Cloud security issues

Piyush gupta
Assistant Professor, Department of Computer Science
Kamla Memorial College sidhi M.P
Affiliated to Apsu Rewa

Abstract: Cloud computing security or, more simply cloud security is an evolving sub domain of computer security, network security, and broadly, information security. It refers to a broad set of policies, technologies, and controles deployed to protect data, applications and the associated infrastructure of cloud computing.

Organization use the cloud in variety of different service models (Saas, paas, and IAAS) and deployment models (Private, Public, Hybrid). There is number of security issues associated with cloud computing but these issues fall into 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.

The responsibility goes both ways, however, the provider must ensure that their infrastructure is secure and their clients data and applications are protected while the user must ensure that the provider has taken the proper security measures to protect their information, and user must takes measures to use strong password and authentication measures. While cost and ease of two great benefits of cloud computing, there are significant security concerns that need to be addressed when considering moving critical applications and sensitive data to public and share cloud environments. To address these concerns, the cloud provider must develop sufficient controls to provide the same or grater level of security than the organizations would have if the cloud were not used.

There are ten items to review when considering cloud computing security.

1.Where’s the data?
2.Who has access?
3. What are are your regulatory requirements?
4.Do you have right to audit?
5.What type of training does the provider offer their employees?
6.What type of classification system does provide to use?
7.What are service level agreement (SAS)terms?
8.What is the long term viability of the provider?
9.What happens if there is a security breach?
10.What is disaster recovery/business continuity plan(DR/BCP)?

Keywords: Cloud security, Information security, Virtualization, Authentication, Inteigrity, confidentiality.

Introduction

Cloud evolution can be considered synonyms of banking system evolution. Earlier people used to keep all their money, moveable assets(precious, metals, stones)in their personal possessions and

And even in under ground lockers as they thought that depositing their hard earned money with bank can be disastrous. Banking system evolved over the period of times. Legal and security process compliances protected by law played a big role in making banking and financial system trustworthy. Now people hardly keep any cash with them. Most of us carry plastic money and transact digitally.

Cloud computing done in same way.

Robust cloud architectures with strong security implementation at all layers(SaaS, PaaS, Iaas)in the stack powered with legal compliances and government protection is the key to cloud security. As bank didn’t vanish despite frauds, thefts and malpractices ,cloud security is going to get evolved but as much faster rate. Cloud is complex and hence security measures are not simple too. Cloud needs to be at all layers in its stack. Different levels of cloud security are as follows:

Infrastructure level: A sysadmin of the cloud provider can attack the system since he/she has got all admin rights. With root privilages at each machine, the sysadmin can install or execute all sorts of software to perform an attack. Furthermore with physical access to machine, a sysadmin can perform more sophisticated attacks like cold boot attacks and even tamper with the hardware.

Protection measures: The major steps are given below:

1. No single person should accumulate all these previleges.

2. Provider should deploy stringent security devices, restricted access controle policies, and surveillance mechanisms to protect the physical integrity of the hardware.
3. Thus, we assume that by enforcing a security processes, the provider itself can prevent attacks that require physical access to machine.

Platform level: Security model at this level relies more on the provider to maintain ndata integrity and availability. Platform must take care of following security aspects:

1. Integrity: It assures us that data has not been changed without our knowledge. The information cannot be altered in storage or transit between sender and intended reciver without the alteration being detected. When we download a file over the internet, we would like to be sure that the file we hget is the one we wanted ,we would like to be assured of the files integrity. The following are the three goals of integrity:
a. Prevention of the modification of information by unauthorized users.
b. Prevention of the unauthorized or unintentional modification of information by authorized users.
c. Preservation of the internal and external consistency.

2. Confidentility: Confidentility assures us that data cannot be viewed by unauthorized people(The information cannot be understood by anyone for whom it was unintended).Confidentility is concerned with preventing the unauthorized disclosure of sensitive information. The disclosure could be intentional, such as breaking a cipher and reading the information, or it could be unintentional, due to carelessness or incompetence of individuals handling the information. The confidentiality services protects system data and information from unauthorized disclosure.

3. Authentication: The sender and receiver can confirm each others identity and the origin/destination of the information .Verification that the users claimed identity is valid, such as through the use of a password. At some fundamental level, we want to be sure that the people we deal with ate really who say they are. The process of proving identity is called authentication.

4. Defense against the inrusion and doss attack: Denial of service (DOS)is very popular attack in computer fields. The main aim of such type of attack is to slow down or totally interrupt the service of system. The attacker may have many ways to achieve this target. For example any unauthorized user might sends too many logins request to a server using random ids one after the other in quick succession can overload the network. The denial of service prevents or inhibits the normal use of management of communication facilities. This attack may have a specific target; for example an entity may suppress all messages directed to a particular destination.

5. SLA: A service level agreement(SLA) is a part of service contract where a service is formally defined. In practice the term SLA is sometimes used to refer to the contracted delivery time.

Application level: The following key security elements should be carefully considered as an integral part of application development and deploymdent process:
1. Application deployment model
2. Regulatory compliance: In general compliances means conforming to a rule, such as a specification, policy, standard or law. Regulatory compliance describes the goal that organizations aspire to achive in their efforts to ensure that they are aware of and take steps to comply with relevant laws and regulations.
3. Data segregation: Segregation is the sepration of an individual or group of individual from a larger group, often in order to apply special treatment to the sepreated individual or group. Segregation can also involve the sepration of items from larger groups, as seen with the handling of funds in certain type of accounts.
4. Avilability: This refers to whether the network, system, hardware,and software are reliable and recover quickly and completely in the event of an interruption in service. Ideally these elements should not be susceptible to denial service attacks.
5. Backup/recovery Procedure.

Data level: A part from securing data from corruption and losses by implementing data protection mechanism at infrastructure level, one needs to also make sure data is encrypted during transit and at rest.

Cloud security services

Cloud security service is a web based identity and access management solution. Cloud security services allows Software as a service, Platform as a service and infrastructure as a service providers to offer their enterprise customer the ability to deploy their existing identity infrastructure in a cloud. cloud security services is the cloud security brokers, a collection of cloud elements that work together to provide a secure place for cloud workloads and cloud storage. Software as a service and platform as a service platforms access the security broker via identity and event connecters, while the enterprise accesses the broker via on-premise secure bridge run from the data center. This secure bridge, which is firewall friendly, provides a protocol proxy, policy agent, audit agent, secure communication manager and key agent. The broker ensures that sensitive information always remains behind the firewall. According to their different functions, cloud security services can be divided into four layers namely virtualization platform, infrastructure services, fundamental services and application services.

1. Cloud security virtualization platform: Virtualization technology is the core of the cloud. virtualization platform is the base of the cloud computing security service model. virtualization platform can isolate running program among different operating systems on the same machines avoiding resource conflicts. In addition virtualizations can improve the utilizations of the underlying hardware dynamically distributing idle hardware to the program needed. Virtualizaton can be broadly divided into infrastructure virtualization, software virtualization, and system virtualizatons.

2. **Cloud security infrastructure service:** Cloud security infrastructure serves cloud application with security store and computing. It can not only defense against attack from hacker ,but also ensure users data and applications not be jeopardized.In cloud computing infrastructure platform comprehensive security measures must be taken, such as access controle system in physical layer ,data in tegrity, log management, data encryption, backup and disaster recovery in storage layer, vulnerability management in application layer.

3. Cloud security fundamental service: Cloud security fundamental service belongs to paas is an important method to satisfy the goal of user for the security. There are several cloud security services.

a. cloud user identity management service.
b. cloud access controle service.
c. cloud audit service.
d. Cloud cryptographic service.

4. Cloud security application service: Traditional network security technologies are limited in defense capabilities, response speeds,system scope, it is difficult to meet the increasingly complex security reqirements. The large scale computing power of massive storage capacity provide bt cloud computing significantly increases the security event collection correlation analysis, virus prevention and other aspects of performance.

Cloud design principals

Every enterprise has different levels of risk tolerance and this is demonstrated by the product development culture, new technology adoption, IT delivery service model, technology strategy, and investments made in the area of security tools and capabilities. When business unit within an enterprise decides to leverage. Software as a service for business benefits ,the technology architectures should lend itself to support that model. Additionally the security architecture should be aligned with the technology architecture and principals. Following is a sample of cloud security principals that an enterprise security architect needs to consider and customize:

a. Services running in a cloud should the principal of least privileges.

b. Isolation between various security zones should be guaranteed using layers of firewall, cloud firewall, hypervisor firewall, guest firewall application container. Firewall policies in the cloud should comply with trust zone isolation standards based on data sensitivity.

c. Applications should use end to end transport level encryption (SSL, TLS, and IPSEC)to secure data in transit between applications deployed in the cloud as well as to enterprise.

Secure cloud requirements

Many organizations dealt with various types of security requirements in cloud computing. It is also hard to understand which types requirements have been under researched and which are more investigated. We can classify cloud security requirements into twelve sub areas: Authentication, Single sign on, Delegation, Confidentility, Integrity, Non repudation, Privacy, Trust, Policy, Authorization, Accounting and audit.

1.Authentication: At an automated bank machine, we identify ourself using bank card. We authenticate ourself using a personal identification number (PIN).The PIN is shared secret, something that both we and bank know. presumbly we and the bank are the only ones who this number. When we use a credit card we identify ourself with the card. We authenticate ourself with our signature. Most store clerks never check the signature ,in this situation possession of the card is authentication enough.

2. Single sign on: Single sign on (SSO)is a session/user authentication process that permits a user to tnter one name and password in order to access multiple applications. The process authenticate the user for all applications they have been given rights to and eliminates furthure prompts when they switch applications during particular applications.

3. Delegations: If a computer user temporarily hands over his authorizations to another user then this process is called delegations.

4. confidentiality: The confidentiality service protects system and information from unauthorized disclosure. When data leave one extreme of a system such as a clients computer in a network, it venture out into nontrusting environment. So recipient of that data may not fully trust that no third party like a cryptanalysis or a man in the middle has eavesdropped on the data.

5. Intigrity: Intigrity can be used in reference to the proper functioning of network, system, or application. For example whwn the term integrity is used in refrence to a system it means that the system behaves according to design, specifications, and expectations even under adverse circumstances such as an attack or disaster.

6. Nonrepudation: Repudation is the denial by one of the entities involved in the communication of having participated in all or part of the communication. Such denials can be prevented by nonrepudation. Nonrepudation allows an exchange of data between two parties in such a way that the parties can not subsequently deny their participation in exchange. Non repudation can be achived using digital signature.

7. Privacy: Internet privacy involves the desire or mandate of personal privacy concerning transactions or transmission of data via the internet. It also envolves concerning transaction or transmission of data via the internet. It also involves the exercise of controle over the type and the amount of information revealed about a person on the internet and who may access said information. Personal information should be managed as a part of data used by organization. It should be managed from the time the information is conceived to its final disposition.

8. Trust: Organizations belief in the reliability, truth, ability, or strength of someone or something. Trust involves around ‘assurance’ and confidence that people, data, entities, information or processes will function or behave in expected ways.

9. Policy: The term policies are high level requirements that specify how acces is managed and who under what circumstances may access what information. A security policy should fulfill many purposes. Under what circumstances may acces what information. A security policy should fulfill many purposes.

10. Authorizations: Authorizations is the act of checking to see if user has a proper permission to access a particular file or performs a particular actions. It enables us to determine exactly what a user is allowed to do.

11. Accounting: Accounting service keep track of usage of services by other services so that they can be charged accordingly.

12. Audit: Audit services keep track of security related services.

Policy implementation

Organization implementing cloud computing should think about security first before deploying a production environment according to the national institute of standard and technology (NIST). ons should consider when outsourcing data, applications

Guidelines of security and privacy in cloud computing provides an overview of the security and privacy challenges for cloud computing and present recommendations that organizations should consider when outsourcing data, applications, and infrastructure to a public cloud environment. The key guidelines recommended to federal departments and agencies and applicable to private sector include:

1. Carefully plan the security and privacy aspects of cloud computing solutions before engaging them.
2. Understnad the cloud computing environment offered by cloud provider and ensure a cloud computing solutions satisfies organizational security and privacy requirements.

Cloud computing security challenges

Cloud com putting attracts users with its great elasticity and scability of resources with an attractive tag line **“pay-as-you-use”** at realatively low prices. Compared to the constructions of their own infrastructure customers are able to cut down on expenditure by migrating computation storage and hosting on to the cloud. Although this provides savings in terms of finance and man power it brings with new security risks. Considering the influence of cloud computing with respect to its business benefits and technological transformations the future applications are going to be completely dependent on it. It has its benefits nevertheless it has numerous issues and challenges with respect to the security aspects. There are many research organizations, cloud vendors, product development enterprises and academic research institutes working on various security classifications of cloud computing and its solutions. The current security challenges in cloud computing enviromnment based on following two categories.

Category1:

a. Logical storage segregation & multitenancy security issues
b. Identity management issues
c. Insider attacks
d. Virtualizations issues

Category2:

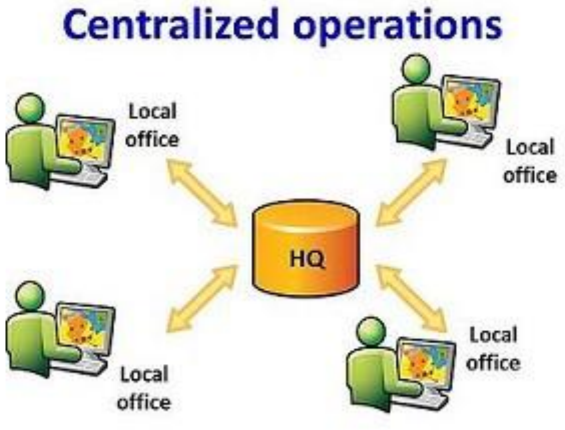
a. Insecure APIS
b. cloud and cloud services provider (csp) migration issues

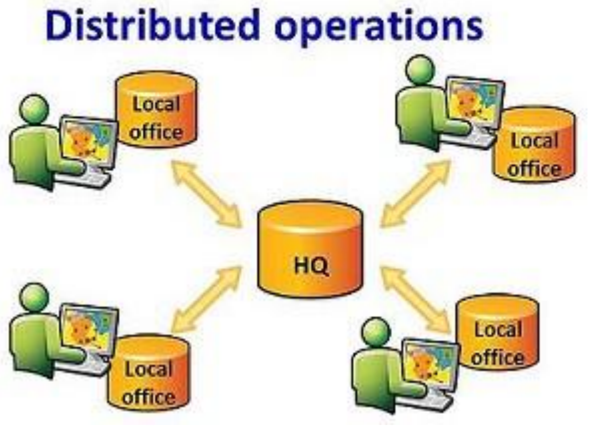
Virtualization Security management

Virtualization security focuses upon end to end security, Integrity, auditability, and regulatory compliance for virtualizations and clouds. virtualizations security starts where cloud and virtual environment begin: the end user computing device. Virtualization and cloud security is implemented where there is an intersection between user, data and application while maintain strict controle of management interfaces. As such virtualization security looks into all aspects of security devices, tools, controles, and guides that impact or can be used to secure virtual and cloud environments.

Cloud central security system Architecture

This topic discusses the architecture of central cloud security system which is designed and delivering “Security -as -a -service” model to cloud stack. Central security system is based on the facts that by shifting all the security related services to application level. a generic and secure framework for cloud based platform can be deployed. This menas that all security related services ,like security service, identity, access cntrole, authentication and authorizations mechanisms are provided by cloud security infrastructure.





Conclusion:

Cloud computing is a new technology which is being quickly adopted by many organizations due to the benefits it has and one of the most important aspect is the Security. We discussed here some security issues that can be adopted as countermeasures.

References

[1]. http://searchvirtualdatacentre.techtarget.co.uk/news/1510117/Community-cloud-Benefitsand-drawbacks.

[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]. Harjit Singh Lamba and Gurdev Singh, “Cloud Computing-Future Framework for emanagement of NGO's”, IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.

[4]. Dr. Gurdev Singh, Shanu Sood, Amit Sharma, “CM- Measurement Facets for Cloud Performance”, IJCA, , Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, June 2011.

[5]. Joachim Schaper, 2010, “Cloud Services”, 4th IEEE International Conference on DEST, Germany.

[6]. Tackle your client’s security issues with cloud computing in 10 steps, http://searchsecuritychannel.techtarget.com/tip/Tackle-your-clients-security-issues-withcloud-computing-in-10-steps.

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

[8]. Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(2), 39-51, University of Texas, USA, April-June 2010.