IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ICRAESIT - 2015

B V Raju Institute of Technology, Narsapur

Vol. 2, Special Issue 2, December 2015

SaaS Model Security Issues In Cloud Computing

G. Sudhakar[1], Dr. Ahrmed Abdul Moiz Qyser[2], Dr. S. Durga Bhavani[3]

Asst. Professor, SIT, JNTUH, Hyd India[1]

Professor, CSE Department, MJCET, Hyd, India[2]

Professor, SIT, JNTUH, Hyd India[3]

Abstract: Cloud computing has emerged as a popular Computing model, with numerous advantages both to end users and providers in the form of providing convenience and reliable services to the end user. In few years, acceptance of cloud computing from Small ,Medium Enterprises (SME's) to major enterprises is increasing, but businesses are now finding difficult with the number of issues related to security which are been addressed, when end users venture into the cloud. If one wishes to enable cloud-driven growth and innovation through security, one must have a clear framing on what is meant by cloud security. Cloud security has been notoriously hard to define in the general case. Security concerns grow up as more and more sensitive date is communicated in the internet and when placed in the cloud. Building trust in the providers also is a very major problem when we adapt Cloud computing. The biggest disaster for the Organizations is breaching in the security components of the cloud. The major concern in the SaaS Model is security to the Data hosted in the service provider's datacenters.

Key Words: SME's, Cloud Driven, security, SaaS, Service Provider.

I. INTRODUCTION

For any enterprise when migrate in to the cloud enterprises are worried much about the number of risks included in securing critical information like the protection of intellectual property, trade secrets, personally identifiable information that could fall into the wrong hands, so availability of information on the internet requires a considerable investment in security controls and monitoring of access to the contents. When it comes to SaaS Model cloud environment, the enterprise/ organizations may have very little or no visibility to storage and backup processes and has a little or no physical access to storage devices at the cloud provider. Moreover, because the data from multiple customers may be stored in a single repository, forensic inspection of the storage media and a proper understanding of the access and deletion will be a significant challenge [2]. According to [3] vulnerability "is a weakness in the security system" that could be exploited to cause harm. Like any other technology that uses the public internet for connectivity Cloud computing is just a vulnerable entity. The vulnerability includes eavesdropping, hacking, cracking, malicious attacks, denial-of-service attacks and outages.

Moreover when it comes to protecting of our cloud network, irrespective of the size of the Enterprise/Organization, big company, small company, are the startup company, most of the hackers still want your information and stealthily poke holes in your network wherever they can as everything (Computation, storage..Etc,) is done using Internet.

When it comes to SaaS Model, companies have become vital for anyone who is looking to deploy security for everything starting from simple documents to entire business. Sometimes "Security as a service" can be loosely described as a "software as a service" so many security tools doesn't require any on-premise hardware or software distribution. Unlike older security tools, like anti-virus software that needs to be installed on every single computer on your network, it's almost plug and play activity to get major security resources at your fingertips.

Security requires a holistic approach and so Cloud Security Alliance [21] and Gartner [20] have identified various security threats to cloud computing. [6] Classifies security threats in cloud based on the service delivery models of a cloud system. Among the security issues/vulnerabilities in each service delivery model, some are the responsibility of cloud providers while others are the responsibility of cloud customers. In case of SaaS model as the application specifications lies in with the Service provider, customer has a lot of concern about data security.

1. Security Characteristics of Cloud Computing.

Stakeholders:

Stakeholders plays a vital role in the cloud computing, where in this computing model there are different stakeholders involved: cloud provider (an entity that delivers infrastructures to the cloud customers), service provider (an entity that uses the cloud infrastructure to deliver applications/services to end users), and customer (an entity that uses services hosted on the cloud infrastructure). Each stakeholder has their own security management systems / processes, expectations (requirements) and capabilities (delivered) from/to other stakeholders.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ICRAESIT - 2015

B V Raju Institute of Technology, Narsapur

Vol. 2, Special Issue 2, December 2015

Control of Third-Party:
Neither the owner of the application nor the end user will have control on the data processing; an entity in between who is called a third party has the control. For the organizations that are into cloud computing, the biggest problem will be the reduced control, even after they are being tasked to bear increased responsibility for the confidentiality and compliance of computing practices in the organization. Third-Party Control is probably the prime cause of concern in the cloud. With the growing value of corporate information, his access can lead to a potential loss of intellectual property, trade secrets and the issue of a malicious insider who abuses access rights to tenant information.

Governance:
To make governance easier for the customers, cloud providers should make the management and maintenance of cloud services more and more transparent and easily auditable for the customers. This should include recording logs and complete control over administrative sessions affecting the part of the cloud infrastructure used by the customer. When requested by the customer it should be made accessible to the customer as in traditional IT outsourcing. Using cloud services most of the times require the customer to give up control over his IT infrastructure.

Cloud Providers control:
As providers are not aware of Hosted services architectures, they are not able to provide efficient and effective security controls. They are also faced with a lot of problems when it comes to changes in security requirements, because of having a variety of security controls deployed that needs an update. This activity further complicates the cloud providers' security administrators' tasks.

Multi tenancy:
Multi-tenancy is a feature unique to resource sharing in clouds. Essentially, it allows cloud providers to manage resource utilization more efficiently by partitioning a virtualized, shared infrastructure among various customers. All tenants share computational resources like storage, services, and applications. By multitenancy, clouds provide simultaneous and secure hosting of services for various customers utilizing the same cloud infrastructure resources. To reach the high scales of consumption desired, service providers have to ensure dynamic flexible delivery of service and isolation of user resources.

Scalability:
Scaling resources assigned to services based on the current users demand is essential property of cloud computing. Scaling up or scaling down of a tenant's resources gives the opportunity to other tenants to use the tenant's previously assigned resources.
Scaling is of two types i) Scaling out (Horizontal) which means increase in the number of shared resources like storage. ii) Scaling Up (Vertical) which means increasing the computation capacity of the resources like storage, and is done on demand by the end user.

Multi- in- Nature:
We have multi processing, virtual storage, multiple tenants to manage, and multiple applications running at same time in the cloud's 'virtual infrastructure' [1, 3] and is very complex and dynamic in nature. In addition to this, there is a huge amount of traffic flowing in and out of each physical server and/or a logical VM. Since, the virtual architecture of the cloud erases many of the physical boundaries that are traditionally used in defining, managing and protecting an organizations' IT assets within a traditional Data Center, it leads to a very complex virtual architecture which by itself needs to be protected from all threats caused by whether an insider or outsider.

2. SaaS model Security aspects:
Irrespective of size of organizations, and enterprises, one need to get security measures in place and act very fast, when it comes to protecting cloud network. All companies which are into cloud are suffering from the aspect of providing security to the cloud data in the SaaS Model, so providing security has become vital area for anyone who is looking to deploy security in to cloud. Security is needed in every phase starting from documents to all other phases of one's entire business. There are many software tools in the software market used for solving the SaaS model issues, which doesn't require any on-premise hardware or software distribution, unlike anti-virus software that needs to be installed on every single computer of one's network, SaaS security tools are almost plug and play and readily available. Most of the security services aren't the same as an on-premise firewall that watches the network from a physical appliance attached in your data center, but security tools promise to protect you from malware, help you keep track of who is signing into your network and monitor all other cloud applications. (E.g. Sales force, Google Docs, etc.) For the above kind of distribution model small businesses can benefit, because it doesn't require a big IT or security teams to get it up and running. Of course, we trust a lot on another company for your security, because in reality these security-focused third parties have more resources like spend money to focus on security than we do, so we need to depend on them.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ICRAESIT - 2015

B V Raju Institute of Technology, Narsapur

Vol. 2, Special Issue 2, December 2015

3. SaaS model Security issues:

Web Apps issue:
In SaaS the first issue is protecting the most used applications, like web app's. Securing web apps through cloud-only solutions form others is crucial, as we want to remain compliant free from users. Tools are needed to assess our Web apps and identify the holes and solve the issues. Tools are also needed to act as a firewall that virtually patches found issues and protect the web apps. Also need tools which always keep scanning the web apps for vulnerabilities and keep the existing date safe.

Information threat issue:
As in cloud computing SaaS model to avoid information loss, analyzing the threat information is necessary, so making sure that nothing enters in to our system by any vulnerable means can help in avoiding information loss. We need software tools that can analyze the threat information are expected to be placed in right place in the Structure.

Malware issue:
Malware has become a very big head ache for the cloud providers, as it is affecting the computation and communication process as well. So detecting and verifying the existing malware and fixing it will help the applications of the SaaS Model to run smoothly. So Software tools which can detect, verify and fix the existing malware is necessary for SaaS Model.

Web app Scan issue:
Always keep scanning the web app's for vulnerabilities while keeping the existing date safe is very important in SaaSmodel[21].

Firewall issue:
Providing a firewall (cloud specific) provide safety for websites from other harms[21].

Code Process Issue:
Detect current threat information while coding so that we void coding vulnerabilities for the web sites in the next go[21].

Pre-production issue:
A preproduction security issue before we launch the website is very important in SaaSModel[21].

Logic Issues:
Identification of logic issues once it is launched is also important in SaaSModel[21].

Updating issues:
We need a research arm in order to provide us the updated information on threats found outside our network[21].

Identity management issues:
Identity management (knowing who is where and why in the cloud network) plays a vital role in SaaS Model and is one of the most important parts about securing your network, which is simply knowing the where a bout's of the insider (employees, customers, partners) in the cloud network[21].

Login Issues:
Managing the logins across all of our applications as well as apps like Google Apps, Salesforce, Workday, Box, SAP, Oracle, and Office 365 is very important. Implementing policies across devices is curtail and single sign-on options is very important in SaaS Model.

Attack vector issues:
The hole (email pop outs which are the weakest link) in the cloud network where attackers can get in. sometimes email needs the cloud-only service tailored to both enterprises and small to medium sized businesses to protect the outgoing Data.

Persistent threat Issues:
Sometimes with the given flexibility of the cloud we need to monitor total network and specific, local networks as well. We also need to monitor all the traffic that comes in and goes out of your network just like a "check post in the cloud", but you don't have to filter all that traffic in from one central point[21].

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ICRAESIT - 2015

B V Raju Institute of Technology, Narsapur

Vol. 2, Special Issue 2, December 2015

Priced Data Issues:

In cloud computing everything is a service, so it is very important to protect the company's prized data, as we are just giving in the form of services and also should protect communication process[21].

File sharing Issues:

Sometimes we have to stop file sharing process from happening, because the file is accessed by unintended person. By setting user privileges for each person we share a document and tracking everyone who opens the file and looking at the data. When it is used by the unintended person, we should be able to pull back the documents, effectively "without sharing them[21].

4. CONCLUSION

Most security professionals think securing data in the cloud is harder than keeping on-premises systems safe, but they're preparing for a cloudy future regardless. In most of the conferences eminent professionals view cloud security as a bigger concern every year, according to a survey's by cloud data Protection Company's above 66% think the cloud is substantially more difficult to secure than on-premise options. "It's time to be proactive and put long-trusted security tools such as encryption and tokenization in place to make sure that no matter where your data is, it is protected." There are various powerful software tools available in the software market to purchase and secure the SaaS Model Applications[21].

REFERENCES

[1] Ramgovind, s. et ai, "The management of security in Cloud", Proceedings of lnformation Security for South Africa (lSSA), 2010 .
[2] Information Security Magazine, The three cloud computing risks to consider. Issue: June 2009. Retrieved from http://www.arma.org/press/ARMAnews/Infosecurity.pdf
[3] C. P. Pfleeger, S. L. Pfleeger, Security in Computing. Fourth Edition. Prentice Hall.
[4] SANS Institute, An Introduction to information system risk management http://www.sans.org/reading_room/whitepapers/auditing/an_ introduction_to_information_system_risk_management_1204?show= 1204.php &cat= auditing
[5] L. J. Zhang and Q. Zhou, CCOA: Cloud computing open architecture,2009 IEEE Int. Conf. on Web Services (ICWS'09), July 2009, pp. 607-616.
[6] S. Subashini, V. Kavitha, A survey on security issues in service delivery
[7] models of cloud computing, J. of Network and Computer Applications,
[8] vol. 34, no. 1, 2011, pp. 1-11.
[9] Hamlen, K. et ai, "Security issues for Cloud Computing", International
[10] Journal of Information Security and Privacy, Vol4 , Issue 2, April-June
[11] 2010.
[12] Srinivasamurthy, S., David Q. Liu, "Survey on Cloud Computing Security", Proceedings of 2nd IEEE International Conference on Cloud Computing Technology and Science, 2010
[13] D. Shin and G.-J. Ahn, Role-based privilege and trust management,Computer Systems Science & Eng. J., vol. 20, no. 6, 2005, pp. 401
[14] P.J. Bruening and B. C. Treacy, Cloud computing: privacy, securitychallenges, Bureau of Nat'l Affairs, 2009; www.hunton.com/files/tbl_s47Details/FileUpload265/2488/CloudComputing_Bruenig-Treacy.pdf.
[15] S. Dokras, et al., The role of security in trustworthy cloud computing. White paper, RSA, The Security Division of EMC
[16] J. Snyder, Six strategies for defense-in-depth: securing the network from the inside out. http://www.arubanetworks.com/pdf/technology/whitepapers/wp_Defense-in-depth.pdf
[17] B. Axel, and K. Lodewijks, Cloud security guidance: IBM recommendations for the implementation of cloud security, http://www.redbooks.ibm.com/redpapers/pdfs/redp 4614.pdf.
[18] IBM, IBM point of view: security and cloud computing, ftp://public.dhe.ibm.com/common/ssi/sa/wh/n/tiw14045usen/TIW14045USEN - HR.PDF.
[19] Amazon. Amazon EC2 SLA. http://aws.amazon.com/ec2-sla/
[20] D. K. Holstein, Stouffer, K., Trust but verify critical infrastructure cyber security sol.s, in HICSS 2010, pp. 1-8.
[21] R. Buyya, et al., Market-oriented cloud computing: vision, hype, and reality for delivering IT services as computing utilities, Future Generation Computer Sys, vol. 25, no. 6, June 2009, pp. 599.
[22] How to secure cloud computing. http:// searchsecurity.techtarget.com/ magOnline/0, sid14_gci1349550, 00.html.
[23] R. Chow, et al., Controlling data in the cloud: Outsourcing computation without outsourcing control. In ACM Workshop on Cloud Computing Security, 2009
[24] J. Brodkin, Gartner: Seven cloud-computing security risks. In: Infoworld2008 http:/ / www.infoworld.com/d/security-central/gartnersevencloudcomputing-Security-risks 53?page=0,1
[25] G. Zhao, et al., Deployment models: Towards eliminating security concerns from cloud computing. in: Int. Conf. on High Performance Computing and Simulation (HPCS), June 28 - July 2, 2010, Caen, France, pp. 189 – 195
[26] Cloud Security Alliance, Security guidance for critical areas of Focusin cloud computing, V2.1, 2009.