THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Review of Different Security Assessment Models Using in Cloud Environment

Jasdeep singh
Research Scholar, CE Section, Yadawindera College of Engineering, Punjabi University, Guru Kashi Campus, Talwandi sabo, Punjab, India
Manoj Kumar
Assistant Professor, CE Section, Yadawindera College of Engineering, Punjabi University, Guru Kashi Campus, Talwandi sabo, Punjab, India

Abstract:
Cloud computing is providing us a suitable choice of computing and storage of the resources mainly for the BUSINESS in which user "pay per usage". But most of the organizations are not using the cloud computing due to the lack of the trust on the service provider. In this time data breaches in cloud services are also increasing year-by-year by the hackers which are trying to compromise the security of the cloud. In this paper we have performed a depth analysis of cloud trust models for the existing functional and non-functional aspects to accurately evaluate the trust of cloud provider and the theory of assessment of the security level of insider threats. Firstly, we describe the modeling methodology which captures several aspects of insider threats and show threat assessment methodology to reveal the possible attack strategies of an insider.

Keywords: *cloud computing, assessment models, Security, threats, attacks*

1. Introduction

Cloud computing is involved in everyone's life. It provides us the applications and storage space as services over the network at a small cost or free of cost. Most of us use the clouds services in our daily life. In which we use different search engine and there cloud servers for store our search results (Google, yahoo, Bing); use of email services for exchange of data and information to someone (Google, Yahoo and etc.); use of the social networking websites for messaging to friend and stay connected with them (Facebook, Myspace and Twitter); for the storage purpose of music, image, videos and documents (Dropbox, iCloud and etc.); in cloud computing also the facility of online backup of the system or the data which automatically backup the file over the internet(jungledisk, mozy). Cloud computing is also using in companies for their business purposes. Companies rent the servers, virtual machine and the other resources from the cloud services provide. These companies pay the services provider as per usage of the resources. It saves maintains and the operational cost of the resources. For example: The social news website rents amazon elastic compute cloud (EC2) for their digital bulletin board services [1]

There is no question on the resources and the less cost of the cloud services changed our lives; but there are some security issues included in cloud computing scarce everyone to the cyber-crimes which are happening in daily life. Hackers use the lots of techniques to compromise the access of the cloud server without using the legal authentication. It is a challenge for providing the competent security to the cloud service for perform as aimed.

In general computer security identifies three main objectives [2]

- Confidentiality: it is that objective of cloud computing service or the data is only usable for the authorised user and no unauthorized access of the data.
- Integrity: it assures that data is not changed neither when it is stored nor while it is trans formed over the network
- Availability: it assures that services and the data will be available when it needed.

These security objectives need use of security mechanism and services to be implemented. So we will be able to identify the process, a device aimed to detect, prevent and recover the attack. There are several security techniques are used like encryption, cryptography and hash function.

Because once the exact location of the data is located by the hackers they will use the information and the data for wrong purposes. They will steal the private information and give them whom this needs for criminal reasons. In leakage accident, Epsilon leaked millions of names and email address from the customer database. Stratfor's 75,000 credit card numbers and 860,000 user names and passwords were stolen [3].

2. Cloud Computing Service Models

Cloud computing includes the providing of the computing services (storage, application and server) to the user by cloud computing service provider. User can access the cloud assets by the internet. Cloud services provider grantee the merit of services. In cloud computing there are three layers in cloud service model: platform layer, application layer, system layer.

The first layer or bottom layer is the system layer which includes the memory, network devices, storage and the computational assets for example infrastructure of servers. System layer is also known as infrastructure as a service. Computational assets are made available for user on demand services. Infrastructure as a services also provide the virtual machines by which user can create a complex infrastructure. It reduces the cost of buying the physical resources and also reduces the load of the network administration because IT professional is not needed for the monitoring of the physical network. we have an example of cloud services provider which provides the IaaS is Amazon's EC2[1]. It gives the virtual computing with network interface, by using this interface user can use virtual machines over Linux, Window and Solaris and run their own applications.

The middle layer is platform layer which is specially designed for the user to develop their specific application. This layer is also known as the platform as a services. It provides development platform and service provider in this model provide the tools and the libraries for the development of the applications and allows the user to control over the application development and configuration settings. By using the PaaS user do not need to by software development tool, hence it also reduces the development cost of application. Google apps is an example of PaaS it is a package of Google tools. That provides Google search engine, Gmail, Google Groups, Google Talk and Google Docs. It gives the user to customize their tools over his domain.

The top layer is the application layer, it is also known as software as a service (SaaS). Application layer provide the service to rent the running application over the cloud instead of purchasing these applications. It reduces the cost of the application; SaaS is so popular in companies that do business. In the example of Saas Groupon is the one of many, by provided online support system it processes thousands of tickets more efficiently of their daily customer [1]. Table 1 is the example of cloud service provider on three cloud service models.

Cloud Service Models	Cloud Service Provider
SaaS	Antenna Software, Cloud9 Analytics, Google Apps, Microsoft 365, Rackspace and IBM.
Paas	Google Apps, Netsuite, WorkXpress and Microsoft Azure.
IaaS	Amazon Elastic Compute Cloud, Rackspace, Bluelock and Openstack.

Table 1: Cloud Service Provider on Cloud Service Models

In cloud computing these are three main services models out of five. In this mainly the concentrate on the bottom layer which is IaaS. It is the layer which is provided the access control of the virtual infrastructure like virtual machine. Cloud IaaS have changed everything in developer's way for deploy their applications. Before that developers spend their lots of time for own data centres, managing and hosting companies or services and then they hire operational staff to perform the operations. Now just only go to one of the IaaS provider, get virtual server with in minute [4] and pays as usage. Iaas is completely distant the hardware under it and provide users to use infrastructure without disturbing anything the basic difficulties. Iaas gives only fundamental security (perimeter, firewall, load balancing, etc.) and application running into the cloud will need advanced level of security granted at the host [4].

3. Vulnerabilities

Vulnerabilities are the hole or the weak spot in the security that can be used by hacker or threat to gain the unauthorised right to use of the assets. There are four areas of vulnerabilities in the cloud environment [5]. They are:

- Cloud Infrastructure, Platform and Hosted Code
- Data, Data Integrity, Data privacy.
- Access – Access Control, Authentication and User identity management
- Regulation.
- There are some more vulnerabilities given in the operation / process [6].
- General Stack vulnerabilities: it is known as a virtualized request of a customer someway changes or disturbs another's request.
- Execution Control: it's that when the customer has only the execution but the main control of this execution is under the control of the service provider
- Data Stability:In this customer's data is someway uncovered after the changing or moving of the cloud service provider.
- Multiple party cloud privacy: It is more exact to the privacy concern but also it is related to general stack vulnerabilities.
- Authorization: This ensures that only the authorised resources are provided.
- Access Issue: cloud service provider is more close to the data, there is a fear of unauthorized access of data may occur.
- Identity Management.

3.1. Security Issue in IaaS

With the help of the IaaS the Provider has a good control upon the security until there is no gap in the virtualization manager. Also, during the theory of virtual machine may be capable to address these problems but in real or practical there are number of security issues [7][8]. Another issue isthe reliability of the data which is stored in the service provider's hardware. Due to increasing

virtualization of all in information society, holding the crucial control over data to the holder of the data despite of its exact location will become a topic of greatest interest. To get utmost faith and security on a cloud asset, different method should have to be applied [9]

The security responsibilities of the provider and the user are different from each other in cloud service models. Amazon EC2 (Elastic Compute Cloud) infrastructure as a service giving, as an example, consist of provider in security responsibilities up to hypervisor, it means that they can only provide security over physical layer, virtualization and environmental security. The user is in charge for the security control which includes the IT system, application, data and operating system [10].

While cloud structural design is an ad hoc technology, the basic technologies stay the similar. The cloud is presently built upon the internet and all the security concern related to internet are also acted by the cloud. The base of the cloud tools makes the user and service provider live at diverse location and nearly access the resources upon the web. Even if vast quantity of security is set in the cloud, still the data is broadcasted through the basic Internet technology. So, the security fears which are menacing the Internet also menace the cloud. But, in a cloud, the risks are significantly high. This is because of its weakness and the plus value of the resources and their environment of them living in together. Cloud schemes still uses basic procedures and security calculates that are used in the Internet but the needs are at advanced level. Encryption and secure protocols provide to the requirements to a positive degree but they are not framework oriented. A strong set of policies and set of rules are needed to help safe broadcast of information inside the cloud. Fear regarding interference of data by outside non Customers of the cloud during the internet should also be measured. Methods should be set in place to create the cloud location secure, confidential and inaccessible in the Internet to keep away from cyber criminals attacking the cloud.

4. Threats to Cloud Computing

In this section we consider threats related to cloud service in security architecture. Here are some possible threats which are related to cloud and IaaS based on review of papers and knowledge [11].

- Change in Business Model: Cloud computing changes the technology and way of IT services. Services are provided by external service providers. Business needs to assess the risks related with the failure of manage over the infrastructure. This is the higher threats which get in the way usage of cloud computing services.
- Insecure Interface and APIs: Service provider frequently provides the set of API to the user to design an interface to communicating with the cloud service. These interfaces add a level on the top of the structure and it increases the complexity of the cloud. It allows the vulnerabilities to move to the cloud environment. Offensive use of those interfaces pose threats like clear text authentication, improper authorization and broadcast of content. There type of threats may affect the IaaS, Saas and Paas.
- Malicious Insider: Most of the organization hides the procedures in the access of the employees and their using policies for the employees. Then how a user can get the access of confidential data and policies. It always happens due to lack of clearness in cloud provider procedure and process. Inside threats a lot use the bypass through the firewall so the detection system thinks that it is a legal user or activity. In this condition insider can harm the cloud service providing. For example, insider can get private data and can access the control over tje services without any detection risk. These types of threats also related to IaaS, SaaS and PaaS.
- Shared technology issues: In shared technology architecture, virtualization is used to provide on-demand shared services. Same application is used in different users to get access the virtual machine. There vulnerabilities allow a malicious to gain the control and access another user' virtual machine. IaaS services are used over mutual assets, which might not be intended to afford strong isolation.
- Data Loss and Leakage: Data can be negotiated in differenttypes. This might contain data negotiation, removal, or change. Because of the dynamic and divided nature of the Cloud, these threatscan provide a key issue leading to information theft. Examples of these risks are lack of verification, approval and review control, weak encryption procedures. This threat can applicable to IaaS, SaaS, and PaaS.
- Identity theft: Identity theft is a type of scam in which someone makes believe to be someone else, to useassets or get credit and other profit. The casualty (of identity theft) can experience poor cost and losses and supposed responsible for the executor actions. Significant security threatscontainweak password recovery techniques, key loggers and etc. This affects IaaS, SaaS, and PaaS.

5. Various Assessment Models

Cloud-Trust is a Security Estimation Model for Infrastructure-as-a-Service (IaaS) Clouds [12] is bestowed by Gonzales, D. et. all. it's a cloud design reference model that includes a good vary of security controls and best practices, and a security assessment model. Cloud Trust is which estimates high level security metrical to compute the quantity of confidentiality and integrity presented by a Cloud Computing Systems (CSS) or cloud service supplier. it is employed to measure the protection level of 4 multi-tenant IaaS cloud structures equipped with various cloud security controls and to indicate the likelihood of CCS penetration (high price information compromise) is high if a negligible set of security controls square measure enforced. CCS penetration likelihood drops considerably if a cloud defence thorough security architecture is given thatdefend virtual machine (VM) images at rest, supports CSP and cloud occupier computer user access controls, and that employs various network security controls to attenuate cloud network police investigation and discovery of live VMs. In optimized fine-grained and truthful rating theme [13], two powerful problems are

addressed for IaaS platform: (1) the profits of resource suppliers and customers usually contradict mutually; (2) VM-maintenance overhead like start-up price is commonly too vast to be neglected.

A model referred to as a multi-tenancy trusty computing surroundings model (MTCEM) for cloud computing has been designed to deliver trusty IaaS to users with a twin level transitive trust system that supports a security task division purpose at the same time [14]. Because cloud services relate to several stakeholders admire Cloud Service suppliers(CSP) and users, they relate to various security area and provide totally different security smatter at the same time. The totally different stakeholders could also be driven by different motives admire finest service, maximization of the come back on asset and therefore may go damaging to the opposite party concerned. therefore, cloud computing ought to have the capability to part every client and CSP and support security duty separation shaping clear and flawless security depend ability limits for CSP and users. MTCEM has been purposed as two level pecking order transitive trust string model that supports the safety duty division and supports three forms of distinct stakeholders particularly, CSP, users and auditors. During this model, CSP suppose the responsibilities to stay infrastructures trusty whereas the client assumes responsibility ranging from the guest operating system which put in by the client on the Virtual Machines given by the CSP. The auditor checks the services provided by the CSP on behalf of the user. The authors have enforced an example system to show that MTCEM is able of being enforced on business hardware and computer code. However, no analysis of the example on performance has been bestowed.

The ENISA report [15] conjointly given associate approach for risk assessment primarily based the estimation of risk levels. Security risk would be high if each the chance of the event and its impact area unit high. Risks area unit categorised into 3 groups: policy and structure risks, technical risks and legal risks. The assessment provided is semi-quantitative, because it uses price ranges for each event chance and impact, however doesn't take into account their combined influence during a quantitative manner. Instead, the ultimate risk assignment (as High, Medium or Low) relies on knowledgeable opinion, that takes the 2 factors into thought. Maybe, risk because of trafficker lock in is assessed to be High, as a result of its chance is high, however impact is Medium. Loss of Governance is shown as a risk with each high chance and high crash, and thence a 'very high risk'. Atotally quantitative risk assessment framework would any improve this technique, as a result of it allows the stakeholders to relatively measure the risks concerned and protection measures. Many alternative application domain, appreciate atomic energy, public health and environmental coming up with, use such totally quantitative frameworks [16].

A quantitative risk and impact assessment framework (QUIRC) is given [17], to assess the protection risks related with cloud computing policy. This structure, called QUIRC, defines risk as a mix of the likelihood of a security threat occurrence and its brutality, calculated as its Impact. Six key security objectives square measure known for cloud platforms, and it's projected that the majority of the everyday attack vectors and events map to 1of those six classes. Wide-band Delphi technique is projected as a scientific means that to collect the knowledge necessary for assessing security risks. Risk assessment knowledge bases may well be developed specific to each business vertical, that then function in puts for security risk estimation of cloud computing policy. QUIRC's key advantage is its absolutely quantitative and unvaried convergence approach, which allows stakeholders to relatively assess the relative lustiness of various cloud vender offerings and approaches in an exceedingly defendable manner.

6. Conclusion

Trust Assessment is getting key priority with the growth of cloud service providers that takes and store user data in their Data warehouses. Trust assessment provides user with a level of trust in the provider as enterprise and user data security is a key parameter. Various trust assessment models have been developed, each having different way to define trust etc. In this review, we have looked upon at various trust assessment models namely, Cloud-Trust, MTCEM, ENISA and QUIRC. Each model has different key advantages and user base. Cloud-Trust provides a ground level bare metal security assessment scheme. MTCEM provides an enterprise as well as cloud administrator a peek at cloud security by providing multi-tier support. ENISA provide the assessment based on system policy and legal aspect of it. QUIRC is based on a mixed probability model to assess risk analysis. Although each has mixed advantage, none of the model directly addresses Insider attack and its potential vulnerability assessment. This leaves us to develop a model that addresses this issue.

7. References

i. Te-Shun Chou, "Security threats on cloud computing vulnerabilities" International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, June 2013
ii. Mohammed M. Alani, "Securing the Cloud: Threats, Attacks and Mitigation Techniques" International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, June 2013
iii. Sophos Security Threat Report 2012. http://www.sophos.com/
iv. Ramkumar.et.all, "Towards A Theory Of Insider Threat Assessment" International Conference on Dependable Systems and Networks (DSN'05)
v. Frederick R. Carlson, "Security Analysis of Cloud Computing" fcarlson@ieee.org
vi. Scarfone, K., Souppaya, M., & Hoffman, P. U.S. Department of Commerce, "National Institute of Standards and Technology. (2011). NIST Special Publication 800-125 - Guide to Security for Full Virtualization Technologies". Retrieved from http://csrc.nist.gov/publications/nistpubs/800125/SP800-125-final.pdf
vii. Attanasio CR,"Virtual machines and data security" Proceedings of the workshop on virtual computer systems. New York, NY, USA: ACM; 1973. p. 206–9.

viii. Gajek S, Liao L, Schwenk J,"Breaking and fixing the inline approach" SWS '07, Proceedings of the ACM workshop on secure web services. New York, NY, USA: ACM; 2007. p. 37–43.
ix. Descher M, et al. "Retaining data control to the client in infrastructure clouds". International conference on availability, reliability and security, ARES '09, 2009, p. 9–16.
x. Seccombe A, et al. Security guidance for critical areas of focus in cloud computing, v2.1. Cloud Security Alliance, 2009.
xi. Top 7 threats to cloud computing. HELP NET SECURITY. http://www.netsecurity.org/secworld.php?id=8943
xii. Gonzales D, et.all "Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds", IEEE Transactions on Cloud Computing, pp 1. (2015).
xiii. Hai Jin, Xinhou Wang, Song Wu and Sheng Di, "Towards Optimized Fine-Grained Pricing of IaaS Cloud Platform", IEEE Transactions on Cloud Computing. Vol 3, issue 4, pp. 436-448, (2015).
xiv. Xiao Yong Li, Li Tao Zhou, Yong Shi, and Yu Guo, "A trusted computing environment model in cloud architecture," in Ninth International Conference on Machine Learning and Cybernetics(ICMLC), vol. 6, Qingdao, China, 2010, pp. 2843-2848.
xv. ENSIA Report on Cloud Computing Security Risk Assessment.http://www.enisa.europa.eu/act/rm/files/deliverables/cloudcomputing-risk-assessment.
xvi. Saripalli, K.P, et.al, 2003. Risk and hazard assessment for projects involving the geological sequestration of CO2 In: Gale, J. and Y. Kaya (eds.) Sixth International Greenhouse Gas Control Conference, Kyoto, Japan, pp. 285–289.Elsevier Ltd. (2003).
xvii. Prasad Saripalli, et.al, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security" 2010 IEEE 3rd International Conference on Cloud Computing