International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 02, February-2015

An Analysis of Security Issues and Solutions for Cloud Computing

Aakanksha Singh
Department of Computer Science
Rajasthan Technical University
Udaipur, Rajasthan, India

***Abstract*— Cloud Computing provides the capability to use computing and storage resources on a metered basis and reduce the investments in an organizations computing infrastructure. Cloud computing has been on the rise for many years but the threats to this technology are now more tangible than ever. It must first overcome a series of potential threats, beyond just cyber crime, if the industry is to be legitimized by the concerned citizen. Most of the business people are not well aware about the security issues and the risks concerned with cloud computing. It seems to be a huge barrier to the adoption of cloud services. The information regarding how to manage data security within a cloud, data privacy in the cloud, cloud security standards, the regulatory and compliance implications of migrating to a cloud model, etc. should be well understood before adopting the cloud service and solutions. This paper presents an understanding of this complex scenario and clarifies all these issues by identifying and classifying the main security concerns and solutions in cloud computing and provides comprehensive guidance to the cloud computing users on how to navigate the field of cloud computing to achieve the maximum return on cloud investments without compromising information security.**

Keywords*— *Cloud computing; data privacy; security; service model; solutions;

I. INTRODUCTION

Cloud Computing is generally defined as an IT model or computing environment composed of IT components which commonly consists of hardware, software, network and services [1].

The cloud computing model is most commonly composed of six essential characteristics, three service models and four deployment models. The six essential characteristics are as follows:

i. Resource pooling
ii. On-demand self-service
iii. Ubiquitous network access
iv. Measured service
v. Location independence
vi. Rapid elasticity

The three service models are as follows:

a) Software as a Service (SaaS) [2] - It uses provider's applications over a network.
b) Platform as a Service (PaaS) [3] - Used for deploying customer-created applications to a cloud.
c) Infrastructure as a Service (IaaS) [4] - Used for storage, network capacity, rent processing, and other fundamental computing resources.

The deployment models can be either internally or externally implemented. There are commonly four different types of deployment models which are summarized in the NIST [7], [8] and are defined as follows:

1) Public cloud - Sold to the mega-scale, public infrastructure.
2) Private cloud - Enterprise leased or owned.
3) Hybrid cloud - Composition of two or more clouds.
4) Community cloud - Shared infrastructure for specific community [9].

This paper presents security problems encountered in cloud computing, and has a research on many technical solutions for cloud security problems.

The rest of this paper is organized as follows. Section II proposes the scope of cloud computing security, gives an overview on cloud security industry, and discusses and lists the various security threats of cloud computing both on the customers and operators. Section III discusses many security technical solutions to overcome the challenges from cloud security etc. Then section IV, a conclusion of the cloud computing security threats and solutions.

II. CLOUD COMPUTING SECURITY CHALLENGES

Cloud computing infrastructure and environments are very simple that companies can very simply access the best-of-breed business applications by simply tapping into the cloud. It is also possible to share and optimize their infrastructure resources at very low costs. Even though it depicts the simplicity of cloud computing technology, it actually questions the security of the cloud environment. Most of the business people are not well aware about the security issues and the risks concerned with cloud computing. It seems to be a huge barrier to the adoption of cloud services. The information regarding how to manage data security within a cloud, data privacy in the cloud, cloud security standards, the regulatory & compliance implications of migrating to a cloud model, etc should be well understood by the cloud computing users before adopting the cloud service and solutions.

According to Nathan Eddy in the article named "Security a Rising Concern for Cloud-Based Application Usage" a survey was conducted which indicated that unsafe password management continues to be a challenge, as is the application usage which is not sanctioned by the company [10].

Here is the list of various security threats found in cloud computing:-

I. Network Availability:
The value of cloud computing in a particular environment can only be realized when your network connectivity and bandwidth meet the minimum requirement which are:
According to the need of the customer the cloud should be available, i.e. every time the customer asks for it, the customer should be provided with his requirement [1].

II. Cloud Provider Viability:
As the cloud providers are relatively new to the business, the viability and commitment of the provider has raised many questions. When a provider requires tenants to use proprietary interfaces, this concern deepens, thus leading to tenant lock-in.

III. Security Incidents:
All the users and tenants need to be appropriately informed by the provider when a particular security incident occurs. For responding to audit or assessment findings users or tenants may require support of the provider. Also, a provider may not offer sufficient support to users or tenants for resolving investigations.

IV. Loss of Physical Control:
Since users or tenants lose most of the physical control over their applications and data, this results in a range of concerns:

a. Privacy and Data:
In regards with community or public clouds, data may not remain in the same system and hence raising multiple legal concerns.

b. Control over Data:
Data belonging to a organization or user may get comingled in various different ways with data belonging to others.

V. Legal and Regulatory Compliance:
It may be unrealistic or difficult to utilize public clouds, if the data you need to process is subject to legal restrictions or regulatory compliance. Due to many technical and nontechnical factors including the current stage of cloud knowledge, it is very challenging to address the needs of regulated markets and achieving certifications for building and certifying clouds as is expected by the providers. As the best practices for cloud computing encompasses greater scope, this concern should largely become a historical one [1].

VI. Data Breaches:
Data breaches are one of the top threats to cloud computing. Virtually any person can access all the computer systems connected by the Internet, this ultimately results in exposing service providers of cloud computing to the threat of skilled hackers with malicious intentions. As the number of national (and international, as we have witnessed with China) underground hacking communities continues to grow, and hence more and more breaches are expected.

VII. Account Hijacking:
Another potentially serious threat is hijacking of accounts at cloud computing companies. Remote access of cloud data via mobile devices or remote computers is usually possible for authorized company personnel. "When employees are accessing sensitive information via remote platforms that don't necessarily have the security mechanisms in place that would otherwise exist at a workstation computer, the potential for account hijacking, or data hijacking, increases" notes from Texas based Microsoft Dynamics Partner, Tom Caper.

VIII. Insecure application programming interfaces (APIs):
Another threat to cloud computing is Insecure application programming interfaces (APIs). Security of the interfaces which offer ways for programs to communicate with each other is not always completely guaranteed. Granting people with malicious intentions access to sensitive information passing through the communication channel are the loopholes in security.

IX. Data Handling:
A risk to the data being handled is always posed by sharing of technology and resources among different organizations. Sometimes at cloud computing firms servers are configured to work with data from few clients. The system when adds data from a client with different requirements, there are number of things that can go wrong [11].

X. Data streaming security:
Data is streamed through the internet in a cloud environment. Data can be said to be safe and secure if it travels through secure "https" channels. However, the packets can be accessed when data streams over open lines, even though encrypted. Additionally, the chances of errors can lead to illegal access or data corruption by eavesdroppers since data in the cloud is accessed frequently.

XI. *IAAS, SAAS and PAAS each with its own set of issues:*
Platform as a service (PaaS), software as a service (Saas) and infrastructure as a service (IaaS) are three different pathways in cloud computing as discussed earlier. Each of the pathway has its own vulnerabilities that are not fully resolved. For instance, the same software is deployed as software as a service which is used in desktop and network environments and secure coding that will plug the loopholes and guard against penetration has yet to be developed by the developers.

XII. Service Level agreements:
Service level agreements are different for every cloud service provider which are aligned to fit in with their method of operation. In terms of security and safety, these SLAs may not perfectly match client expectations. There are plenty of unresolved and continuous questions such as who shares logical and physical resources and about assessments and audits [12].

Whether or not a cloud provider might surreptitiously exploit sensitive data for its own gain and the continued availability of the cloud users data over long periods of time is also a major concern for the cloud users[9].

III. CLOUD COMPUTING SECURITY SOLUTIONS

The cloud must be able to gain the trust of the public, as there is a little doubt that the cloud is the way the future for computing. Those in charge of local installations can do their part by ensuring that their cloud implementations are as secure as possible.

Here is the list of key strategies that could be implemented to secure the data in the cloud:

A. Recognize and Allocate Value to Properties:
Assets might be featuring antivirus apps, customer relationship management (CRM) or data, accounting; comprising personal customer details; or infrastructure like hosted web servers and OS.

B. Examine Your Responsibilities:
Among the largest cloud protection issues is the jeopardy of breaches causing theft or loss of sensitive exclusive information. If the details leaked are proprietary to your firm, obligation is not an issue. Still you should understand where obligation lies if client or patient details goes missing out.

C. Study Compliance Necessities:
In few markets finance and healthcare are instances industrial regulations or government establish criteria for how digital information is managed, featuring stating the level of protection in place. You could not even be allowed to set up antivirus, or there could be limitation, like the data need to be kept within the borders of your own nation.

D. Conclude Your Risk Tolerance:
These preliminary actions all play into this undoubtedly somewhat imprecise, but crucial, following step. The essential factor to consider is the expense of making certain safety, whether in the cloud or at your own workplaces.

E. Password security:
The essential component when it comes to security in a cloud installation is the password. A wreak havoc in a cloud installation could be created unfortunately, as many people are being reckless with the passwords. One broken password can break the trust, as the cloud relies on trust [11].

F. Use Complex Passwords:
All network tools, from NAS drives to routers to printers, and so on must be set up with complex passwords. That implies as a minimum eight characters, with combined case letters, symbols and letters and no dictionary words or appropriate names.

G. Consider going beyond passwords:
Using a two-level authentication technique could be a possibility. A number of different technologies could be used to accomplish this, and each of them offer some distinct advantage. It should be noted, however, test it thoroughly to ensure that users will be able to understand it, before deciding to use one of these options.

H. Encryption:
It is often said that any server can be broken as some security holes are unavoidable. It can never be completely known that a particular server is secure, while this point is debatable. Encryption can give users confidence that their data will be secure, and it will limit the damage that can be done from a break-in.

I. Log everything:
Getting work done and accessing information gets simpler for end users by cloud installations. However, there are certain complexities that are unavoidable on the servers. In addition, even experts only have a few years of experience and the cloud paradigm is still relatively young. Because of this, when trying to analyze problems it can be easy to become confused.

J. Do not forget the firewall:
An effective firewall is still the best frontline solution for the prevention of unauthorized access as opposed to as in recent years new methods of securing networks have become popular. Remote access is very necessary, for running a successful cloud implementation. By taking extra steps to ensure that the firewall is only allowing as much access as necessary, it may be possible to fend off malicious attackers [11].

K. Inquire about Safety and Integrity Certifications:
One means small companies could short-circuit unpaid attentiveness on companies' protection controls is to inquire different certifications they could have, or seek reference of them at the manufactures website. By considering just those manufactures with recorded, verifiably sound security techniques might remove few of the necessity to research deeper.

L. Disable Remote Management:
Virtually all routers have a remote management tool, which permits you log in to see or edit network configurations from the Web. To decrease the danger of unapproved outsider accessibility to your network, you must disable remote management hence administrative jobs can simply be carried within the network.

M. Create Security Controls into the Agreement:
The manufacturer might not be keen to discuss anything, or might not want to expand flexibility to small businesses. At least, cloud computing users should cautiously learn the agreement language as it associates with security controls.

N. Use WPA2:
You perhaps already understand that protecting your Wi-Fi network with WEP encryption is hardly much better than none in any way. However, the greatly remarkable WPA is amazingly at risk to breach, specifically when dictionary-based or/ and short passphrases are used.

O. Check out the Cloud Security Alliance Control file:
The CSA[5][17] has developed a comprehensive file detailing the due diligence it suggests businesses commence when considering relocating information and apps into the cloud.

These strategies are defined to support the three principal cloud security objectives, these objectives are, assuring the integrity, availability, and confidentiality of information resources.

IV. CONCLUSION

Although in the cloud the security and privacy services can be managed and fine-tuned by experienced groups that can potentially provide threat assessment services and efficient security management, the issues we have discussed here show that existing security and privacy solutions of cloud computing must be critically re-evaluated with regard to their appropriateness for clouds.

Please note that I am not trying to defame cloud service providers. In cloud computing many service providers are reliable and for cloud users data on cloud the cloud service providers will even give you a high security guarantee but the fact is that the online data is affected when an occurrence such as data failure occurs then cloud computing users will probably be put on a waiting queue and be forced to work according to their schedule like many other thousand cloud users, all these at the expense of business of cloud users. Then, it all zeros down to the basics of data security, if users data is that important, cloud or not, just make sure you have a backup as well as the local copy in your machine just in case.

Newer and more mature solutions as well as many enhancements in existing solutions are urgently needed to ensure that cloud computing benefits are fully realized as its adoption accelerates. Cloud computing is still in its infancy, and how the privacy and security landscape changes will impact its successful and widespread adoption.

REFERENCES

[1] J. R. Vic Winkler, "Securing the Cloud: Cloud Computing Security Techniques and Tactics", 2011.
[2] Amazon Elastic Compute Cloud web services, http://aws.amazon.com/ec2
[3] SalesForce Force.com Platform as a service, http://developer.force.com
[4] NetSuite SaaS portal, http://www.netsuite.com
[5] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," http:// www.cloudsecurityalliance.org/csaguide.pdf.
[6] D. Catteddu and G. Hogben, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," ENISA,2009;www.enisa.europa.eu/act/rm/files/deliverables/cloud -computing-risk assessment/at_download/fullReport.
[7] National Institute of Standards and Technology (NIST),http://www.nist.gov.
[8] NIST, Guidelines on Security and Privacy in Public Cloud Computing, http://csrc.nist.gov/publications. 2011
[9] Ronald L. Krutz, Russell Dean Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", July 2010.
[10] Nathan Eddy, "Security a Rising Concern for Cloud-Based Application Usage", http://www.eweek.com/security/secutiy-a-rising-concern-for-cloud-based-application-usage, January 2013.
[11] "Top Cloud Computing Security Threats and Responses", http://alegix.com/top-cloud-computing-security-threats-and-responses, September 2013.
[12] Pravin Anchan, "Top 5 Unresolved Security Issues in cloud Computing", http://www.cloudcomputingpath.com/top-5-unresolved-security-issues-in-cloud-computing/, January 2013.
[13] IDC, "Cloud computing 2010 – an IDC update," slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update, September 2009.
[14] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski,G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,"Above the clouds: A berkeley view of cloud computing," University of California at Berkeley, eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html, Tech. Rep. UCB/EECS-2009-28, February 2009.
[15] S. Shankland, "HP's Hurd dings cloud computing, IBM," CNET News,October 2009.
[16] D. Catteddu and G. Hogben, "Benefits, risks and recommendations for information security," European Network and Information Security Agency, enisa.europa.eu/act/rm/files/deliverables/cloud-computing-riskassessment, Tech. Rep., November 2009.
[17] CSA, "Security guidance for critical areas of focus in cloud computing,"Cloud Security Alliance, Tech. Rep., December 2009.
[18] T. Mather and S. Kumaraswamy, Cloud Security and privacy: An Enterprise Perspective on Risks and Compliance, 1st ed. O'Reilly Media, October 2009.
[19] Y. Chen, V. Paxson, and R. H. Katz, "What's new about cloud computing security?" University of California at Berkeley, eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html, Tech. Rep.UCB/EECS-2010-5, January 2010.
[20] Mell and T. Grance, "The nist definition of cloud computing," National Institute of Standards and Technology,www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, Tech. Rep. 15, July 2009.
[21] D. Hubbard, L. J. H. Jr, and M. Sutton, "Top threats to cloud computing," Cloud Security Alliance, Tech. Rep., March 2010. [Online]. Available: cloudsecurityalliance.org/research/projects/ top-threats-to-cloud-computing/
[22] Tompkins, "Security for cloud-based enterprise applications,"http://blog.dt.org/index.php/2009/02/security-for-cloud-basedenterprise-applications/, February 2009.