern is whose security policies governs the cloud, the user's or the cloud service provider's. Obviously it is the provider's polices which specify the service level agreement. But what happens if the service policy of cloud provider is not acceptable by the user, because the agreement may be missing some policies which the user thinks is essential for achieving the security requirements for their data. To ensure that the data in the cloud is properly maintained the data users must carry out due diligence on the provider, must appropriately classify the information to determine their security and regulatory compliance requirements, must consider viability of each cloud model in relation to their information assets requirements and also consider the return of investment of the cloud in relation to the security of the information.

CONCLUSIONS

Cloud Computing is a technology that offers unparalleled distributed computing resources at affordable infrastructure and operating costs. But cloud requires careful and vigilant attention from both users and providers due to the inherent risks associated with the technology. Traditional security mechanisms may not work well in cloud environments because of its underlying complex architecture. However, new security measures are required that can work well with cloud architecture.

REFERENCES

1. Nick Antonopoulos, Lee Gillam “Security Issues to Cloud Computing,” in Cloud Computing Principles, Systems and Applications, 2010, XVIII, 382 p.

2. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, “A view of cloud computing,” Communications of the ACM, 2010.

3. R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. “Cloud Security Issues.” In PROC ‘09 IEEE International Conference on Services Computing,’ 2009.

4. B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010.