IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 4 (Mar. - Apr. 2013), PP 33-37
www.iosrjournals.org

Security and Privacy Issues of Cloud Computing; Solutions and Secure Framework

Sherin Sreedharan
(*Dr. MGR Educational and Research Institute, Chennai*)

Abstract :*The National Institute of Standards and Technology (NIST) defined cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or cloud provider interaction [Def:1]. Cloud computing has the potential to change how organizations manage information technology and transform the economics of hardware and software at the same time. Cloud computing promised to bring a new set of entrepreneurs who could start their venture with zero investment on IT infrastructure. How ever this captivating technology has security concerns which are formidable. The promises of cloud computing, especially public cloud can be shadowed by security breaches which are inevitable. As an emerging information technology area cloud computing should be approached carefully. In this article we will discuss the security and privacy concerns of cloud computing and some possible solutions to enhance the security. Based on the security solutions suggested i have come up with a secured framework for cloud computing.*
Keywords**:** *Cloud computing, Security and Privacy, Information Technology, IT, Software as a service, Platform as a service*

I. Introduction

Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends Information technology‘s existing capabilities. Cloud computing promotes availability, zero maintenance, subscription based service. There exist different service models of cloud computing namely cloud software as a service which allows the consumers to use service providers‘ applications over the network. Cloud platform as a service allows consumers to deploy applications on to providers‘ platform. Consumers do not have to manage or control infrastructure including network servers, operating systems or storages but has control over the deployed area. Cloud Infrastructure as a service is also referred as Hardware as a service. This provides on demand storage on the cloud. It primarily focuses on providing IT resources, processing power, storage, data centre space, services and compliance – on demand. Organizations should have a well defined methodology before migrating to cloud computing. Moving the application to the cloud depends on the security objectives of an organization, cloud computing should be approached carefully with due consideration of the sensitivity of data that the organization is planning to move beyond their firewall. The less control you have for your data means more you have to trust the providers‘ security policies. Security and privacy issues have to be addressed from the initial phase, considering after the deployment will be more complicated, expensive and risky. Every organization should thoroughly study the safety measures and policies followed by the provider and should make sure that it is aligned with the privacy and security requirements of the organization. In the past the cloud services that faced security breach was never expected to succumb to vulnerabilities and it‘s evident that cloud providers also face the security concerns faced by other organizations. The usual security norm in public cloud is service level agreements (SLAs) which talks about the expected level of services provided by the cloud provider to the cloud consumer. Consumers should make sure that the contract they sign have reference to the security measures that the provider have in mind and also make sure that the contract meet the expected security norms from their business perspective. SLAs are usually of two types, off-the-shelf non negotiable contracts and customized negotiable agreements. Public clouds usually follow non negotiable SLA‘s which may not be acceptable for business that have crucial data. Organizations who want to deploy critical applications can think about private clouds over public clouds which offer better insight and control over security and privacy.

II. The Jeopardizes Of Cloud Computing

Cloud computing encompasses a client and a server .Client side security is always over looked. As first step towards secure data management business should strengthen the client side security. To provide physical and logical safety to client machine is a big challenge. Built in security measures can be eluded by an erudite person with out much difficulty. To maintain secure client, organizations should review existing security practices and employ additional ones to ensure the security of its data. Clients must consider secure VPN to connect to the provider.Web browsers are majorly used in client side to access cloud computing services.

Cloud providers usually provide the consumers with APIs which is used by the latter to control, monitor the cloud services. It is vital to ensure the security of these APIs to protect against both accidental and malicious attempts to evade the security. The various plug-ins and applications available in the web browsers also causes a serious threat to the client systems used to access the provider. Many of the web browsers do not allow automatic updates which will append to the security concerns. To ensure secure cloud organizations should work on the existing internal policies and improvise its security strategies if necessary.

III. Security Concerns

` There exist many security concerns in server side. To adopt cloud computing it is necessary to ensure providers security measures. To enhance the trust factor providers can get their system verified by external organizations or by security auditors. Aside from the security factor other issues that needs attention is about the data in the cloud, if at the provider goes bankrupt or being acquired by another business. Traditional data centers used to have regular security audit and mandatory security certifications which ensure the data security. Cloud providers should also incorporate these measures to assure secure transaction among its customers. Issues concerning data ownership is an on going debate and it is a crucial aspect in cloud computing. When consumers migrate critical company data to the cloud they are not giving the data tenure to the providers. Providers should ensure that the business-data customers store on the cloud should not be compromised under any circumstances. It is mere common sense that the right to use data, manipulate, modify and ownership of data stored in the cloud is customers and there should be an agreement in place that prohibits the data usage by providers. In traditional data centers business had the privilege to know about the data flow, exact data location, precautions used to protect data from unauthorized access. In public cloud the idea of data storage is distinct; business is unlikely to know where and how the data is stored, when data is moved, and what particular security measures are in place. The ‗physical location' raises the question of legal governance over the data. Another impediment issue is incase of disputes arises between the provider and the customer, which country's court system will settle the issue. [Def 2]. Another confront of cloud computing is the privacy breach. In case of privacy infringement due to providers fault the confusion still exist on who will take the responsibility and will compensate to the affected people. Lack of common security standards also adds to the concern of data storage over cloud.

IV. Lack Of Control Over The Data

Two recent events have exposed the dark sides of cloud computing for both businesses and consumers. These incidents—the partial outage of Amazon's EC2 cloud service and the security breach of Sony's PlayStation Network and Qriocity music service—underscore a key issue of the cloud computing model: customers' lack of control over their data.[Def 4]. Non cloud services also have security concerns but cloud has additional risk of external party involvement and exposure of critical and confidential data outside organizations control. Modifying security measures or introducing pristine best practices relevant to one particular organization is also unattainable. Cloud provider stores the data in providers side and maintenance is exclusively done by the providers hence clients have no means to check on the providers security practices, providers employees, their skills specializations etc. Insider threats go beyond those posed by former employees to include contractors, organizational affiliates, and other parties that have received access to an organization's networks, systems, and data to carry out or facilitate operations [Def 5]

Many incidents can occur like sabotage of information, theft of confidential information. Incidents may also be caused unintentionally where employees mistakenly send across the sensitive data to wrong recipient.

V. Network Security

Public cloud services are delivered over the internet, exposing the data which were previously secured in the internal firewalls. Applications which people used to access within organizations intranet are hence exposed to networking threats and internet vulnerabilities which includes distributed denial of service attacks, phishing, malwares and Trojan horses. If an attacker gains access to client credentials, they can eavesdrop on all activities and transactions, manipulate data, return falsified information, and redirect 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. [Def 7].

VI. Securing Data In The Cloud

A secure infrastructure ensures and builds confidence that the data stored is secure in providers' side. Proper implementation of security measures is mandatory in cloud computing. The fact that application is launched over the internet makes it susceptible for security risks. Cloud providers should think beyond the customary security practices like restricted user access, password protection etc. Physical location of stored data

is also vital and it's the responsibility of the provider to choose the right location of storage. Restricted user access can vary from simple user name / password protection to CAPTCHA log in forms. When an employee no longer has a business need to access datacenter his privileges to access datacenter should be immediately revoked. Cloud Providers can also consider one time password authentication where the clients will get one time temporary password from SSN /mobile device which helps in data security even if password is compromised.

VII. Installation And Maintenance Of Firewall

Installation of firewall and its maintenance is mandatory to ensure the protection. A firewall should be present in all external interfaces. A list of necessary port and services should be maintained. Assessment of firewall policies and rule sets and reconfiguration of router should be done in regular intervals. Build and deploy a firewall that denies access from ―untrusted‖ sources or applications, and adequately logs these events. Build and deploy a firewall that restricts access from systems that have direct external connection and those which contain confidential data or configuration data. [Def 13].

VIII. Data Encryption

In public cloud the resources are shared by multiple cloud consumers and hence its providers responsibility to bestow data separation among their clients. Data encryption is one common approach the providers follow to safe guard their clients data but the question is whether the data is getting stored in encrypted format or not. Many providers follow private/public key encryption to ensure data security. To store crucial data organizations can think of private or hybrid cloud where the data will be in secure corporate firewall. Providers should allow the customers to determine the security measures followed, data storage details so that the customer can ensure data security.

Data access to the cloud by the employees should be monitored and recorded so that the providers will be able to furnish the detailed report of who has accessed what data at a given point of time.

IX. Back Up And Recovery

In cloud computing data is stored in distributed location. The cloud customers will never be able to make out the exact storage location of their records and there comes the importance of data back up and recovery. Backup software should include public cloud APIs, enabling simple backup and recovery across major cloud storage vendors, such as Amazon S3, Nirvanix Storage Delivery Network, Rackspace and others, and giving consumers flexibility in choosing a cloud storage vendor to host their data vault. [Def 8] One debatable question is whether to back up the entire data or to backup critical and vital data. If provider agrees to backup crucial data then the question arises on how to determine the priority of data. The easiest and least complicated way is to protect the entire workstation or the server.

It is critical for the backup application to encrypt confidential data before sending it offsite to the cloud, protecting both data-in-transit over a WAN to a cloud storage vault and data-at-rest at the cloud storage site. Consumers need to verify that the cloud backup software they choose is certified and compliant with the Federal Information Processing Standards (FIPS) 140 requirements issued by the National Institute of Standards and Technology. FIPS 140 certification is required for government agencies as well as for regulated financial, healthcare and other industries for compliance with data retention and security regulations such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley and other legal requirements. [Def 6]

A growing number of cloud providers support the SAML standard and use it to administer users and authenticate them before providing access to applications and data. SAML provides a means to exchange information, such as assertions related to a subject or authentication information, between cooperating domains. SAML request and response messages are typically mapped over the Simple Object Access Protocol (SOAP), which relies on the eXtensible Markup Language (XML) for its format. SOAP messages are digitally signed. For example, once a user has established a public key certificate for a public cloud, the private key can be used to sign SOAP requests.

SOAP message security validation is complicated and must be carried out carefully to prevent attacks. For example, XML wrapping attacks have been successfully demonstrated against a public IaaS cloud [Gaj09, Gru09]. XML wrapping involves manipulation of SOAP messages. A new element (i.e., the wrapper) is introduced into the SOAP Security header; the original message body is then moved under the wrapper and replaced by a bogus body containing an operation defined by the attacker [Def 10, Def 11]. The original body can still be referenced and its signature verified, but the operation in the replacement body is executed instead.

SAML alone is not sufficient to provide cloud-based identity and access management services. The capability to adapt cloud subscriber privileges and maintain control over access to resources is also needed. As part of identity management, standards like the eXtensible Access Control Markup Language (XACML) can be used by a cloud provider to control access to cloud resources, instead of using a proprietary interface. XACML focuses on the mechanism for arriving at authorization decisions, which complements SAML's focus on the

means for transferring authentication and authorization decisions between cooperating entities. XACML is capable of controlling the proprietary service interfaces of most providers, and some cloud providers already have it in place. Messages transmitted between XACML entities are susceptible to attack by malicious third parties, making it important to have safeguards in place to protect decision requests and authorization decisions from possible attacks, including unauthorized disclosure, replay, deletion and modification [Def 9].

X. Security Enhancements For Cloud Computing

The Following Practices Can Be Followed To Improvise The Security Of Cloud Computing

- Implement security practices at organizational level and make sure that the providers security plans are in alignment with the business.
- Employ and maintain secure Infrastructure in client side (secure VPN , changing default vendor provided passwords) and host side (firewalls , patch managements ,anti-virus updates)
- Ensure accurate user permissions and restricted access at both sides

Data sanitizations at the right time

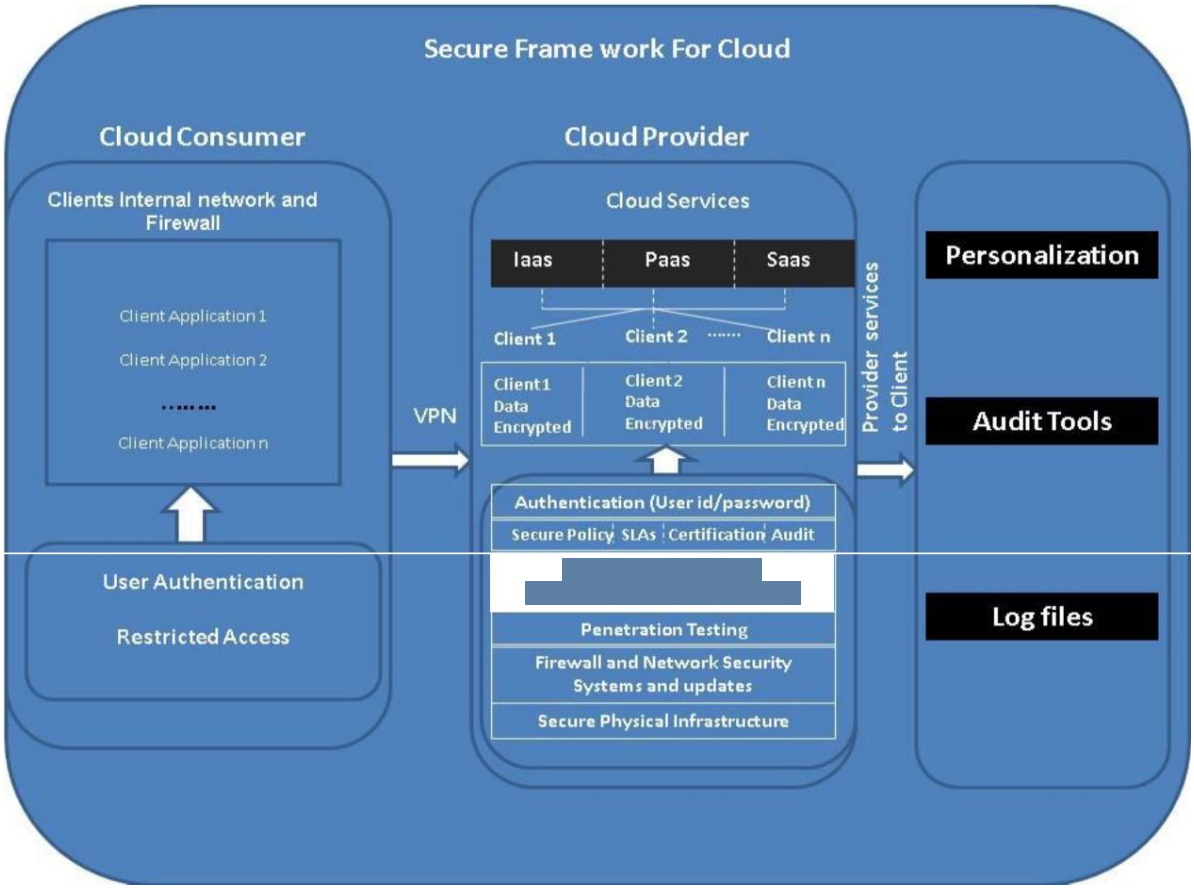
The above deployed frame work offers a secured environment in which the clients need to access the providers' network using secured VPN.

Cloud Providers have number of clients and they may offer any of the services namely Iaas, Paas, Saas.

In this framework the providers check for user authentication, make sure that the clients approaching them are authorized and genuine. Once the providers are confident about the clients' credentials their data will be encrypted and stored.

Steps involved in security framework are explained below:

Cloud Computing: A Secure Framework



Security Policies

- Providers should come up with a formal plan to ensure security
- Employees should be given training on related technologies
- Background check of employees.
- Access restrictions / privilege setting to staff
- Obligatory password change within stipulated time.
- Supplier provided password of Server / hardware should not be used.

Data Backup, Recovery, Sanitization, Patch Updates And Logs

- Data backup should be carried out in regular intervals.
- Alternate plans should be ready to meet unexpected disasters.
- Providers should be equipped with data recovery plans in all emergencies.
- Deleting data from servers, backup devices when the service is removed or server is removed from the cloud.
- Patch updates and system files updates have to be conducted accurately.
- System logs must be maintained with the following details users accessed the data, when, how much time was spend , and modifications made.

Penetration Test

- To ensure providers system is not affected by any vulnerabilities, testing has to be done in regular intervals.

Firewalls And Network Security

- Firewalls must be installed and its policies , configurations , rules must be revised in habitual basis
- Antivirus updates must be done with out fail.

Secure Physical Infrastructure

- Physical Location of server is vital; cloud providers should keep the storage devices in secured places with proper physical protection.

XI. Conclusion

Cloud computing provides scalable and efficient means to manage IT resources in organizations. The flexibility the cloud brings in has some disadvantages over privacy and security. If the providers and consumers follow the security measures discussed above cloud computing will be more secure. As and when the issues around security and privacy are elucidated cloud computing will be accepted widely.