Cloud security – challenges and best practices

Safwan Riyazudeen Paul Sirajudeen

East Carolina University

Paulsirajudeens18@ecu.edu

Abstract

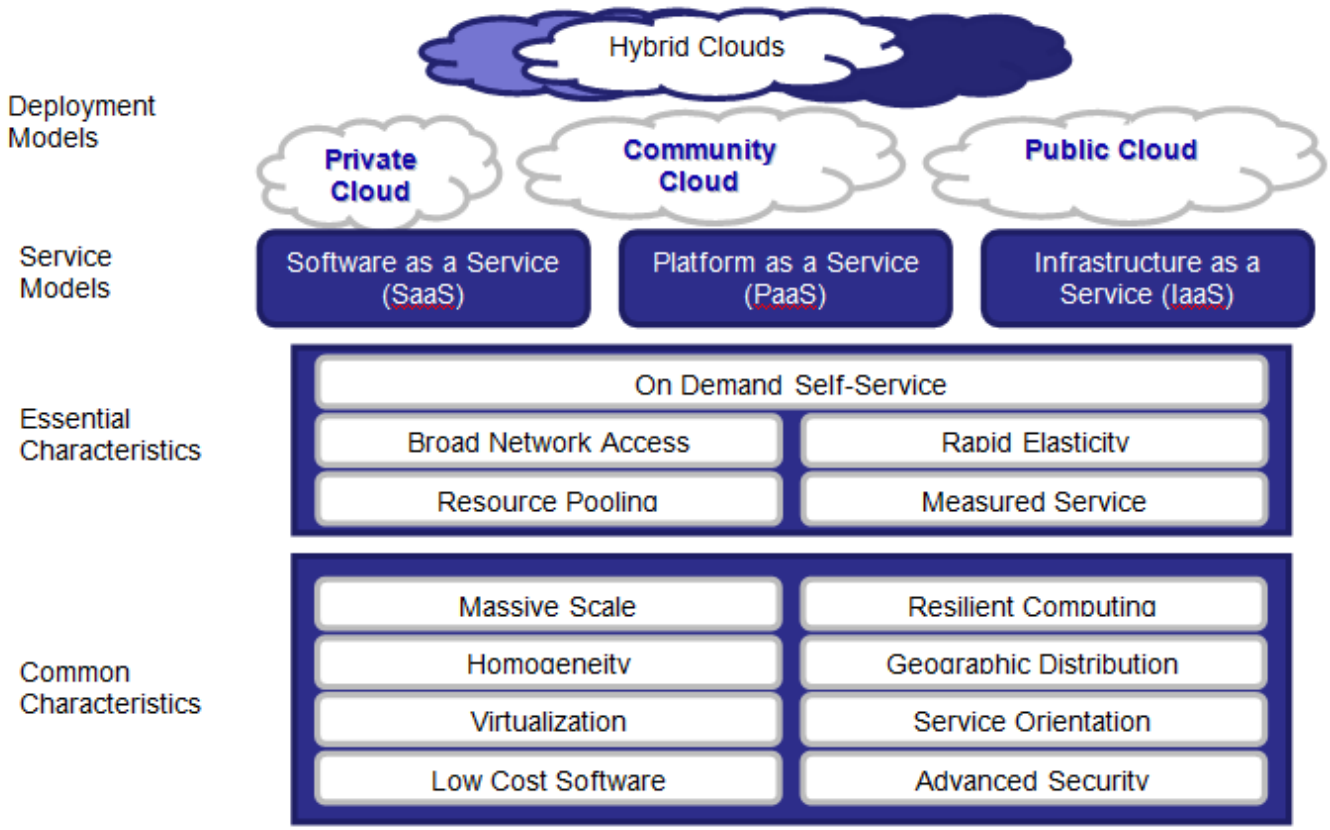
The quest to access data effectively and efficiently has brought forth the birth of cloud computing technology. The cloud computing industry is experiencing hyper-growth recently in the technology community. It is difficult to imagine an enterprise without the usage of cloud services due to its low cost of ownership and maintenance. Cloud computing makes state-of-the-art facility available remotely to anyone with an internet connection, resulting in reduced costs associated with maintaining a plethora of physical hardware and IT workforces, thus greatly helping small and medium sized businesses. However, the numerous benefits provided by cloud infrastructure also comes along with its vulnerabilities and security concerns. With the recent increase in high-profile security breaches, cloud security and privacy have become a rising public policy concern. This article provides an overview on some of the challenges faced by technology community using cloud services and some of the best practices that can be adapted to address them.

Keywords: Cloud computing, cloud security, service models, cloud threats, security challenges, best practices

Introduction

There is an increasingly prominent trend in many organizations to move a substantial portion or even all of IT operations to cloud computing. NIST defines cloud computing, in NIST SP 800-145 (The NIST Definition of Cloud Computing, September 2011) as' "a model for enabling ubiquitous, 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." Cloud service providers (CSPs) create an end user virtual application that provides the clients with software resources along with the essential hardware components required to keep all the data secured. As per the NIST definition, cloud computing is the threefold service model consisting of essential characters, service models, deployment models as shown in fig. The essential characteristics are On demand self-service, broad network access, resource pooling, rapid elasticity, measured service, and multitenancy. Clients are given range of options of service models when purchasing cloud services: software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), security as a service (SecaaS) and XaaS ('X' – anything as a Service). XaaS is used as a collective term to refer to vast number of technologies CSPs now deliver to clients as a service over a network. It includes Storage as a Service (SaaS), Database as a Service (DBaaS), Malware as a Service (MaaS), Communication as a Service (CaaS), Network as a Service (NaaS) etc., In all cloud servers, there are four different deployment models of cloud systems; the public cloud, private cloud, the hybrid cloud and the community cloud. Due to easy access to abundance of software applications and zero expense of buying costly storage equipment, many individuals and firms started hosting their data in the cloud. With rise in use of cloud computing, there have also been raises in the number of security

issues, particularly in the area of database security. Though cloud computing is appealing to many companies due to its tremendous benefits, looming security concerns remains a major hurdle for many other companies when comes to augmenting or replacing their on-premises systems with cloud services. Still many cloud service consumers (CSC) remain reluctant to embrace cloud services fully due to the fact that there will be loss of substantial amount of control over resources, services and applications. In cloud paradigm, data and applications are always under the control of the third party, which raises many security concerns. This paper describes the different kind of service models and deployment models used in cloud computing and also talks about challenges that are encountered when using cloud services and best practices that can be implemented to tackle them.



Cloud Service Models

The most common service models encompasses of SaaS, PaaS, IaaS, SECaaS

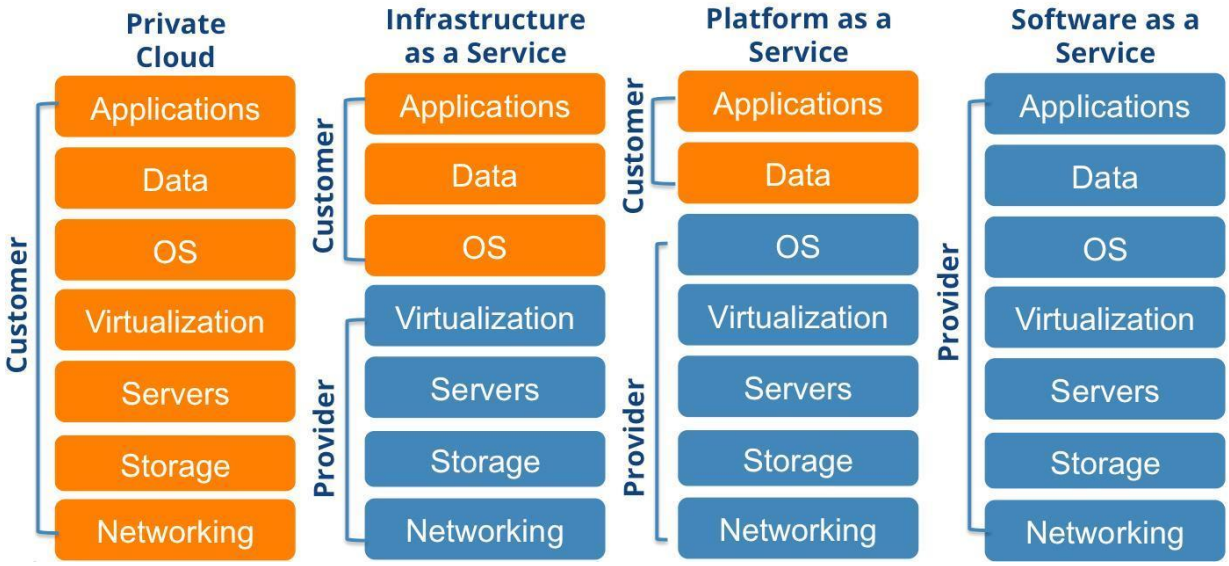
- Software as a Service (SaaS): SaaS provides consumers with software applications. It enables the consumer to use the CSPs applications running on the provider's cloud infrastructure. It can be accessed through a simple interface such as Web browser. The use of SaaS avoids the cost of software installation, maintenance, upgrades and patches.

- Platform as a Service (PaaS): PaaS provides consumers with platform on which the customer's application can run. It allows the customer to deploy their application onto the cloud infrastructure. Essentially, PaaS is an operating system in the cloud.

- Infrastructure as a service (IaaS): IaaS provides consumers with resources to run virtual machines (VMs). Users have control over operating systems, deployed applications and can select networking components. IaaS offers users with processing, storage and other fundamental computing resources. In this, users almost have full control without the need to purchase any hardware components or software applications.

- Security as a service (SECaaS): SECaaS is a new service fulfilled in the cloud computing environment to protect the IaaS, PaaS, and SaaS, along with all data and resources that are used within the clouds. To provide a secure environment, cloud computing providers are implementing several measures of SECaaS that form security measures in cloud computing. SECaaS protects SaaS, PaaS, and IaaS levels, where at the SaaS level, security services protect user data, as well as provider software. The SECaaS services at the PaaS level protect user applications, as well as the provider platform, whereas at the

IaaS level, SECaaS protects user virtual machines and provider infrastructure.



Cloud Deployment Models

Deployment models in cloud computing shows how users have access to the cloud storage. There are four most prominent deployment models for cloud computing.

- Public Cloud: A public cloud infrastructure is open to general public. The cloud provider is responsible for the cloud infrastructure and for the control of data and operations within the cloud. It is the least secure deployment model and may not offer guarantees against data loss or corruption. The major advantage of the public cloud are cost and scale to meet needs.

- Private Cloud: A private cloud infrastructure is implemented within an organization, no outside users can access the data. It provides tighter security environment for users and less risk of data loss. Private clouds deliver IaaS internally through an intranet or

the Internet via a virtual private network (VPN). Other advantages includes easy resource sharing within the organization and flexibility to meet client demands. Also, cloud servers and storage devices may exist on site, off site or both.

- Community cloud: It is a cloud system in which services are shared by multiple organizations that have common interests and similar requirements. It has restricted access. Community cloud infrastructure is deployed in health care industry.

- Hybrid cloud: It is a system of connected cloud systems consisting of at least one public cloud and one private cloud. They remain unique entities but are bound together by proprietary technology that enables data and application portability. This system provides secure way to transfer data between each cloud system. Advantage of hybrid cloud is sensitive information can be placed in a private area of the cloud and less sensitive data can make use of the benefits of public cloud.

Security implications

Cloud computing is a promising invention, but the security issues preventing it from being the next generation technology. The data in the cloud is much more vulnerable to risks rather than in traditional on premise computing.

- Confidentiality issues: It includes two concepts – data confidentiality and privacy. Confidentiality is defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information". Some of the confidentiality issues faced by cloud subscribers are data leakage due to multi tenancy, application privacy, data proliferation, Transborder data

flow, unauthorized data usage. The storage of data in some remote place and multi-tenancy feature of Cloud services gives rise to data leakage. Multi-tenancy implies administration of action resources, storage, services, and applications with another tenant. Multi-tenancy allows users to share common processing resources which results in various privacy and confidentiality threats to cloud system hosts and users. Co-tenancy, co-location and co-residence attacks are some of the issues that comes up with the exploitation of multi-tenancy since customer valuable data may be located at the same physical location. Due to that, attacker can access neighbor VMs or running applications. Another issue is there is no standardization of SLA between involved parties, despite the paramount necessity of it to portray the availability and privacy of user data. According to Modi et al., many cloud providers like Google, Amazon and SalesForce hide many parameters of the fully proposed SLA from the users.

- Integrity issues: It includes two concepts – data integrity and system integrity; Integrity means guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. Integrity is an issue in cloud security, wherein any malicious user can change or delete the data.

- Availability issues: It stands for "ensuring timely and reliable access to and use of information", which means presence of network, providing adequate communication bandwidth and redundancy.

- Architectural issues: The CSPs architecture is best known for its virtualization, which allows multiple users to access the services of cloud simultaneously. Virtualization is run by software known as Virtual machine monitor (VMM) or Hypervisor. The

VMM allows installation of multiple Virtual machines (VM's) or guest operating systems on the similar underlying architecture. Hypervisor enables virtualization through resource pooling and multi-tenancy. But this feature raises to many security implications in the cloud paradigm such as VM cloning, VM isolation, VM escape, VM migration, VM rollback, VM sprawl, VM hyperjumps, VM poaching. Hyperjacking occurs when a malicious intruder gaining control over the hypervisor through a malicious VM with attempt to take over the control of the virtualization layer. This results in single-point-of-failure.

VM cloning - Creation of a copy of an existing VM with the same identifier (ID), computer name, Internet Protocol (IP) address and Media Access Control (MAC) address is called VM cloning. Security issues come due to duplication of IP address.

VM isolation: Isolation of VM ensures safety and security even if another VM on the same host gets compromised but it may result in consequences when hypervisor gets compromised. This may end up degrading the entire system.

VM migration: This is the process of migrating VMs from one server to another for improving the utilization of resources effectiveness. This process can be automated to achieve load balance and save energy. This dynamic nature of the migration leads to security risks, not only to the migrated VM, but also for the new VM host.

VM Escape: Any attempt of the VM for direct interaction with the hypervisor, when VMs is running in an isolated environment, results in the escape of the VM. It may result in compromise of the entire virtual setup.

VM rollback: Casting back of VMs to its previous state can result in exposing of VM's to more security vulnerabilities. The revocation may be of the infected VM's to the former state with harmful virus/worms. VM rollback, if not handled in a secure manner, leads to activation of even more harmful virus/worms.

VM sprawl: It is defined as a situation where there is uncontrolled deployment of VMs, while a majority of them remain inactive. There results in of wastage of plenty of the host's resources.

VM Hopping/VM Hyper jumps: VM hopping is gaining access to another VM. This is possible through the vulnerability of the hypervisor, resulting in remote attacks and malware to compromise and attain control over the middleware packages. The hypervisor vulnerability leads to a single-point-of failure.

VM poaching: The vulnerabilities present in the OS/apps utilize the system resources, making other VMs on the same host to starve/fail.

- Cloud service model related issues:
    - IaaS issues: VM safety is the main issue in IaaS. Due to lack of bandwidth, hypervisor is exposed to DoS attacks and cross-VM side-channel attacks. Further, VM escape, rollback, migration, isolation vulnerabilities can result in attacker getting full control of the hypervisor. These vulnerabilities have been shown to compromise the confidentiality and integrity of tenant's data because of its dynamicity across VMs. Network Virtualization is another security challenge in IaaS since most VM monitors use virtualization to

interconnect directly and efficiently between VMs. Network virtualization is prone attacks as sniffing and spoofing virtual network. Network is exposed to several attacks due to the complexity of cloud computing architecture. Some of the attacks faced at network level security are Domain Name Server Attacks, Prefix Hijacking in Border Gateway Protocol, Issue of Reused IP Addressing, Sniffer Attacks, and DoS, DDoS attack, flooding and browser attacks, internet protocol vulnerabilities. Authentication, intrusion backdoor attack and session hijacking are the major security threats provoking the scalability of network.

- PaaS issues: Interoperability is the main issues in PaaS. It is the ability for different cloud to interact with each other at three different levels (SaaS, PaaS and IaaS), results in working with more than one cloud provider simultaneously, regardless of the differences between the providers. But applications written to use specific services from a vendor's PaaS will require changes to use similar services from another vendor's PaaS. As a result, PaaS becomes vulnerable to DOS assaults, Man-in-the-center assaults, XML-related attacks, Replay attacks, lexicon assaults, Injection attacks and input validation related attacks.

- SaaS issues:

  Data security: Since data resides in the database, weak access control system can give way to unauthorized access, resulting in loss of data confidentiality.

Application security: Since SaaS applications are managed over the web, security challenges like SQL injection attacks, DoS attacks, DDoS attacks, Cookie Poisoning, Hidden Field Manipulation, Dictionary Attack, Google Hacking, and CAPTCHA Breaking etc. must be addressed to avoid providing opportunities for attackers to gain control over the applications.

Best Practices when implementing Cloud services

The emergence of Cloud based IT landscape brings along with it many uncertainties and vulnerabilities which many organizations are concerned about. Cloud services is irresistible not to adapt to but at the same time remains risky. Hence, organizations will need to implement some best practices if they plan to migrate to Cloud services to combat the threats and ensure data security.

Choice of provider: Organizations must rigorously research about the choice of providers and ensure the terms and conditions of the CSP align well with their business scope. CSPs security standards and governance model should be reviewed. Businesses may visit CSP's data center to evaluate its physical security. Other critical factors that need to be analyzed include data sovereignty, location, data storage security and recovery protocol.

Data selection: It is equally important for the organization to decide what data will be shifted to Cloud and which ones will be retained in-house. Ideally, most sensitive customer data should be stored in the on premise cloud architecture. Hence, hybrid cloud model becomes the de facto choice for many businesses. Organization must make sure that there are specific security policies put in place in order to access on premise and off-premise cloud services.

Contract: Organization should make sure that the contract between them and the CSP is in detail and clear. All necessary information such as user rights, type of service, compensation in case of a breach, data backup, redundancy plan and security policies should be disclosed within the contract.

Access control: Data security is the top most priority for all the organizations. To ensure the integrity and confidentiality of data, companies must ensure that there is a strong access control system in place. Through access control process, attribute based encryption is deployed wherein access right of each user is determined by the attributes given to them. Some CSP also use RBAC (Role Based Access Control) for securing access.

Data Encryption: Encryption is crucial to prevent data leakage and data theft. Best practice for the companies is to encrypt the data before it leaves the premises. Encryption consists of two levels -the base phase and surface phase. In the base phase, the data is encrypted by the owner of the data. Following the base phase, a re-encryption program is implemented on the encrypted data by the cloud servers during the surface phase. This ensures two layers of encryption. Virtual hard disk files should also be encrypted to protect data at rest.

Cryptographic Separation of Data: To ensure confidentiality and integrity of data, organization must ensure that there is cryptographic separation of data using symmetric and asymmetric algorithm.

Auditing: Organizations can deploy an auditing process to assess their CSP in terms of the deployment of VM's, storage of confidential data, maintenance of physical hardware, monitoring and service repairing of architecture, interaction with other tenants etc.,

Virtual Private Cloud: Organization can also improve their visibility about where there data is going by using VPC. With VPC, business can add an extra layer of security to their data by installing virtual firewall in their cloud.

Robust authentication framework: Organization should make sure that their CSP adapting not only traditional authentication methods (password and tokens) but also advanced authentication method like biometric features to enhance security.

Vendor Lock-in: Organization must also consider the threat of not being able to migrate to competitive CSP and being locked in within a vendor due to incompatibility issues and switching costs. When signing the contract, companies should ensure that the CSP will assist the firm in deconversion process.

Operational security practices: Organization must ensure there is a regular process of updating certificates/licenses, patch management, VM updates etc., There should be proper security policies in place to prevent abuse of passwords by the employees. Also, businesses should use dedicated private connection when connecting to Cloud services instead of public internet. Using public network can cause issues in terms of speed, manageability and security. Some applications cannot tolerate latency; using public internet for accessing cloud applications is not a viable option in this case.

Education: Education is key. Organization must educate its employees about the dynamics of the cloud services before making the shift. Businesses must keep themselves aware of the security risks involved in the cloud services and mitigation strategy required to combat them.

Conclusion

Cloud computing is no doubt serving the technology community beyond expectations and growing number of businesses are employing cloud-first approach, but its exponential growth will be slowed by the security challenges if not addressed timely. While subscribing to the services provided by CSP, businesses must educate themselves about the security policies of the CSP. Identifying the security issues and implementing appropriate best practices will help business organizations to pave way for a smooth transition to cloud services and reap maximum benefit.

List of Abbreviations

CSP – Cloud Service Provider

CSC – Cloud Service Consumer

NIST – National Institute of Standards and Technology

IaaS – Infrastructure as a Service

SaaS – Software as a Service

PaaS – Platform as a Service

SECaaS – Security as a Service

VPN – Virtual Private Network

VPC – Virtual Private Computing

VM – Virtual Machine

VMM – Virtual Machine Monitor

RBAC – Role Based Access Control

References

Dave Nicholson, Cloud first – tackling the security challenges, Computer Fraud & Security, Volume 2018, Issue 1, 2018, Pages 8-11, ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(18)30005-8.

El Balmany Chawki, Asimi Ahmed, Tbatou Zakariae, IaaS Cloud Model Security Issues on Behalf Cloud Provider and User Security Behaviors, Procedia Computer Science, Volume 134, 2018, Pages 328-333, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2018.07.180.

Kumar, A., Malage, G., Kumar, H., & Gopal, K. S. (2018). CLOUD COMPUTING FEATURE SCURITY AND EXPECTED SOLUTION- SURVEY PAPER. International Journal of Advanced Research in Computer Science, 9, 267-272. doi:http://dx.doi.org.jproxy.lib.ecu.edu/10.26483/ijarcs.v9i0.6247

M, A. J. (2018). Cloud computing: Major challenges and counter acts. *International Journal of Advanced Research in Computer Science, 9*(2), 618-625. doi:http://dx.doi.org.jproxy.lib.ecu.edu/10.26483/ijarcs.v9i2.5861

Modi, C., Patel, D., Borisaniya, B. et al. J Supercomput (2013) 63: 561. https://doi.org/10.1007/s11227-012-0831-5

Musa, K. (2018). *The intention to adopt cloud computing based on security-as-a-service measures using technology acceptance model (TAM)* (Order No. 10747659). Available from ProQuest Dissertations & Theses Global. (2021741426).

Nalini Subramanian, Andrews Jeyaraj, Recent security challenges in cloud computing, Computers & Electrical Engineering, Volume 71, 2018, Pages 28-42, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2018.06.006.(http://www.sciencedirect.com/science/article/pii/S0045790617320724)

Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," 2009, http://www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def-v15.pdf, Accessed April 2011.

Stallings, William. & Brown, Lawrie. (2018). Computer security : principles and practice. Hoboken, New Jersey, Pearson Education, Inc