Volume 8, No. 5, May – June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Control Management in Cloud Computing Architecture using Security and Reliability Matrix

Arun Kumar
Department of information Technology
Babasaheb Bhimrao Ambedkar University
Lucknow India

Raj Shree
Department of information Technology
Babasaheb Bhimrao Ambedkar University
Lucknow India

Abstract:In this article, we are going to present a paper on Control Management in Cloud Computing Architecture using Security and Reliability Matrix. Cloud computing is basically is a type of internet based computing. It provides shared approach among computer systems processing resources and data to devices. Cloud Computing Security Control matrix proposed in this article to improve the security and reliability relationship. Here in this article, the security challenges are described in detail. In cloud computing, the security issues fall down in many two categories, the firstcategory the issues faced by cloud providers and second are their customers. Mainly the security challenge comes down from the cloud service providers and their customer experiences faced during the operability of this service. After the review of security challenges, we focused on security controls. In this article, we are discussed many types of controls behind a cloud security architecture. The extensive use of controls in cloud security addresses the security management. The need for cloud computing controls and security to provide safeguards any weakness in the computer system or a device that reduces the possibility of the effect of an attack.

Keywords:cloud computing; security matrix; reliability matrix; security control

I. INTRODUCTION

The NIST definition of cloud computing "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources(e.g. networks server, storage, application, and services) that can be rapidly provisioned and released with minimal management effort or services provider interaction" Cloud computing is the platform which stores some data applications and infrastructure. Cloud computing provides services to many users for data storing in cloud storage without thehelp of any extraordinary hardware. Cloud computing is the broad technology to groom our infrastructure building and concepts [1].Cloud computing is the easiest platform to perform many operations like document creation, information sharing, data storing and updating. Cloud computing used by the several users so security is the important factor to protect the data on thecloud. We are facing many security challenges to secure to data. Security should be robust and consistent. This paper presents a review of the security challenges in the context of cloud computing [2]. There are three major aspects where we have to focus on challenges.

- The first aspect is thetransmission of client's data to the cloud server.
- Transmission of cloud server data to the client's machine.
- Cloud is aremote server but it is not owned by theclient.

Cloud computing is implemented from distributed grid computing. The cloud computing perspective categorized into two different perspectives –

1. To rent the panel in cloud
2. To rent any specified service in the cloud.

The first perspective deals with the hardware and software usage on the cloud, the second perspective deals with only software usage.

The cloud computing world deals with the security challenges when it is faced several activities on the cloud. In cloud computing, security concern is a broad issue to discuss the problem of usage. This paper is aconcern with the review to identify the security challenges and control that is deployed in cloud-basedcomputing.

II. SECURITY CHALLENGES AND ITS SOLUTION

1. Security challenges

Cloud computing is a broad platform where the users can access, share, manipulate the file. The security should be enabled in the cloud computing. Withoutsecurity, the user canlose the control from their files[3]. The security may be incorporated within three layers of cloud computing [4][5]. There is a lot of security challenges that are given below –

a) Loss of regulation- the first security challenges loss of regulation or governance. When be deploy the public cloud customer loss the control to the cloud provider over a large number of problems that can affect security. The commitment between the customer and provider don't offer to resolve the problems that appear in the cloud challenges.
b) Responsibility darkness - The responsibility may be split between the user and provider the responsibility term used over an aspect of security. For defacing the file system the responsibility should be allocated clearly between user and customer. The responsibility of each party may be varying according to thecloud model.
c) Authorization and authentication- The third most appropriate challenge of cloud computing is authorization and authentication. On cloud

computing, there is a lot of user and cloud providers working together. The sensitive information may be stored in the cloud by the user. The information should be access, shared and manipulated by the authorized user. Authentication term used to authenticate the activity of user over a cloud computing.

d) Failure of isolation- In public cloud computing, there are several users access the same file at the same time or the user can use the shared resources over a cloud. The risk contains a mechanism of cloud computing for separating the usage of storage, routing, and memory.

e) Legal issues- In thecurrent scenario, the industry and businesses expand their achievements and activities like investments, certification, demonstration etc. Sometimes the cloud customer investments may be lost their certifications if thecloud provider doesn't provide the evidence own compliance both the relevant information. Sometimes cloud provider does not permit audits.

f) Handling of security phenomenon- There is a lot of security breaches on a cloud, these detections are not incorporated in thenegotiation of cloud computing agreement. So we can say that handling of security phenomenon and incidence is the challenge to increase the efficiency of safe access over a cloud.

g) Management of interface of vulnerability- Some time the interface may be incorporated with the vulnerability because the interface possesses by the traditional cloud providers. The interface allows the users to access the larger sets of resources it possesses a high risk to communicate with the applications.

h) Protection of application- The security challenge of cloud computing is theprotection of application. The protection of application from the hackers or attackers is thetoughest work. The system is never 100% secure. So we can say that the protection of application over a cloud is the biggest challenge. Sometimes the access control and protection (security) areto break by the attackers over the network.

i) Protection of data- Data protection is one of the most security challenges of cloud computing because the sensitive information or data may be used over the cloud. This data is enough to misuse to phishing, high jacking, fraud, and others.

j) Business failure of the cloud providers- Such type of failures may be rendered data and applications essential to the users business unavailable over an extended period of time.

k) Service unavailability- This can be caused by hardware, software or communication network failure.

l) Incomplete data deletion- When the customer terminates the contract with the service provider, the provider may not delete the customer's data. This incomplete delete data may be used in future for theillegal purpose [6].

2. Solution

a) In a public cloud deployment, the user should follow the regulation of the cloud computing agreement that is signed by the customer and provider.

b) The responsibility should be split into the parts according to the customers and providers with respect to cloud computing model.

c) In public cloud computing deployment, it ensures that the user of shared resources is identically authorized by the entities and parties.

d) In public cloud deployment, the provider must be ensured that sharing of among resources should be mutual handling by the interface.

e) The user should following the procedure of agreement and policies incorporated by the providers over the cloud.

f) When the user a developer detects the incident, it should be mention is thenegotiation of cloud service agreement.

g) The interface should be combined with the remote access and web browser application. The interface may be deal with the vulnerabilities via an authorization.

h) The application should be copyrighted with the authorized organization because the application may be revealed from the server for the purpose of misuse this application.

i) The data should be protected by the encryption technique like password, acombination of text, encrypts words.

j) The business should be incorporated into the agreement when the business failure occur the data should be deleting or protect by the authorized governance.

k) The service should be incorporated with recovery and backed up data. When the service is unavailable the recovery technique of data is working on the instead of.

l) When the termination of the user to access the specific type of service the provider should destroy or delete the whole data of the past customer. The governance should take care of each and every cloud provider under the surveillance[7].

III. PROPOSED SYSTEM

The proposed system ensures that the security threat is negligible to the user usage. It provides the powerful security control matrix that consists the relationship between the security and reliability. The Security matrix contains the entire element or attributes of security and reliability matrix contain all the elements of reliability that are represented here.

It will help to prevent from the security threat. The possible security threat is given below that can be resolved by the security control matrix.

- Broken Authentication
- Data breach
- Temper interface and API
- Account Hack
- Malicious Intruder
- Data loss
- Service abusing by attack(DDoS, Phishing, etc.)
- Shared Resources Misuse

A. Security matrix

Confidently	Access Limit	Integrity
Authorization	Correctness	Availability
Authentication	Non Repudiation	Persistent

0.11	0.13	0.12
0.10	0.08	0.09
0.15	0.04	0.16

B. Reliability Matrix

Accessibility	Scalability	Accuracy
Maintainability	Efficiency	Agility
Compatibility	Affordability	Configurability

0.14	0.17	0.03
0.15	0.06	0.13
0.18	0.05	0.07

C. Security Elements Probability:

Let assume expected value of security =1

Access Limit probability	= 0.13
Integrity probability	= 0.12
Authorization probability	= 0.10
Correctness probability	= 0.08
Availability probability	= 0.09
Authentication probability	= 0.15
Non Repudiation probability	= 0.04
Persistent probability	= 0.16
Actual probability of security	= 0.98

D. Reliability Elements Probability:-

Similarly, assume expected value of reliability =1

Accessibility probability	= 0.14
Scalability probability	=0.17
Accuracy probability	=0.03
Maintainability probability	=0.15
Efficiency probability	=0.06
Agility probability	=0.13
Compatibility probability	=0.18
Affordability probability	=0.05
Configurability probability	=0.07
Actual probability of Reliability	= 0.98

Security Control Matrix = Security Matrix * Reliability Matrix

E. Security Control Matrix:-

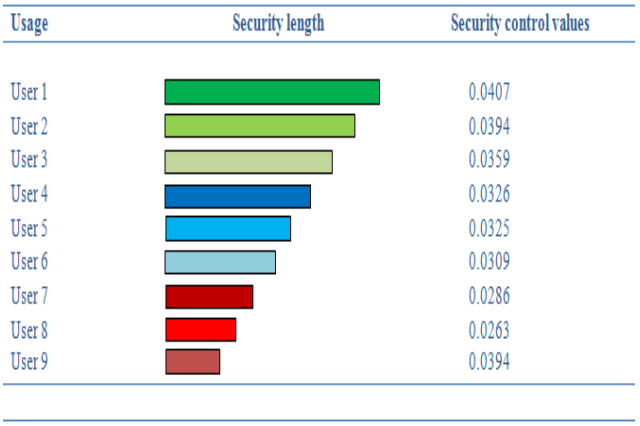
0.0407	0.0325	0.0286
0.0309	0.0263	0.03394
0.03326	0.0359	0.0109

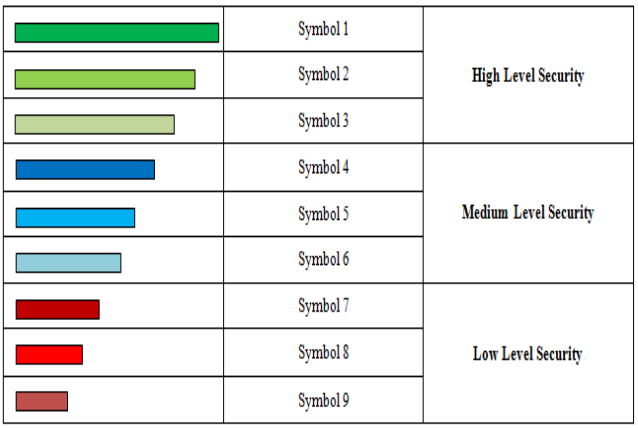
F. Usage of security control matrix:-

The usage of security control matrix defines the user security length over the cloud server. These are values taken from the combination matrix of security and reliability matrix. The resultant matrix is called security control matrix. This matrix includes all the elements of security and reliability in a balancing way.

The security control matrix will help in identifying the user security length that is taken from the user's own provided security standard. For example, when a user does login over the cloud application, a user provides security length at the time of registration in the form of user's password length. The following table helps to understand the functionality of the proposed system.

Colors of symbol 1, symbol 2, and symbol 3 indicate the High level of user's security, symbol 4, symbol 5, symbol 6 indicate the Medium level and symbol 7,symbol 8, symbol 9 indicate the low-level security





IV. CONCLUSION

In this paper, the cloud computing security control is proposed to increase the efficiency of cloud computing. This research describes the security and reliability matrix which contain the few types of elements. These elements will help to identify the balancing capability of the security control matrix. The security control matrix completes the objective of this paper. The objective of security control matrix is to secure the cloud computing with the reliability. After all, this paper opens the various path to improve the security of cloud computing. In future, these security control matrix elements will enhance the lots of functionality to the cloud computing users. This article shows that a relationship between the security matrix element and reliability matrix .the relationship of security and reliability will most appropriate matrix for future usage of cloud computing.

V. REFERENCES

[1] John W. Rittinghouse and James F.Ransome" Cloud Computing, implementation, management and security", Auerbach Publication,by CRC Press, August 17, 2009.

[2] Mehrdad Mahdavi Boroujerdi and Soheil Nazem, "Cloud Computing: Changing Cogitation about Computing",World Academy of Science, Engineering and Technology,International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:3, No:10, 2009.

[3] Brodkin, Jon, "Gartner:Seven Cloud-Computing SecurityRisks", Published by Network World, 2008.

[4] Florin Ogigau-Neamtiu, "Cloud Computing Security Issues", Vol 3, Issue 2(5)/2012, Journal ofDefense Resources Management , 2012.

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

[6] Dahbur, Kamal, Bassil Mohammad, and Ahmad Bisher Tarakji, "A survey of risks, threats, and vulnerabilities in cloud computing",Published in ACM Digital Library, 2011.

[7] Amar Gondaliya,"Security in Cloud Computing", Information Technology, Hasmukh Goswami College of Engineering, Ahmedabad, in Technical Paper Contest, 2011.