International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

A study on Security Issues Associated with Public Clouds in Cloud Computing

[1]Sandeepraja Batchu, [2]J.N. Chaitanya, [3]Sai sagar.N, [4]Eswar Patnala,

[1,3,4]Dept of IT, GIT, GITAM University, [2] Department of CSE, Sanketika Vidyaparishad Engineering College

Abstract

An important issue in cloud computing is security, and it plays a major role in the cloud computing. Normally in private cloud computing there will be extremely strong password authentication, so, there will be less number of threats will be attacked to the private cloud when compared public clouds. So, in this paper we discuss about the security issues that provide security to the data in the public clouds, suppose there is a private cloud that belongs to a community and it want to change it to the public or hybrid clouds. For this migration process many transformations are required like change in the infrastructure, change in the bandwidth etc. But most important that should be provided is security to the data that present in the cloud.

1. Introduction

The one of the computing resources that delivers the services over the network is the cloud computing. The Name itself represents that it appears like a cloud shaped and it consists of complex infrastructure for satisfying the enterprise that belongs to the cloud. Mainly cloud computing used for computations and to provide services to the users and for the software applications.

Cloud computing shares characteristics with

- Autonomic computing — Computer systems capable of self-management [4] [11].
- Client–server model — Client–server computing refers broadly to any distributed application that distinguishes between service providers (servers) and service requesters (clients)[4][12].
- Mainframe computer — Powerful computers used mainly by large organizations for critical applications, typically bulk data processing such as census, industry and consumer statistics, police and secret intelligence services, enterprise resource planning, and financial transaction processing[4][1].
- Utility computing — The "packaging of computing resources, such as computation and storage, as a metered service similar to a traditional public utility, such as electricity[4][2][3].
- Peer-to-peer — Distributed architecture without the need for central coordination, with participants being at the same time both suppliers and consumers of resources (in contrast to the traditional client–server model).
- Cloud gaming - Also known as on-demand gaming, this is a way of delivering games to computers. The gaming data will be stored in the provider's server, so that gaming will be independent of client computers used to play the game [4].

2. Service models for providing security to the public cloud computing

2.1 Infrastructure as a service (IaaS)

It is one of the most important service model for providing security to the public cloud computing. And it provides computers, machines which are used for maintaining the clouds and other resources for maintain the cloud with security.

IaaS clouds often offer additional resources such as images in a virtual-machine image-library, raw (block) and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles[13].IaaS providers keep the all data in the data centre's and supply those resources, when users are requested. The Users can access the supplied resources through different modes like local area network, wide area network or through Internet [5].

2.2 Software as a service (SaaS)

It is second type of service model for providing security to the public cloud computing. In this model, the providers that maintaining the cloud will install the software and the clients that belong to that particular cloud provide access to the users of that cloud. So, this type of service provides more comfort because the users of cloud can access the software application without installing in their own computer because a cloud client provides access to the cloud user. So there will be a less concern on maintaining it [6][14][25].

2.3 Network as a service (SaaS)

It is third type of service model for providing security to the public cloud computing by providing authentication to the network. The basic network for the cloud computing is the Internet, as internet is the collection of large networks by maintain all those networks we achieve security.

A category of cloud services where the capability provided to the cloud service user is to use network/transport connectivity services and/or inter-cloud network connectivity services. NaaS involves the optimization of resource allocations by considering network and computing resources as a unified whole [7][15].

2.4 Platform as a service (PaaS)

It is one of the most important service model in cloud for providing effective services to the cloud users, In this cloud providers provide a computing platform for accessing their applications, so, user develop their programs and execute in the execution environment provided by the cloud providers. In this the resources that are existing with cloud users such as computers storage resources are automatically match with the application of particular computing plotform.so that they no need to accommodate the resources manually.

3. Security issues associated with the public cloud

The issues that are raised when dealing with the public clouds are divided into types, they are mainly faced by two communities they are cloud providers and cloud users. Mainly Issues associated with the cloud providers are whether the Infrastructure is secure or not and the data that belongs to the customers are secure are not, these are some security issues associated with the cloud Providers, whereas the security issues that are associated with the cloud users are, they think whether the cloud providers take necessary security measures while developing application that is provided for their accessibility [8][16].

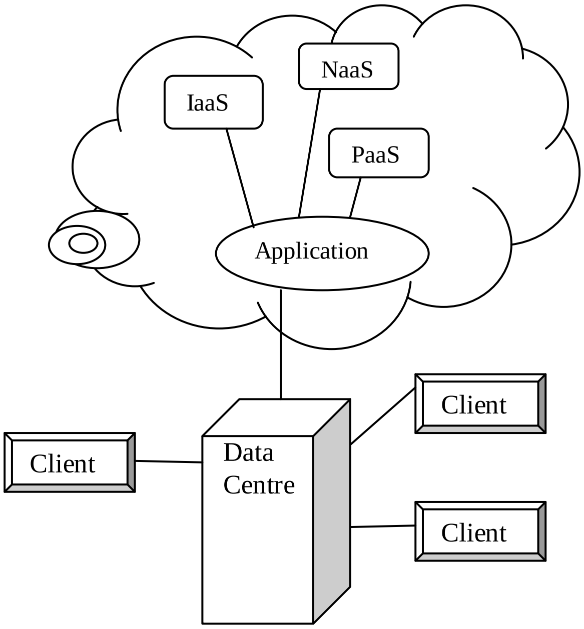

Figure 1. Service models in Public cloud computing

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 [8][17][18][19].

3.1 Common Public Cloud Architeture

The common Public clouds Architecture consists of cloud components like cloud Infrastructure, cloud storage, clouds services and cloud platform. Each cloud component has their own significance in providing services to the cloud architecture, combination of all these forms a complete cloud structure.

Figure 1 represents a complete Cloud Architecture, which contains cloud Platform, cloud Services, cloud Infrastructure and Cloud storage.

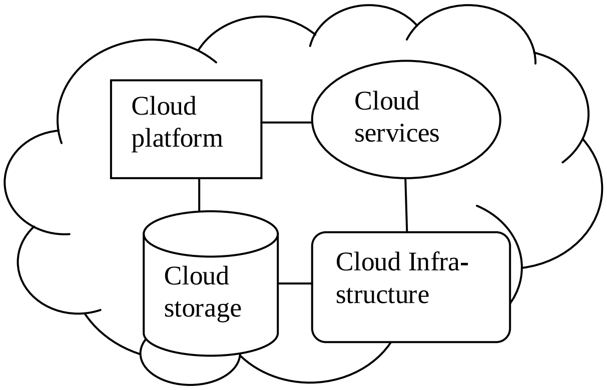

Figure 2. Public cloud Architecture

4. Security controls for providing security to the public cloud

The complete public cloud architecture works efficiently only when it is provided by necessary security controls [22][23][24].

There are some security controls which are used for the security management in the cloud security architecture

The following are security controls used for security management they are: Deterrent controls, preventative control, corrective control, Detective control [9][20][21]

4.1 Deterrent Controls

It is a most important security control for the security management in the public cloud security architecture, mostly it provides the warning message to the cloud user and it will not remove the threat that is occurred to the system. And this type of control is placed where we rise the warning compulsorily.

4.2 Preventative controls

It is one of important security control used to defend from the attack, for such defending it increases the strength of the system by upgrading it. By using this type of controls Damage to the system can be reduced and if there any attacks preventative controls keep away the system from the attack. it does not take any action on the effected data

4.3 Corrective controls

It is another most important security control, till now we see two types of security controls both of them did not take any action on the data affected by threat. Now the corrective control is the only tool which is used reduce the attack.

4.4 Detective control

It is one of the most efficient security controls; because it is used detect the attacks that are occurring in future. And after detecting it send messages to both deterrent controls and preventative controls. so, both these controls now become alert and starts their process.

5. Security structure

In order to provide efficient security to the public cloud the following structure may lead to the better results. Figure3 gives an idea how to secure a public cloud by taking all the above information into consideration in this. Initially we have to keep the customer identity safe from attackers and then we have keep safe, the information and the data that belongs to an enterprise, and then we have to design the applications by including all security controls. And then we have to maintain efficient servers and Infrastructures for proper communication [10].

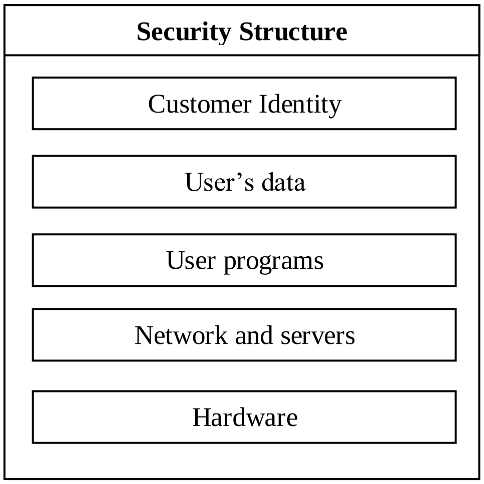

Figure 3. Security Structure of Public cloud computing

6. RSA algorithm for providing data security to in clouds computing

6.1 RSA Algorithm

It is one of the examples of the Asymmetric cryptosystem. It includes three processes they are

- Key generation
- Encryption
- Decryption

Key generation:

Select two large primes p & q such that (∃) $p \neq q$

Find $n= p \times q$ where n is used as public and private keys for modulus

Then compute $Ø (n) = (p-1) \times (q-1)$

Select 'e' Such that (∃) $1 < e < Ø (n)$ and e & Ø (n) are co-primes

And find $d = e^{-1} \bmod Ø (n)$

Public key = (e, n)

Private Key =d or (d, n)

Encryption:

Encryption is the process of converting original plain text (data) into cipher text (data). User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme [26].

Let M be the plain Text, C is the cipher text

$M < n$

$C = M^{e} \bmod n$

This cipher text or encrypted data is now stored with the Cloud service provider.

Decryption:

Decryption is the process of converting the cipher text (data) to the original plain text (data). The cloud user requests the Cloud service provider for the data [26]. Cloud service provider verity's the authenticity of the user and gives the encrypted data i.e., C.

Let M be the Plain text, C is the cipher text, and d be the private key component

$M = C^{d} \bmod n$

Once m is obtained, the user can get back the original data by reversing the padding scheme.

7. Experimental results

Now, let us consider some sample data in order to implement the algorithm

7.1 Key generation

Select two large prime numbers 17 & 11 where p=17 and q=11

Then calculate $n= p \times q = 17 \times 11 = 187$

And compute $Ø (n) = (17- 1) \times (11-1)$

$= 16 \times 10 = 160$

Select 'e' such that $1 < e < Ø (n)$ and e & Ø(n) are co-primes, here we choose e = 7.

$d = e^{-1} \bmod 160$

Or $d.\ e =1 \bmod 160$

$d.7=1 \bmod 160$

Hence d= 23 so the private and public keys of above example are public key (7, 187) and private key (23, 187). This private key is kept secret and known to only the users.

Let the message be equal to 88, now we should encrypt and decrypt this message

7.2 Encryption

The Public-Key (7, 187) is given by the Cloud service provider to the user who wishes to store the data. Data is encrypted now by the Cloud service provider by using the corresponding Public -Key which is shared by both the Cloud service provider and the user.

$C = 88^{7} \bmod 187 = 11$

. This encrypted data i.e., cipher text is now stored by the Cloud service provider [26].

7.3 Decryption

When the user requests for the data, Cloud service provider will authenticate the user and delivers the encrypted data (If the user is valid)[26]. The cloud user then decrypts the data by computing,

$M= 11^{23} \bmod 187 = 88$

Once the m value is obtained, user will get back the original data.

8. Conclusion

The above all data gives us the information how to protect the data that is residing in the public cloud. In order to protect the data that is residing in the public cloud's ,the above mentioned service model plays a major role, after creating the cloud using the service model then we should control and maintain the cloud. For this maintaining we use different type of security controls, these controls warn us, if there are any attacks. And the Security Structure gives the Brief idea what should be keep safe from the attackers.

References

[1] "Sun CTO: Cloud computing is like the mainframe". Itknowledgeexchange.techtarget.com. 2009-03-11. Retrieved 2010-08-22

[2] "It's probable that you've misunderstood 'Cloud Computing' until now". TechPluto. Retrieved 2010-09-14

[3] Danielson, Krissi (2008-03-26). "Distinguishing Cloud Computing from Utility Computing". Ebizq.net. Retrieved 2010-08-22.

[4] http://en.wikipedia.org/wiki/Cloud_computing

[5] http://en.wikipedia.org/wiki/Infrastructure_as_a_service#Infrastructure_as_a_service_.28IaaS.29

[6] http://en.wikipedia.org/wiki/Infrastructure_as_a_service#Infrastructure_as_a_service_.28IaaS.29

[7] http://en.wikipedia.org/wiki/Infrastructure_as_a_service#Infrastructure_as_a_service_.28IaaS.29

[8] http://en.wikipedia.org/wiki/Cloud_computing_security#References

[9] http://en.wikipedia.org/wiki/Cloud_computing_security#References

[10] ftp://ftp.software.ibm.com/common/ssi/sa/wh/n/tiw14045usen/TIW14045USEN_HR.PDF

[11] ^ "What's In A Name? Utility vs. Cloud vs Grid". Datacenterknowledge.com. Retrieved 2010-08-22

[12] "Distributed Application Architecture". Sun Microsystem. Retrieved 2009-06-16.

[13] Amies, Alex; Sluiman, Harm; Tong, Qiang Guo; Liu, Guo Ning (July 2012). "Infrastructure as a Service Cloud Concepts". Developing and Hosting Applications on the Cloud. IBM Press. ISBN 978-0-13-306684-5.

[14] Hamdaqa, Mohammad. A Reference Model for Developing Cloud Applications.

[15] "Cloud computing in Telecommunications". Ericsson. Retrieved 16 December 2012.

[16] "Swamp Computing a.k.a. Cloud Computing". Web Security Journal. 2009-12-28. Retrieved 2010-01-25.

[17] Winkler, Vic. "Cloud Computing: Virtual Cloud Security Concerns". Technet Magazine, Microsoft. Retrieved 12 February 2012.

[18] Hickey, Kathleen. "Dark Cloud: Study finds security risks in virtualization". Government Security News. Retrieved 12 February 2012.

[19] Winkler, Vic (2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics. Waltham, MA USA: Elsevier. pp. 59. ISBN Securing the Cloud Cloud Computer Security Techniques and Tactics.

[20] Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 2010. 179-80. Print.

[21] Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 2010. 179-80. Print.

[22] http://eprints.covenantuniversity.edu.ng/912/1/vol2no10_11.pdf

[23] http://www.ijater.com/Files/IJATER_05_01.pdf

[24] http://www.ijsi.org/ch/reader/create_pdf.aspx?file_no=i68&flag=1&journal_id=ijsi

[25] http://www.ijarcsse.com/docs/papers/10_Octoer2012/Volume_2_issue_10_October2012/V2I10-0044.pdf

[26] http://www.ijrcct.org/index.php/ojs/article/download/53/40