International Academic Institute for Science and Technology

International Academic Journal of Innovative Research
Vol. 2, No. 1, 2015, pp.31-41.

ISSN 2454-390X

International Academic Journal of Innovative Research

www.iaiest.com

Analysis of challenges and solutions in cloud computing security

Mahdi AliPour Kondori[a], Mohammad Hassan Peashdad[b]

[a,b]*Department of computer, ferdows Branch, Islamic Azad University, ferdows, Iran*

Abstract

Remarkable potential of cloud computing resources to provide a powerful, affordable, flexible and easy to manage on the Internet. Cloud computing hardware resources through efficient use and collaborative capabilities greatly increases. These features encourage organizations and individual users and their applications and services to the cloud transfer. For example, even vital infrastructure and the index of production and distribution have also been transferred to the cloud computing paradigm. However, cloud services and third party service providers to provide services that are associated with security risks. User migration and transfer of assets (data, applications, etc.) are outside the control of administrators in a collaborative environment that multiple users are taken together, exacerbate security concerns. In this study, in detail, of the nature of cloud computing security issues described above. Meanwhile, new solutions have been proposed in the literature to deal with security issues. While security vulnerabilities in mobile cloud computing also briefly examine.

Keywords: Cloud computing, multi-ownership, security, virtualization, Web services

Introduction:

Cloud computing paradigms and broad global popularity since its emergence in the industry and the academic community has won. Economic access, scalable, appropriate, consistent, and on-demand to shared resources such as cloud characteristics that change business processes to the cloud transfer has been terminated. Cloud computing because of the potential to provide significant benefits for Industry and society is highly regarded by the scientific community.

Resources available to users, and query a set of shared resources are released. According to the request source offerings ensures optimal resource allocation and cost-effective while as well.you can use this resource. Another advantage is the ease of use of cloud computing in that it is necessary to have extraordinary skills in the field of technology-specific or customer-specific cloud is not. IT Service Management and is transmitted from the user end and the target servers. (2015, Ali et al) using various technologies such as cloud computing, Web services, virtualization and virtual resources Chndmalkyty provides to customers. Cloud services are the customer via the Internet. Web applications and managing cloud resources used to achieve an important component of web apps, cloud computing makes. Customer processes run in a virtual environment instead of physical resources they use.

Multiple virtual machines the same physical processes are allocated to different users that are separated logically. This increases the multi-ownership in the cloud. Despite the benefits of this environment, cloud computing is not exempt from risks and its risk security issue. Security is one of the biggest obstacles to widespread adoption of cloud computing in the brain. Processing, move and manage data, applications in the administrative domain, organizational performance are implemented. On the other hand, organizations and cloud infrastructure management controls and not enjoy pleasure. Management practices that cloud service providers (CSP) generally adopted for organizations are clear. There is a large percentage of users who had no connection with the organization's concerns will be exacerbated. But users should not trust cloud providers do not need to trust each other.electronic safe has done. In addition to taking on only the issue of privacy has been given. (2011, Che et al) cloud computing security models known as cube models, modeling and risk assessment model to examine Chndmalkyty. (2011, Che et al) In addition to taking on cloud computing also poses security risks. The risk posed by different Mnzrs·hamdaran such as customers, the government has payers Vdydgah maintenance operations and technology are not included.

Cloud Computing Architecture Framework:

Cloud computing technologies to serve diverse end-users. Understand the security issues associated with cloud computing involves defining concepts related to cloud computing. The definition of the National Institute of Standards and Technology (NIST) definition of cloud computing is accepted. (2014, Fernando et al) NIST defines cloud computing as a model of a triple provide services. The original specification, b. And (c) service models. Open models will be considered. (Figure 1) concepts NIST cloud computing definition in the shadows are as follows:

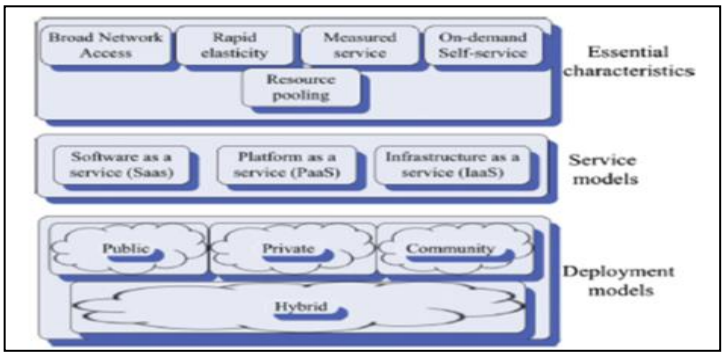


Figure 1: NIST definition of cloud computing

The original specification:

Reliable on-demand service:

Customers can without any human contact with CSP request and manage services from the cloud. Provide services and related resources in times of need is usually done via web services and management interfaces. (2014, Fernando et al).

Access WAN

Merging two collections

Cloud resources in a multi-ownership mergers and acquisitions are shared among multiple customers. Location resource for customers is obvious. Drawing and mapping between physical and virtual resources placed at the disposal of clients.

Several property

NIST defines cloud computing five attributes above. The Cloud Security Agency (CSA) has raised Chndmalkyty as an important feature of cloud computing. Several proprietary features that take advantage of multi-client enable single source that may belong to an organization or not. Chndmalkyty lead to more efficient use of resources and different customers that reasonably could be separated.

Service models

NIST cloud computing services is divided into three categories:
Software as a Service (SaaS), platform as a service (PaaS) and Infrastructure as a Service (IaaS).

Software as a Service (SaaS):

Take advantage of SaaS applications over the Internet, enabling PSP to run on cloud infrastructure. Thin client interface such as a web browser used to access the application. SaaS facility does not create an application or software. Only through internet software and thus offers a model for software distribution via the web. Consumer prices and their customers to use software and not the owner.

Platform as a Service (PaaS):

applications that are owned by the customer should have a framework for the implementation and management. Which contains integrated development environments (IDE), operating system and the platform layer resources. These services are provided as a PaaS. PaaS lets you control the underlying cloud infrastructure for customers, but customers can only control applications move to the cloud.

Infrastructure as a Service (IaaS)

IaaS referred to as CSP offers hardware infrastructure including network, storage, memory, CPU and other various computing resources. Resources provided in the form of virtual systems that are accessible via the Internet. CSP fundamental resource control.

Open models

Cloud computing infrastructure we have developed four models: private cloud, public cloud, public cloud and hybrid cloud.

Private Cloud

Cloud that just to run and manage an organization's private cloud is called. Perhaps the owner of the physical infrastructure or not, and be managed by the organization itself or a third party. In addition, private cloud may be located at the geographic organization or not. However, in any case, only for the use of an organization's private cloud and other customers are not allowed to use the resources.

Public cloud

CSP owner of the physical infrastructure cloud and all organizations and the public sector can use it. Resources are shared among all customers and clients who use the services and resources to the cloud owner pay. Physical infrastructure in places distant from the customers and is managed by the CSP.

Cloud collective (public)

The cloud is forming a community among a number of organizations or clients to be shared. In general, community interests such as Mission (Mission), security requirements, policy (policy) considerations reception. Cloud collective (social) may be used by each of the organizations in the community or be managed by a third party.

Hybrid Cloud

Hybrid cloud is a combination of two or more clouds (private, public or community) is. All the clouds have their status as a unique component technology, standardized or proprietary maintain but to share.

Security challenges

Characteristics and cloud computing models such services improved, optimized and low-cost to customers are located. As the above models that have the characteristics of different technologies such as virtualization and implementation are Chndmalkyty. Open cloud service technologies and models with

cloud-specific vulnerabilities and risks as well as risks and dangers have in common with traditional IT infrastructure. Source Integration possible to use an identical set by the user through virtualization technologies, and provides Chndmalkyty. Chndmalkyty risk visibility And the sequence data for other users and reject the operation ends. Due to the possibility of unauthorized access to web-based management user interface in which the user interface is more traditional systems, self-service feature provides on-demand.

The virtual environment also has its own set of risks and vulnerabilities that malicious collaboration between virtual machines (VM) VM and liberation and escape the Shvd.mdl of service from the perspective of cloud service models are too close together. SaaS applications built on PaaS and IaaS to PaaS radically expanded and dependent. The operational independence of each service models will also lead to a security association. For example, if an attacker manages to gain control of IaaS, the result of which would be jeopardized PaaS IaaS uses. PaaS to SaaS compromised compromised ends.

In addition, all models of compromised service access to allow for another layer of the service model. Private cloud model of the traditional IT infrastructure is identical set of vulnerabilities. That's because the Abrkhsvsy for the use of a single organization. Public clouds, and hybrid social presence for users of various origins and administrative control of a third party risks and vulnerabilities are more specific cloud. In this paper, based on the three issues of architecture, communication and legal issues and contractual issues to the challenges posed by the environment. (Figure 2)

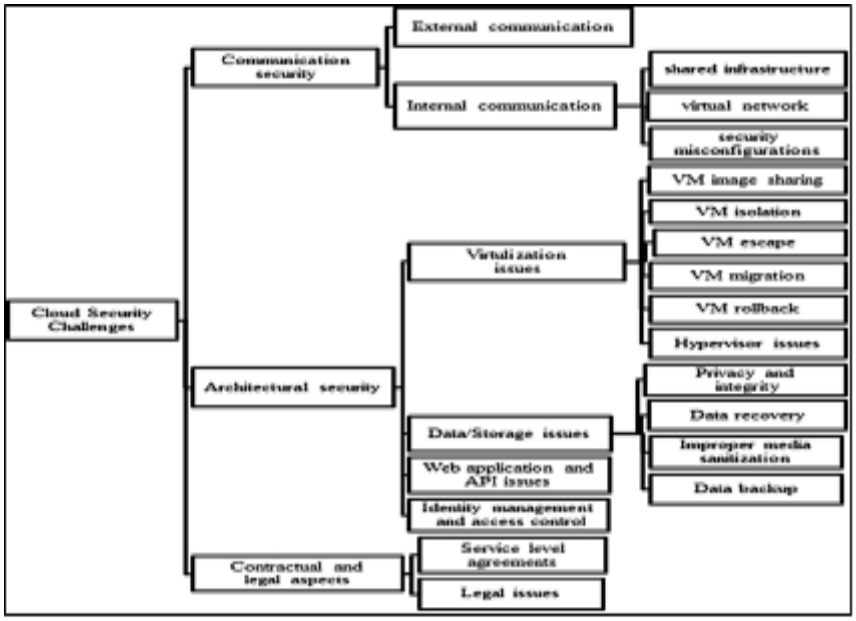


Figure 2: The Challenge of Security in the Cloud

Challenges in Architecture

Virtualization issues

Virtualization is considered a strategic component cloud. Which will allow more customers to use the same physical resources. (2014, Fernando et al) VM separately for each referred user that the virtual machine offers complete operating for the user. Multi-VM on a physical source traced the source to a multi-property integration. VM monitoring (VMM) or hypervisor (hypervisor) module that VM management and a variety of different operating systems at the same time allowed to run on the same physical system. However, virtualization security challenges to provide infrastructure and cloud users.

Issues / data virtualization

Cloud Computing model does not provide complete control over user data. In the traditional model of cloud computing, cloud computing has enabled providers to apply to manage servers and data control. The only certain user controls VM would benefit. The lack of control over data security risks than traditional computing model has brought. In addition to taking on the characteristics of cloud computing, virtualization and Chndmalkyty as compared to traditional computing model is associated with a different attack. Continuing with the security challenges that face data in cloud computing environments.

Challenges in communication

Consultants cloud models are available to customers via the Internet. Internet standard mechanisms and protocols used to communicate between clients and the cloud. Its process leading to the transfer of data / information or applications between the client and the cloud. In addition to taking on, communication between virtual machines within the cloud there. Its cloud into two categories: a. External communications to the cloud (between customers and cloud) and (b). With clear internal communication (communication that falls within the cloud infrastructure) to be divided. Between the outside (external) cloud is similar to other communication on the Internet. So the challenges that face cloud over Internet feature is similar to traditional IT communications challenges.

These challenges include denial of service, the person who is the real communication, eavesdropping, IP spoofing and impersonation. The solution to these challenges as well as traditional solutions such as Secure Socket Layer (SSL), Internet Protocol security (IPSec), encryption algorithms, and rape and abuse detection systems to prevent, relieve traffic congestion and certified digital certificates. Because the challenges and solutions in the nature and existence of traditional IT infrastructure rooted in this article is not to discuss the details. And stressed that the relationship between internal cloud for cloud specific characteristics and challenges of cloud technologies to produce certain.

Common communication infrastructure

Source Integration In addition to sharing computing and storage resources, to share network infrastructure components as well as threats. Share ownership for aggressive network components window provides multiple attack. Vulnerability of features originating source integration and cloud computing IaaS cloud service model affects. Due to the fact that legal monitoring detects network vulnerabilities and work hard

to exceed, usually providers such monitoring are not allowed. Indivisible parts of the network based on IP as unused network resources dynamically been released and is not used for a specified set of users.

Usually superuser access to the cloud users to manage their virtual machines. Bdnyt users are able to access the system's IP or MAC addresses to obtain and misuse of user interfaces have IaaS network. Aggressive user with superuser access to the actual network components in real network attacks such as spoofing do.

Virtual network

Communication activities in cloud computing systems in the network not only real but also virtual networks also play an important role in communication. Virtual networks are logical networks within a physical network can be built. Virtual network responsible for communication between virtual machines (VM) are. Network software components such as bridges, routers and software configurations in a network of networks, the VM Host support. Virtual networking in a cloud environment provide the following security challenges. Assault prevention and detection mechanisms and activities usually traffic patterns and identify anomalies judgment depends attack.

Virtual network creates an obstacle in the way of the goal of such preventive measures. Virtual network shared among multiple virtual machines and the possibility of special attacks, such as denial of service (DoS), Network scam punished. For the purposes of monitoring the traffic rate Bdtyntanh. Encryption keys are vulnerable to leaks. Data belonging to users who are in transition from costly breaches and violations of suffering. (Fig. 3)

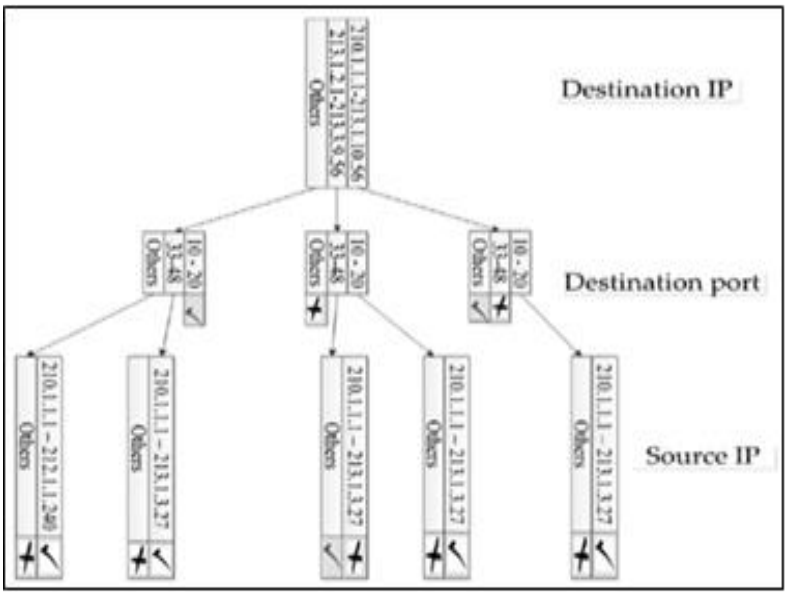


Figure (3): Firewall design tree using the IP address and port

The contractual and legal challenges

The use of cloud computing and applications, organizations can lead to administrative control CSP Dhd.kh This raises several issues, such as the guaranteed performance, comply with regulatory, geographical jurisdictions and monitoring the implementation of the contract shall .msayl service level agreement (SLA), comply with the law and the physical location of the data.

Service level agreement

SLA document that specifies the conditions between the user and CSP and emphasize the first minimi level of performance for CSP identifies and secondly, interactive activities, and thirdly, the consequences of a breach of an agreement between the user and the CSP.

Legal issues and concerns

In addition to technical issues, legal issues related to cloud computing resources of CSP in the areas of law that are working in different geographical regions. If the user data is transferred to a place that has different rules, security policy configuration to comply with the new regulatory areas can be difficult for users.

Security Solutions

Countermeasures for problems of architecture
virtualization

Pictures virtual machine components that require high security and integrity of the VM determines the initial status. Pictures VM basis for cloud computing security system provides total security. CSA following important measures to protect the system against damage virtualization, cloud computing offers:

1. makers should implement all the virtual OS in a virtual machine guest protect themselves.
2. The security measures embedded non-transferable and must be used for virtualized OS.
3. Use third-party security technologies to reduce dependence on CSP can be used.
4. VM disabled should be encrypted.
5. The security vulnerability assessment tools should cover virtualized environment.
6. virtualization-aware security tools must be implemented and used in cloud computing environments.

Security solutions, data / storage

CSA main recommendations with respect to key management and data security are as follows:

1. Key management either by the user or by the service organizations secure encrypted from a credible source.

2. should be of best practices related to key management and cryptographic products used reliable sources.

3.recommended standard technology should be used as much as possible.

4.key range must be maintained at individual and group level.

Countermeasures for communication issues

CSA guidelines for secure network communications using a combination of LAN and, IDS, IPS and virtual firewalls to protect transmitted data suggests. Suggested strategies for virtual network on leaked customer data and use the same infrastructure as well as stress. CSA use these tools with detailed and specific policy offers access management. The use of physical and virtual machines contract is approved by CSA in a virtual network visibility and traffic monitoring guarantees. ACPS different security services including the attacks against users and data sources, CSP CSP. ACPS is divided into several modules that are hosting platform. Is responsible for identifying suspicious activity in the separator module.

Detected suspicious activity alerts registered with the registrar module and set alerts are stored. ACPS Total coping for index defines critical infrastructure. Check periodically checksum also monitored cloud entry points to prevent the attack Dard.jht stable and fixed network infrastructure, in ACPS Search Network with IP tables set alerts and warnings recorded in the identification. In addition to providing network security and critical infrastructure, ACPS security against malicious attacks as well as provide data and virtual machines. An important feature of ACPS is to remain undetected Mandu VM transparent and isolator modules for prevent his identification system call does not block any request.

Contractual and legal solutions

The need for standardized processes for managing SLA's security with a view to security issues related to geographical legitimacy and reduce SLA. Web service agreement (ws) integration and disintegration of authority and service providers define and recognize a pattern-based arrangements to monitor the agreement. Ws agreements based primarily on the quality of service. Ws extended deal with SecAgreement framework was presented to the security and service parameters specified in the SLA. The extended model also integrates elements has specific risks of cloud services is calculated.

Security issues in MCC

Cloud computing makes it possible to access the data of mobile devices to connect to traditional cloud computing services and take advantage of them. Unlike conventional computing equipment, mobile equipment resources are limited. Some less processing power, storage capacity, low energy and limited Internet connectivity and computing does not allow variable storage applications to run on mobile devices. (2013, Fernando et al)

Similar restrictions incentive for new computing paradigm MCC acted as the capabilities of mobile devices with computing and storage transfer activities to promote cloud environment. Today, mobile devices can use the services of computing and storage cloud computing and storage to run heavy processes. MCC paradigm allows users to their applications and data through mobile devices without having to switch to traditional computing machine access and manage them. MCC is based on the traditional cloud computing hence all security issues raised Also inherits above. Although the scarcity in mobile devices take advantage of the proposed security solutions for cloud not allow the routine. Security solutions on the client (mobile device) to lighter versions require that mobile devices have the ability to run. The main security issues in MCC include:

1. Mobile Security Apps
2. User Privacy

3. Verification
4. data security

Mobile Application Security

Mobile devices (mobile) like traditional computing devices are exposed to harmful program vulnerability. Malicious programs can be in the form of Trojan horses, viruses, and worms, and mobile apps to risk. Traditional security software such as antivirus and IDS have the ability to run continuous mobile devices. Compromised security applications would also be compromised identity. The basic concept of computing off load heavy security in a cloud environment used to run programs that detects malicious programs and attacks on mobile devices.

User Privacy

Mobile devices for location-based services can be a source of leakage and seamless user's location. This is a new issue of privacy is that if the enemy knows the approximate location of the user in a worse position ends. Hide the exact geographic location of the user, the user's location protects privacy

Authentication

Another important issue in the field of mobile devices with limited resource or document is authenticated. Keywords with limited ability to input text commonly used for authentication purposes in MCC used to steal sensitive over time. Dynamics of production of credentials used for authentication sure. Credentials production because of low processing power mobile devices and implements reliable and trusted person entrusted.

Data security

Centralized encryption algorithms computing with large keys for low processing power of mobile devices and mobile devices and mobile phones are not able to run. MCC to a form of encryption requires minimal overhead communication, processing and storage is necessary. Activities focused on the calculation of the encryption / decryption for secure transfer of user data to find a trustworthy person.

Conclusion

Despite the numerous advantages of cloud computing, the environment, strengthen security concerns that have prevented the use of cloud computing is speed. All users, whether corporate or individual must be fully aware of the security risks in cloud environments. Understand the security risks and countermeasures also helped organizations to conduct cost-effective analysis and it is bound to change in a cloud environment. Since cloud computing technology, many traditional uses with new technologies and has unique issues and traditional security concerns. Virtualization and multi-ownership to different users allowed to use the same physical source. The specific security risks of cloud technologies has created a cloud that must be understood and evaluated from the perspective of new features. Virtual networks also unique security concerns created with the issues that they face with traditional physical network. There was no separation between virtual machines and sound development made it necessary to describe certain methods with equivalent physical separation. Expanding geographically diverse cloud

computing legal issues in relation to the assets and rights of users and the laws governing it are presented. Identity management and access control to digital resources as well as lack of administrative control Apple organizations in cloud computing is different. In this paper, concerns and security issues arising from the nature of shared, virtual and public cloud computing paradigm discussed.

References

A, Abbas. And S.U, Khan. (2014). A review on the state-of-the-art privacy preserving approaches in e-health clouds. IEEE J. Biomed. Health Inform..

D, AB, Fernandes. And L, FB, Soares. And J,V, Gomes. And M,M, Freire. And P, RM Inácio. (2014). Security issues in cloud environments: a survey. Int. J. Inform. Sec.

J, Che. And Y, Duan. And T, Zhang. And J, Fan. (2011). Study on the security models and strategies of cloud computing. Proc. Eng

K, Alhamazani. And R, Ranjan. And K, Mitra. And F, Rabhi. And S,U, Khan. And A, Guabtni. And V, Bhatnagar. (2013). An Overview of the Commercial Cloud Monitoring Tools: Research Dimensions. Design Issues. and State-of-the-Art. arXiv preprint arXiv:1312.6170,

M, Ali. And R, Dhamotharan. And E, Khan. S,U, Khan. And A,V, Vasilakos. And K, Li. And A,Y, Zomaya. (2015). SeDaSC: secure data sharing in clouds. IEEE Syst. J.

N, Fernando. And S,W, Loke. And W, Rahayu. (2013). Mobile cloud computing: a survey. Future Gener. Comput. Syst.