Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol.6, No.1, 2016
www.iiste.org

Data Safety Contact Control Model of Cloud Computing

Muhammad Tariq
Government College University Faisalabad Layyah Campus Punjab, Pakistan

Abstract
The progress of cloud computing are facing by many difficulties, which one of the most important challenge is data security problem. Everyone wants to use cloud computing due to cost saving and new agile business model which resulted by its dynamic, sharing, openness and highly centralized data. There complex data security challenges in cloud computing. From the view of users the research about data security focused on methodologies that ensuring the safety of data and storage. This paper provides a control model of a secured data access by on MAC access control. This is origin experience from the government cloud platform construction. This model provides the most important technical and management techniques with the security of data accessing. In shortly, the practical applications test showed that the model with corresponding control mechanism cloud meet the necessaries for reliable applications of government cloud.
Keywords: Control Model of Access Control, Security of Cloud Computing, Access Control of Secured Data.

1. INTRODUCTION

Cloud computing is a new computing paradigm where in computer processing is being performed through internet by a standard browser. Access control is a fundamental aspect of information security that is directly tied to the primary characteristics such as confidentiality, integrity and availability. Cloud computing service providers should provide the following basic functionalities from the perspective of access control: (i) Control access to the service features of the cloud based on the specified policies and the level of service purchased by the customer. (ii) Control access to a consumer's data from other consumers in multi-tenant environments. (iii) Control access to both regular user functions. Access control models can be traditionally categorized into three types: (1) Discretionary (2) Mandatory and (3) Role-based. In the discretionary access control (DAC) model, the owner of the object decides its access permissions for other users and sets them accordingly.

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

Cloud security control is effective only if the correct defensive implementations are in place. An efficient cloud security control should recognize the issues that will arise with security management. The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security control, they can usually be found in one of the following categories. However, the progress of cloud computing is also facing the key issues which one of the security issue and it is most important. In 2009 the Gartner's can survey and show the result that more than 70% of CTO interviewed enterprise ensure that the primary cause of the non-adoption of cloud computing by presence of privacy and security of data. Security of service model based on cloud computing according to identity and access security, data security, server security, storage, network and physical device security etc., which is concerned by the academic community and cloud computing service provider. In a international conference of information security RSA2010 it is considered that cloud computing security problem is a serious problem and CSS special seminar on cloud computing from 2009. Many companies, research etc. have research related study; security vendors are also concerned with various categories of cloud computing security products. This paper analyze factors of risk of data security access issues, control model of data security access which is commonly used to secured cloud government building.

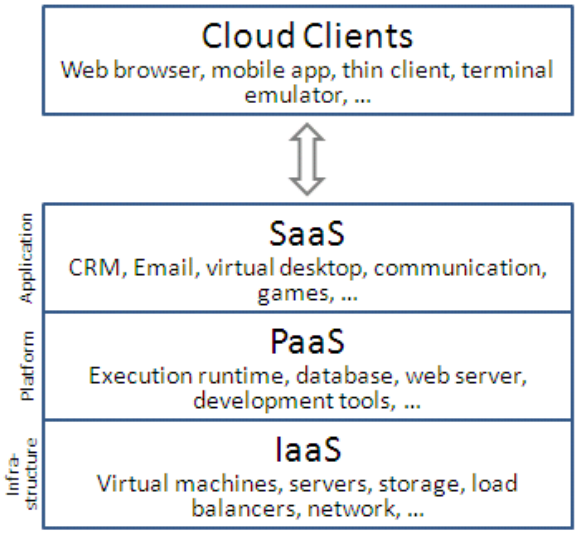
2. RESEARCH ON SECURITY TECHNOLOGY OF CLOUD COMPUTING

Cloud computing aims to flexibly scalable infrastructures using virtualized resources. Although virtualization improves efficiency and flexibility, it also introduces new threats. We mitigate these threats by means of new security technologies for protecting virtual environments. Moreover, we design novel mechanisms that provide protection levels beyond those of today's non-virtualized systems. Our projects follow two goals:

1. to ensure that virtual infrastructures are at least as secure as traditional infrastructures.
2. To leverage new capabilities to further strengthen security.

The first goal ensures that virtualized infrastructures provide a level of confidentiality, integrity, and availability which is similar to that of traditional infrastructures. One important requirement is the proper insulation of multiple customers. One example of a project in this space is the virtual systems security auditing project. The second goal aims at using virtualization to provide stronger or more efficient security. For example, one goal we are pursuing in our virtualization project is the use of virtualized intrusion detection.

Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid,and Community).



There are a 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-,or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the on the cloud). The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures. When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially business sensitive and confidential data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the third biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity.

In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers often store more than one customer's data on the same server. As a result there is a chance that one user's private data can by viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole datacenter to go down or be reconfigured to an attacker's liking.

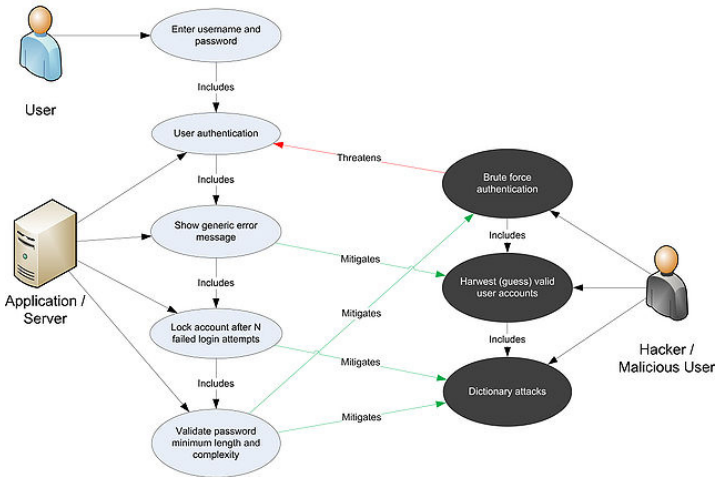
Cloud access security brokers are the top security technology trend for 2014, according to analyst firm Gartner.

Gartner said, in many cases, initial adoption of cloud-based services has occurred outside the control of IT, and cloud access security brokers offer an organization increased visibility and control as its users access cloud resources.

Adaptive access control, a form of context-aware access control that acts to balance the level of trust against risk at the moment of access, was named in second spot.

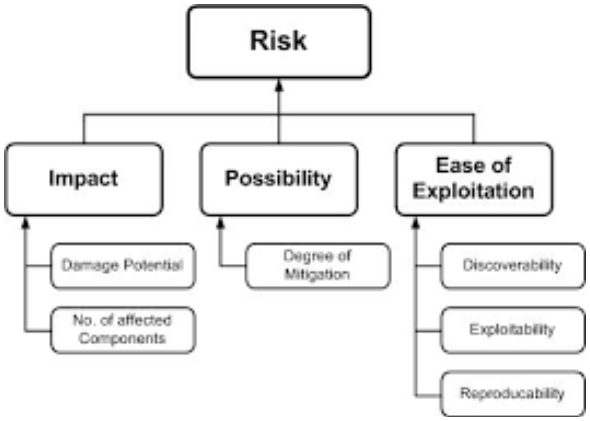
According to Gartner, adaptive access management architecture enables an organization to allow access from any device, anywhere, and allows for social ID access to a range of corporate assets with mixed risk profiles.

3. CATAGORIES AND SOURCES OF DATA SECURITY RISK

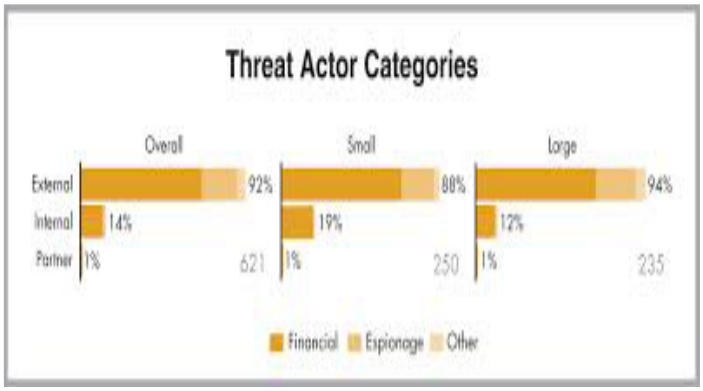


Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). Vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (man-made or act of nature) that has the potential to cause harm.

The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called "residual risk".



Computer system threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, worms, phishing attacks, and trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. Intellectual property is the ownership of property usually consisting of some form of protection. Theft of software is probably the most common in IT businesses today. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile. Cell phones are prone to theft and have also become far more desirable as the amount of data capacity increases. Sabotage usually consists of the destruction of an organization′s website in an attempt to cause loss of confidence to its customers. Information extortion consists of theft of a company′s property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner. There are many ways to help protect you from some of these attacks but one of the most functional precautions is user carefulness.



4. CONTROL MODEL OF DATA SCURITY ACCESS

On the based advantages and disadvantages of access control model, the paper proposed access control model of cloud computing control plateform which apted to the government administration.

A. COMMON ACCESS CONTROL

Access to accounts can be enforced through many types of controls.

1. Mandatory Access Control (MAC)
2. In MAC, users do not have much freedom to determine who has access to their files. For example, security clearance of users and classification of data (as confidential, secret or top secret) are used as security labels to define the level of trust.
3. Discretionary Access Control (DAC)
4. In DAC, the data owner determines who can access specific resources. For example, a system administrator may create a hierarchy of files to be accessed based on certain permissions.
5. Role-Based Access Control (RBAC)
6. RBAC allows access based on the job title. For example, a human resources specialist should not have permissions to create network accounts; this should be a role reserved for network administrators.
7. Rule-Based Access Control
8. An example of this would be only allowing students to use the labs during a certain time of the day.
9. Organization-Based Access control (OrBAC)
10. OrBAC model allows the policy designer to define a security policy independently of the implementation
11. Responsibility Based Access control
12. Information is accessed based on the responsibilities assigned to an actor or a business role

B. DATA SECURITY MODEL BASED ON MAS

Multi Agent system (MAS) architecture is critical to ensure high security facilitation based on the way of its development. A security framework based on MAS architecture to facilitate confidentiality, correctness assurance, availability and integrity of collaborative cloud data storage (CDS) environment is proposed. In order to verify our proposed security framework based on MAS architecture, a pilot study is conducted using a questionnaire survey. Rasch software is used to analyze the pilot data. Item reliability is found to be poor and a few respondents and items are identified as misfits with distorted measurements. As a result, some problematic questions are revised and some predictably easy questions are excluded from the questionnaire,in accordance with the model gives the various stages technologies stratgy and management strategies.

1) Examination and building access control baseline before the event

The event is much lower than tracking and recovery after the event. It can greatly reduce the danger of data loss. Before the event include database security examination, configuration of duties, setting of object level and role level access control, grading marked of sensitive data and permissions setting.

a) Technology strategy

Flow verification and threat evaluation under the normal business examination environment.

- Establishment reasonability defferenciantion strategy standardized DBA user privilege, discrete and form the interaction mechanism, mandatory access RDBMS necessary to establish marking grade protection strategy and MAC for sensitive data limitations.
- The technology channel connected to the database, limiting unauthorized access DB Connection tools.
- The database accounts provided the effective host, identity, addressed, connecting tools under the premise, is allowed to connect.

b) Management strategy

To build the separation of separation of power system and RDBMS accounts settings segregation of duties.

To build internal staff and third party information security system management and monitoring system.

2) Threat monitoring and access control attribution in the event

Monitored contest include network traffic identification and risk threat arbitration over the right to operate marked level requests, illegal tempering with data integrity error etc. Technology stray and management strategy which include threat identification, risk, control, threat, analysis, blocking access to sensitive data over rights, emergency response mechanism and drill, to build mechanism for regular examination.

The construction of city government cloud computing based data security access control model has been portioned more than in year that, to achieve the data security objectives to improve the reliability of the system.

5. CONCLUSIONS

Cloud computing security problems are the most important issues in the cloud computing system. The cloud construction based on the analysis of existing security control for administrative and reliable applications, the MAS based data security access model and after the three stage control technologies and management strategies. According to this Mosel the construction of city government cloud platform running more than a year. It meet high reliable security requirements of government systems and provide reference of government cloud constructions.

REFRENCES

1. Hassan,Qusay(2011). "Demystifying Cloud Computing".*The Journal of Defense SoftwareEngineering* (CrossTalk)2011 (Jan/Feb): 16–21. Retrieved 11 December 2014.
2. ^ Jump up to:[a b c d e f g h] "The NIST Definition of Cloud Computing". National Institute of Standards and Technology. Retrieved24 July 2011.
3. Jump up^ "Know Why Cloud Computing Technology is the New Revolution". By Fonebell. Retrieved 8 January 2015.
4. ^ Jump up to:[a b] "What is Cloud Computing?". *Amazon Web Services*. 2013-03-19. Retrieved 2013-03-20.
5. Jump up^ "Baburajan, Rajani, "The Rising Cloud Storage Market Opportunity Strengthens Vendors," infoTECH, August 24, 2011". It.tmcnet.com. 2011-08-24. Retrieved 2011-12-02.
6. Jump up^ Oestreich, Ken, (2010-11-15). "Converged Infrastructure".*CTO Forum*. Thectoforum.com. Retrieved 2011-12-02.
7. Jump up^ "Where's The Rub: Cloud Computing's Hidden Costs". 2014-02-27. Retrieved 2014-07-14.
8. Jump up^ "Cloud Computing: Clash of the clouds". *The Economist*. 2009-10-15. Retrieved 2009-11-03.
9. Jump up^ "Gartner Says Cloud Computing Will Be As Influential As E-business". Gartner. Retrieved 2010-08-22.
10. Jump up^ Gruman, Galen (2008-04-07). "What cloud computing really means". *InfoWorld*. Retrieved 2009-06-02.