A Survey on security of Cloud-based Data Center Infrastructures

Majid Asadpoor
University of Mazandaran, Babolsar, Iran

ABSTRACT
Cloud computing is an emerging technology paradigm that migrates current computing and technological concepts into utility-like solutions similar to electricity and water systems. Clouds bring out a wide range of advantages including configurable computing resources, economic savings, and service flexibility. Cloud service providers use data centers to house cloud services and cloud-based resources. For cloud-hosting purposes, vendors also often own multiple data centers in several geographic locations to safeguard data availability during outages and other data center failures. Security in Cloud computing is an important and critical aspect, and has numerous issues and problem related to it. Cloud computing is a framework for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. However, privacy and security concerns are shown to be the primary obstacles to a wide adoption of clouds. The new concepts that clouds introduce, such as multi-tenancy, resource outsourcing and sharing, create new challenges to the security community. Addressing these challenges requires, in addition to the ability to cultivate and tune the security measures developed for traditional computing systems, proposing new security policies, models, and protocols to address the unique cloud security challenges.

KEYWORDS:
Cloud computing, Cloud security, security vulnerabilities, Security Issues, Cloud Architecture, Data Protection and Cloud Platform.

1. Introduction

This paper seeks to explore and identify important challenges and security issues facing cloud computing, a now fairly mature technology, along with the methods employed in industry to combat these problems. In order to achieve this goal, we must first understand the concepts behind this technology, as well as its underlying infrastructure. There are now many services being offered by vendors which have the label "cloud" attached to them, using this now fashionable term to entice members of the general public who may not necessarily know any better. In this introduction, we aim to give a succinct description of what cloud computing entails, and in so doing shed light on the various characteristics defining this technology.

Cloud computing is a model for convenient and on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management efforts. Cloud Computing provides capabilities of Information Technology (e.g., applications, storages, communication, collaboration, infrastructure) via services offered by CSP (cloud service provider). Cloud Computing has various characteristics as shared infrastructure, self-service, pay-per use model, virtualized and dynamic, scalable and elastic. Cloud computing has the capacity of scaling and elasticity which is perfect for such an environment.

A cloud computing offer companies an increased storage than traditional storage systems. Software updates and batches are highly automated with reduced number of hired highly skilled IT personnel.

The architecture of the Cloud Computing involves multiple cloud components interacting with each other about the various data they are holding on too, thus helping the user to get to the required data on a faster rate. When it comes to cloud it is more focused upon the frontend and the back end. The front end is the User who requires the data, whereas the backend is the numerous data storage device, server which makes the Cloud.

To successfully address the cloud security issues, we need to understand the compound security challenges in a holistic way. Specifically, we need to: (i) investigate various cloud security attributes including vulnerabilities, threats, risks, and attack models; (ii) identify the security requirements including confidentiality, integrity, availability, transparency, etc.; (iii) identify the involved parties (clients, service provides, outsiders, insiders) and the role of each party in the attack-defense cycle; and (iv) understand the impact of security on various cloud deployment models (public, community, private, hybrid.

1.1 Cloud Computing:

NIST specifies that cloud computing exhibits the following five features in its operation:

A. On-demand self-service

A Cloud Service Customer (CSC) can use an online interface to allocate computing resources like additional computers or network bandwidth without human interaction with their Cloud Service Provider (CSP).

B. Broad network access

CSCs can access computing resources over networks such as the Internet from a variety of computing devices.

Manuscript received October 5, 2017
Manuscript revised October 20, 2017

C. Resource pooling

CSPs can use shared computing resources to provide cloud services to multiple customers. Virtualization and multi-tenancy systems are typically used to both segregate and protect each customer from other customers. They can also be used to make it appear to customers that they are the only user of a shared computer or software application.

D. Rapid elasticity

This refers to the quick and automatic balancing of the amount of available computer processing, storage and network bandwidth as required by customer demand.

E. Pay-per-use measured service

This involves customers only paying for the computing resources that they actually use, and being able to monitor their usage. The service purchased by customers can be quantified and measured

It is hence worth noting that a vendor adding the words "cloud" or "as a Service" to the names of their services and products does not automatically mean that the vendor is selling cloud computing as per the NIST definition. Customers sharing resources is at the heart of cloud computing, and as such looks to be a potential area of concern regarding security. Let us now look at the infrastructure that actual cloud computing services utilize in order to clarify this.

✓ High scalability

Cloud environments enable servicing of business requirements for larger audiences, through high scalability.

✓ Agility and Flexibility

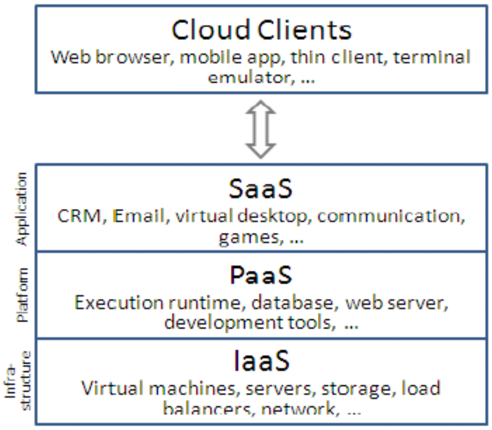
The cloud works in the 'distributed mode' environment. It shares resources among users and tasks, while improving efficiency and agility (responsiveness)

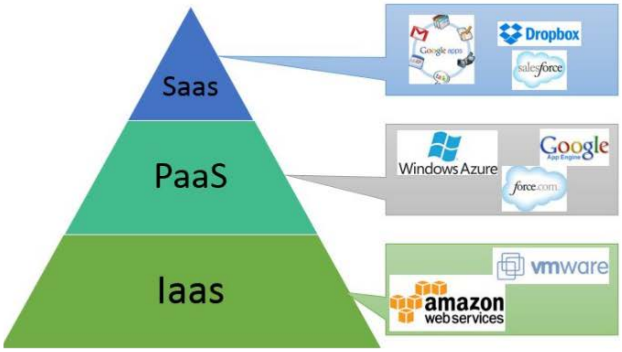
✓ High availability

Availability of servers is high and more reliable as the chances of infrastructure failure are minimal.

✓ Multi-Tenancy

With the cloud working in a distributed and shared mode, multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure.


Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...



2. Security issues in cloud-based services

Cloud computing service models are SAAS, PAAS and IAAS, which provides software as a service, platform as a services and infrastructure as a service to end users or customers. These three service models are built on top of each other, as shown in Fig. 1; as a result their capabilities are inherited as well as security issues and risks. So, service providers are not be able to take care only part of it, rather than as a whole to provide secure environment. In this part of this paper clearly indicate major security issues based on these service models and what needs to be addressed by implementing appropriate countermeasures.

There are a number of areas that are at risk of being compromised and hence must be secured when it comes to cloud computing. Each area represents a potential attack vector or source of failure. By risk analysis, five key such areas have been identified:

Physical Security Issues

The physical location of the cloud data center must be secured by the CSP in order to prevent unauthorized on-site access of CSC data. Even firewalls and encryption cannot protect against the physical theft of data.

Since the CSP is in charge of the physical infrastructure, they should implement and operate appropriate infrastructure controls including staff training, physical location security, network firewalls. It is also important to note that the CSP is not only responsible for storing and process data in specific jurisdictions but is also responsible for obeying the privacy regulations of those jurisdictions.

Technological Security Issues

These risks are the failures associated with the hardware, technologies and services provided by the CSP. In the public cloud, with its multi tenancy features, these include resource sharing isolation problems, and risks related to changing CSPs, i.e. portability. Regular maintenance and audit of infrastructure by CSP is recommended.

Compliance and Audit Issues

These are risks related to the law. That is, risks related to lack of jurisdiction information, changes in jurisdiction, illegal clauses in the contract and ongoing legal disputes.

For example, depending on location, some CSPs may be mandated by law to turn over sensitive information if demanded by government.

Data Security Issues

There are a variety of data security risks that we need to take into account. The three main properties that we need to ensure are data integrity, confidentiality and availability. We will go more into depth on this in the next subsection since this is the area most at risk of being compromised and hence where the bulk of cloud security efforts are focused.

Organizational Security Issues

Organizational risks are categorized are categorized as the risks that may impact the structure of the organization or the business as an entity. If a CSP goes out of business or gets acquired by another entity, this may negatively affect their CSPs since any Service Level Agreements (SLA) they had may have changed and they would then have to migrate to another CSP that more closely aligns with their needs. In addition to this, there could be the threat of malicious insiders in the organization who could do harm using the data provided by their CSCs.

These risk categories have been further split between CSPs and CSCs and are illustrated in the following table:

Risk Categories/Environment	Cloud Provide	Cloud Customer
Physical Security	-Data Location -Server, Storage & Network	-Data Location
Organizational	-Resource Planning -Organization Change Management -Malicious Insiders	N/A
Data Security	-Identity Access Management -Risk of Multi-tenancy -Availability & Backup -Data Privacy & Security	-Data Segregation -Access Management -Availability & Backup -Data Privacy, Security -Secure Data Deletion -Data Loss & Leakage -User Access
Technological	-Application Development -Portability -Lack of Interoperability Standards	-Application Development -Portability -Infrastructure Capability
Compliance & Audit	-Legal Challenges -Compliance & Audit -Business Continuity	-Legal Challenges -Compliance & Audit -Business Continuity

In table we can see the five main areas of concern for a cloud service provider when it comes to security. The bullet points next to each category further narrows down a subcategory that could cause security issues to a CSP.

2.1 Security Issues in SAAS:

In Software as a Service (SAAS) model, the client has to depend on the service provider for proper security measures. The provider must ensure that the multiple users don't get to see each other's data. So, it becomes important to the user to ensure that right security measures are in place and also difficult to get an assurance that the application will be available when needed. As a result, there are some securities issues arise such as: how is being data stored and where, what types of security is being provided for data manipulation and storage. There are some key security basics need to be considered during SAAS deployment and development. These are:

Ø Data Security:

Data control over cloud services make difficult to protect and enforce identity theft and cybercrime security. Sharing resources across multiple domains and failures of data backup also arise some data leakage.

Ø Network Security:

In cloud environment data are being transferred over the Internet, thus data flow security is an important issue to avoid leakage of information. To sniff network packets an intruder can make use of data packet to analyze weakness in network security configuration. Attackers can gain access applications and data through hacking such as: some kind of remote access mechanism and injection (SQL and some bad command) vulnerabilities. DoS (Denial of Service), DDoS (Distributed DoS), man in the middle attacks, social networking attacks and some unauthorized attacks creates grate security issues in cloud.

Ø Data Confidentiality:

Privacy and confidentiality issues are taking placed when data shares between various users, devices and applications.

2.2 Security Issues in PAAS:

Platform as a service encapsulates a layer of software and provides it as a service that can be used to build higher-level services. The PaaS model may be hosted on top of IaaS model or on top of the cloud infrastructures directly. Google Apps and Microsoft Windows Azure are the most known PaaS. The PaaS model is based on the Service oriented Architecture (SOA) model. This leads to inheriting all security issues that exist in the SOA domain such as DOS attacks, Man-in-the-middle attacks, XML-related attacks, Replay attacks, Dictionary attacks, Injection attacks and input validation related attacks.

2.3 Security Issues in IAAS:

Infrastructure as a service (IaaS): Cloud computing providers offer physical and virtual computers, extra storage networking devices etc. The virtual machines are run by hypervisors that is organized into pools and controlled by operational support systems. It is cloud users responsibilities to install operating system images on the virtual machines as well as their application software. Cloud computing combines virtualization technologies are creative way to provide better IT services to consumers. Due to rising virtualization technology poses some security issues for control over the owner of data regardless of physical location. Various security issues are arising to deploy models in IaaS. Private cloud environment creates fewer security risks compared to public cloud. The cloud concept implemented just over the Internet, so whatever security issues and threats are facing in the Internet, for cloud services need to consider as well. Infrastructure is not only appropriate for hardware resources, where data is being reside or processed, but also the way data are being transmitted over the media from source to destination over the open network. There are some possibilities that data can be routed through intruder's network or infrastructure. Infrastructure as a service delivers basic storage and compute capabilities as standardized services over the network. Servers, storage systems, switches, routers, and other systems are pooled and made available to handle workloads that range from application components to high-performance computing applications.

3. Solutions to cloud security issues

There is need for advanced and extended technologies, concepts and methods that provide secure server which leads to a secure cloud.

Network Security:

Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment. For a secure system to prevent unauthorized modification and access to data by using adequate set up or configuration of firewall and auditable access rights. To secure data traffic, some policies should be implemented in router and layer three switch.

Audit and compliance:

A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations.

Regulations written for IT security require that an organization using IT solutions provide certain audit functionality. However, with cloud computing, organizations use services provided by a third-party. Existing regulations do not take into account the audit responsibility of a third-party service provider.

Access Control:

To generate trusted user profiles based on their definitions and roles. Identity management and access security mechanism should be implemented and monitored according to their regular schedule. Service providers should prove that they have adequate security mechanism to protect unauthorized access. All access or changes in cloud services (resources and data) ought to provide auditable report whether it is success or fail and review along with monitoring to be performed regular basis.

Confidentiality and Integrity:

Proper authentication and authorization mechanism should implement to protect illegal disclose and modification of data. Network service providers must be able to monitor network load or traffic for proper load balancing and data distribution over network. Service development and deployment models must be clear for a developer to protect and restrict use of data.

Identity/credentials (management):

Within cloud computing, identity and credential management entails provisioning, de-provisioning, and management of identity objects and the ability to define an identity provider that accepts a user’s credentials (a user ID and password, a certificate, etc.) and returns a signed security token that identifies that user. Service providers that trust the identity provider can use that token to grant appropriate access to the user, even though the service provider has no knowledge of the user. An organization may use multiple cloud services from multiple cloud providers. Identity must be managed at all of these services, which may use different identity objects and identity management systems.

Data Security:

The service providers should have enough skills to prevent, detect and react according to various security breaches. Service logs and service agreement terms inspections are performed regularly. However, there are some validity tests also required for companies to avoid security breach because of malicious data are in cloud such as: cross-sire scripting, insecure configuration, SQL injection flaws and weakness in access control inside companies policies. Data in cloud environment should be identified and classified according to their types. Service providers should provide transparent services (controls, security and operations) for clients.

Security parameters

Are appropriately defined for data segregation and secure cryptographic methods and properties should be implemented in control manner such as: for secure key transfer can be used RAS and for encryption key size should be consider according to their priority of data security or uses. Data replication and backup policies are also need to be standard and provided auditable proof for data restore procedures, which includes accuracy and completeness over time.

References

[1] Wang, Lizhe; von Laszewski, Gregor; Kunze, Marcel; Tao, Jie. Cloud computing: A Perspective study, Proceedings of the Grid Computing Environments (GCE) workshop. Held at the Austin Civic Center: Austin, Texas: 16 November 2008.

[2] Michael glas and paul Andres, “An Oracle white paper in enterprise architecture achieving the cloud computing vision”, CA-U.S.A, Oct 2010.

[3] Dahbur, K., Mohammad, B., "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing.", Int Conference on Intelligent Semantic Web-Services and Applications, 2011, URL: http://www.jisajournal.com/content/4/1/5

[4] Seny Kamara, Kristin Lauter, “Cryptographic cloud storage”, Lecture Notes in Computer Science, Financial Cryptography and Data Security, pp. 136- 149, vol. 6054, 2010. DOI: 10.1007/978-3-642-14992 4_13

[5] “IT-3_Cloud_Computing” A news Letter for IT professionals Issue 3 2012.

[6] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of Network and computer Applications; 2011; 4(1):1–11.

[7] Problems Faced by Cloud Computing, Lord CrusAd3r, dl.packetstormsecurity.net/.../ ProblemsFacedbyCloudComputing.pdf.

[8] Choudhary V.(2007). Software as a service: implications for investment in software development. In International conference on system sciences, 2007, p. 209.

[9] Aderemi A. Atayero, Oluwaseyi Feyisetan , Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption, Journal of Emerging Trends in Computing and Information Sciences, Vol. 2, No. 10, October 2011

[10] Meiko Jensen, Jörg Schwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing,” in IEEE ICCC, Bangalore 2009, pp. 109-116.

[11] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, vol. 34, Issue 1, pp. 1-11, July 2010.

[12] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems, 2011.