International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

CLOUD SECURITY ARCHITECTURE

Ms Sana Sanadi[1], Ms Siddhi Mitake[2] , Ms Dipali Patil[3], Ms Shrushti Bagal[4] , Ms. Kalpana Narayan Rode[5]

[1,2,3,4]Student, Electronics & Telecommunication Department, Sharad Institute Of Technology College Of Engineering Yadrav, Maharashtra, India.
[5]Assistant professor, Electronics & Telecommunication Department, Sharad Institute Of Technology College Of Engineering Yadrav, Maharashtra, India.
Gmail ID: sanasanadi124@gmail.com, siddhimitake456@gmail.com, dipalipatil1292@gmail.com, shrushtibagal2017@gmail.com

ABSTRACT

Cloud computing is ready of resources and services offered through the web. Cloud services are delivered from data centers located throughout the globe. Cloud computing facilitates its consumers by providing virtual resources via net. The foremost important challenge in cloud computing is that the protection and privacy problems caused by its multi-tenancy nature and also the outsourcing of infrastructure, sensitive data and important applications. Enterprises are rapidly adopting cloud services for his or her businesses, measures have to be developed so as that organizations are often assured of security in their businesses and can choose an suitable vendor for his or her computing needs.

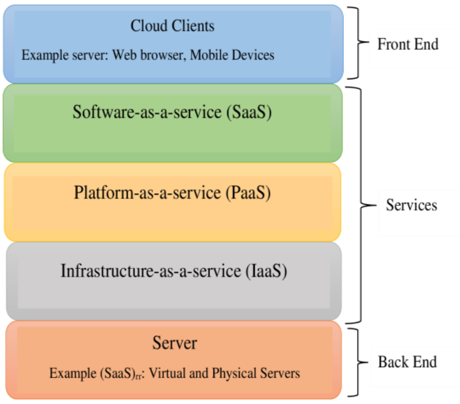
Cloud computing depends on the net as a medium for users to access the specified services at any time on pay-per-use pattern. However this technology remains in its initial stages of development, because it suffers from threats and vulnerabilities that prevent the users from trusting it. Various malicious activities from illegal users have threatened this technology like data misuse, inflexible access control and limited monitoring. The occurrence of those threats may result into damaging or illegal access of critical and confidential data of users. during this paper we identify the foremost vulnerable security threats/attacks in cloud computing, which could enable both end users and vendors to grasp about the key security threats related to cloud computing and propose relevant solution directives to strengthen security within the Cloud environment. We also propose secure cloud architecture for organizations to strengthen the protection.

***Keywords**: Cloud Computing; Security and Privacy; Threats, Vulnerabilities, Secure Cloud Architecture.*

1. INTRODUCTION

With Cloud Computing becoming a well-liked term on the Information Technology (IT) market, security and accountability has become important issues to spotlight. There are varity of security issues/concerns related to cloud computing but these issues fall under two broad categories: Security issues faced by cloud providers (organizations providing Software-, Platform-, or Infrastructure-as-a-Service via the cloud) and security issues faced by their customers. In most cases, the provider must confirmsure that their infrastructure is secure which their clients' data and applications are protected while the customer must confirm that the provider has taken the correct security measures to shield their information.Cloud investing much in new infrastructure, training of personals or licensing new software Advanced Computing. Computing has emerged because the easiest way for IT businesses to increase capabilities on the fly without.NIST defines Cloud computing as a "model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and delivered with minimal managerial effort or service provider interaction". It follows a simple "pay as you go" model, which allows an organization to pay for only the service they use.

It eliminates the need to maintain an in-house data center by migrating enterprise data to a remote location at the Cloud provider's site. Minimal investment, cost reduction, and rapid deployment are the main factors that drive industries to utilize Cloud services and allow them to focus on core business concerns and priorities rather than dealing with technical issues.


Cloud Clients
Example server: Web browser, Mobile Devices
Front End
Software-as-a-service (SaaS)
Platform-as-a-service (PaaS)
Services
Infrastructure-as-a-service (IaaS)
Server
Example (SaaS)$_{rr}$: Virtual and Physical Servers
Back End

According to, 91 % of the organizations in US and Europe agreed that reduction in cost is a major reason for them to migrate to Cloud environment. As shown in Figure. 1, Cloud services are offered in terms of Infrastructure-as-a- service (IaaS), Platform-as-a-service (PaaS), and Software-as-a-service (SaaS). It follows a bottom-up approach wherein at the infrastructure level; machine power is de- livered in terms of CPU consumption to memory allocation. On top of it, lies the layer that delivers an environment in terms of framework for application development, termed as PaaS. At the top level resides the application layer, delivering software outsourced through the Internet, eliminating the need for in-house maintenance of sophisticated software . At the application layer, the end users can utilize software running at a remote site by Application Service Providers (ASPs). Here, customers need not buy and install costly software. They can pay for the usage and their concerns for maintenance are remove.

2. PRINCIPLES OF CLOUD SECURITY ARCHITECTURE

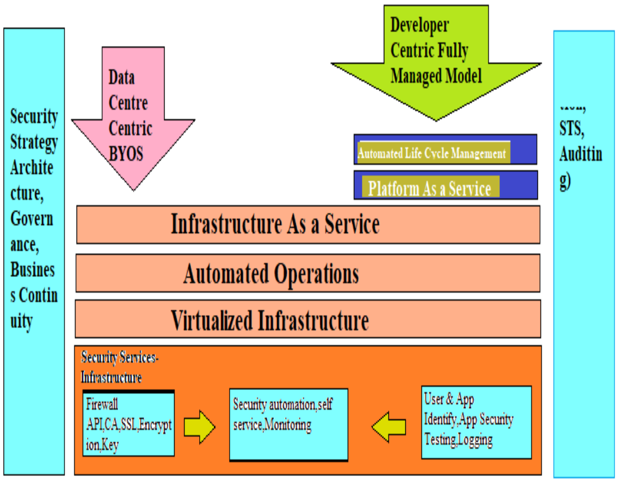
Well-designed cloud security architecture should be based on the following key principles:

- **Identification**—Knowledge of the users, assets, business environment, policies, vulnerabilities and threats, and risk management strategies (business and supply chain) that exist within your cloud environment.
- **Security Controls**—Defines parameters and policies implemented across users, data, and infrastructure to help manage the overall security posture.
- **Security by Design**—Defines the control responsibilities, security configurations, and security baseline automations. Usually standardized and repeatable for deployment across common use cases, with security standards, and in audit requirements.
- **Compliance**—Integrates industry standards and regulatory components into the architecture and ensures standards and regulatory responsibilities are met.
- **Perimeter Security**—Protects and secures traffic in and out of organization's cloud-based resources, including connection points between corporate network and public internet.
- **Segmentation**—Partitions the architecture into isolated component sections to prevent lateral movement in the case of a breach. Often includes principles of 'least privilege'.
- **User Identity and Access Management**—Ensures understanding, visibility, and control into all users (people, devices, and systems) that access corporate assets. Enables enforcement of access, permissions, and protocols.
- **Data encryption**—Ensures data at rest and traveling between internal and external cloud connection points is encrypted to minimize breach impact.
- **Automation**—Facilitates rapid security and configuration provisioning and updates as well as quick threat detection.
- **Logging and Monitoring**—Captures activities and constant observation (often automated) of all activity on connected systems and cloud-based services to ensure compliance, visibility into operations, and awareness of threats.
- **Visibility**—Incorporates tools and processes to maintain visibility across an organization's multiple cloud deployments.
- **Flexible Design**—Ensuring architecture design is sufficiently agile to develop and incorporate new components and solutions without sacrificing inherent security.

Cloud Security Architecture – Plan

As a first step, architects need to understand what security capabilities are offered by cloud platforms (PaaS, IaaS). The figure below illustrates the architecture for building security into cloud services.

3. HIGH LEVEL CLOUD ARCHITECTURE – SECURITY SERVICES


Security Strategy Architecture, Governance, Business Continuity
Data Centre Centric BYOS
Developer Centric Fully Managed Model
STS, Auditing)
Automated Life Cycle Management
Platform As a Service
Infrastructure As a Service
Automated Operations
Virtualized Infrastructure
Security Services-Infrastructure
Firewall API,CA,SSL,Encryption,Key
Security automation,self service,Monitoring
User & App Identify,App Security Testing,Logging

Security offerings and capabilities continue to evolve and vary between cloud providers. Hence you will often discover that security mechanisms such as key management and data encryption will not be available. For example: the need for a AES 128 bit encryption service for encrypting security artifacts and keys escrowed to a key management service. For such critical services, one will continue to rely on internal security services. A "Hybrid cloud" deployment architecture pattern may be the only viable option for such applications that dependent on internal services. Another common use case is Single Sign-On (SSO). SSO implemented within an enterprise may not be extensible to the cloud application unless it is a federation architecture using SAML 1.1 or 2.0 supported by the cloud service provider.The following are cloud security best practices to mitigate risks to cloud services:

- **Architect for security-as-a-service** – Application deployments in the cloud involve orchestration of multiple services including automation of DNS, load balancer, network QoS, etc. Security automation falls in the same category which includes automation of firewall policies between cloud security zones, provisioning of certificates (for SSL), virtual machine system configuration, privileged accounts and log configuration. Application deployment processes that depend on security processes such as firewall policy creation, certificate provisioning, key distribution and application pen testing should be migrated to a self-service model. This approach will eliminate human touch points and will enable a security as a service scenario. Ultimately this will mitigate threats due to human errors, improve operational efficiency and embed security controls into the cloud applications.

- **Implement sound identity, access management architecture and practice** – Scalable cloud bursting and elastic architecture will rely less on network based access controls and warrant strong user access management architecture. Cloud access control architecture should address all aspects of user and access management lifecycles for both end users and privileged users – user provisioning &deprovisioning, authentication, federation, authorization and auditing. A sound architecture will enable reusability of identity and access services for all use cases in public, private and hybrid cloud models. It is good practice to employ secure token services along with proper user and entitlement provisioning with audit trails. Federation architecture is the first step to extending enterprise SSO to cloud services. Refer to cloud security alliance, Domain 12 for detailed guidance here.

- **Leverage APIs to automate safeguards** – Any new security services should be deployed with an API (REST/SOAP) to enable automation. APIs can help automate firewall policies, configuration hardening, and access control at the time of application deployment. This can be implemented using open source tools such as puppet in conjunction with the API supplied by cloud service provider.

- **Always encrypt or mask sensitive data** – Today's private cloud applications are candidates for tomorrow's public cloud deployment. Hence architect applications to encrypt all sensitive data irrespective of the future operational model.

- **Do not rely on an IP address for authentication services** – IP addresses in clouds are ephemeral in nature so you cannot solely rely on them for enforcing network access control. Employ certificates (self-signed or from a trusted CA) to enable SSL between services deployed on cloud

- **Log, Log, Log** – Applications should centrally log all security events that will help create an end-to-end transaction view with non-repudiation characteristics. In the event of a security incident, logs and audit trails are the only reliable data leveraged by forensic engineers to investigate and understand how an application was exploited. Clouds are elastic and logs are ephemeral hence it is critical to periodically migrate log files to a different cloud or to the enterprise data center.

- **Continuously monitor cloud services** – Monitoring is an important function given that prevention controls may not meet all the enterprise standards. Security monitoring should leverage logs produced by cloud services, APIs and hosted cloud applications to perform security event correlation. Cloud audit (cloudaudit.org) from CSA can be leveraged towards this mission.

Cloud Computing Security Framework:

Cloud computing are currently having many security problems, and also become block to the development and popularization of cloud computing, so there need to build a cloud computing security framework, and actively carry out its cloud security key technology research. Here we proposes a cloud computing security framework.

Firewall :

Firewall. The method is to limit the form of open port. Among them, the Web server group opens port 80 (HTTP port) and 443 (HTTPS port) to the world, application server group only open port 8000 (special application service ports) for the Web server group, database server group only open port

3306 (MySQL port) for application server group. At the same time, the three groups of network server open port 22 (SSH port) for customers, and default refuse other network connection. By this mechanism, the security will be greatly improved

Cloud Security Architecture Threats:

Cloud services are affected by the most common types of concerns and threats, including data breaches, malware injections, regulatory non-compliance, insider threats, advanced persistent threats (APTs), credential stuffing attacks, insecure application programming interfaces (APIs), zero-day attacks, account hijacking through stolen or compromised credentials, phishing, and service disruptions due to denial-of-service attacks or misconfigurations. If a breach occurs, liability for the breach is based on the shared responsibility model.

Some threats and issues may also be more specific to the type of cloud service:

IaaS Cloud Security Threats

- Availability disruption through denial-of-service attacks
- Injection flaws
- Broken authentication
- Sensitive data exposure
- XML external entities
- Broken access control
- Security misconfigurations
- Cross-site scripting (XSS)
- Insecure deserialization
- Using components with known vulnerabilities
- Insufficient logging and monitoring
- Data leakage (through inadequate ACL)
- Privilege escalation through misconfiguration
- DoS attack via API
- Weak privileged key protection
- Virtual machine (VM) weaknesses
- Insider data theft

PaaS Cloud Security Threats

- Privilege escalation via API
- Authorization weaknesses in platform services
- Run-time engine vulnerabilities
- Availability disruption through denial-of-service attacks
- Injection flaws
- Broken authentication
- Sensitive data exposure
- XML external entities
- Broken access control
- Security misconfigurations
- Cross-site scripting (XSS)
- Insecure deserialization
- Using components with known vulnerabilities
- Insufficient logging and monitoring
- Data leakage (through inadequate ACL)
- Privilege escalation through misconfiguration
- DoS attack via API
- Privilege escalation via API
- Weak privileged key protection

- Virtual machine (VM) weaknesses
- Insider data theft

SaaS Cloud Security Threats

- Weak or immature identity and access management
- Weak cloud security standards
- Zero-day vulnerabilities
- Shadow IT/unsanctioned cloud applications/software
- Service disruption through denial-of-service attacks
- Phishing
- Credential stuffing attacks
- Weak compliance and auditing oversight
- Stolen or compromised credentials
- Weak vulnerability monitoring

4. CONCLUSION

In recent years, cloud computing is a technology of rapid development, however, the security problems have become obstacles to make the cloud computing more popular which must be solved. This paper analyzed the present situation of the development of cloud computing, and the security problems, and proposed a cloud computing security reference model.

The model put forward a series of solutions for the present Security problems cloud computing meet, but technology realization needs more

organizations and individuals to join into the cloud computing security research.

At the same time, cloud computing security is not just a technical problem, it also involves standardization, supervising mode, laws and regulations, and many other aspects, cloud computing is accompanied by development opportunities and challenges, along with the security problem be solved step by step, cloud computing will grow, the application will also become more and more widely.

REFERENCES

[1] Dikaiakos, M.D., Katsaros, D., Mehra, P., et al.: Cloud Computing: Distributed Internet Computing for IT and Scientific Research 13, 10–13 (2009)

[2] Amazon Web Services. Amazon Virtual private Cloud, http://aws.amazon.com/vpc/

[3] Catteddu, D.: Cloud Computing: Benefits, Risks and Recommendations for Information Security. CCIS, vol. 72, pp. 50–56 (2010)

[4] Amazon Web Services. Overview of Security Processes, http://aws.amazon.com/ec2/

[5] Bikram, B.: Safe on the Cloud. A Perspective into the Security Concerns of Cloud Computing 4, 34–35 (2009)

[6] Boss, G., Malladi, P., Quan, D., et al.: IBM Cloud Computing White Book, http://www-01.ibm.com/software/cn/Tivoli/ao/reg.html

[7] Jamil, D., Zaki, H.: Cloud Computing Security. International Journal of Engineering Science and Technology 3(4), 3478–3483 (2011)

[8] Zhang, S., Zhang, S., Chen, X.: Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks, ICFN 2010, p. 93 (2010) 9.Shen, Z., Tong, Q.: The security of cloud computing system enabled by trusted computing technology. In: 2nd International Conference on Signal Processing Systems (ICSPS 2010), vol. 2, pp. 2–11 (2010)

[9] Somani, U., Lakhani, K., Mundra, M.: Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In: 1st International Conference on Parallel Distributed and Grid Computing