NCRISET-2017 e-ISSN: 2456-3463
International Journal of Innovations in Engineering and Science, Vol. 2, No.6, 2017
www.ijies.net

Security of Cloud Computing - An Emerging Technology

Ku. Ashwini G. Shende
Computer Science(MCA) Student,
Shivaji Science College, Dist. Nagpur
Email: Ashu.shende222@gmail.com

Mr. Sachin P. Dhande
Librarian, 2nd Shift Polytechnic
Tulsitramji Gaikwad-Patil College of Engg. & Tech. Nagpur, India
Email: librariansachin@gmail.com

Mr. Kamlesh S. Shende
Librarian,
G.H.Raisoni Inst. of Engg. & Tech., Nagpur, India
E-mail.:- kamlesh.shende@rediffmail.com

Abstract :

The term "Cloud Computing" has been mentioned for just under two year is relation to services or infrastructural resources. A person sitting in one part of the world may commit a cyber crime in one other part of the world. Conflict of laws in cyberspace has created unique law enforcement related problems as a given act or omission may be illegal in one country and may be legal in another. Cloud computing has been in news in India. The obvious benefit of cloud computing are very vigorously propagated by cloud computing vendors and India is seen as a huge market for cloud computing. The development of cloud computing services is speeding up the rate in which the organizations outsource their computational services or sell their idle computational resources. Even though migrating to the cloud remains a tempting trend from a financial perspective, there are several other aspects that must be taken into account by companies before they decide to do so. One of the most important aspect refers to security, while some cloud computing security issues are inherited from the solutions adopted to create such services, many new security questions that are particular to these solutions also arise, including those related to how the services are organized and which kind of data can be placed in the cloud. Aiming to give a better understanding of this complex scenario, in this article we identify and classify the main security concerns and solutions in cloud computing, giving an overview of the current status of security in this emerging technology. The research objective is to achieve a greater security which is not reveal lot of information to cloud service provider. Along with this it provided the better security.

Keywords—cloud computing, cloud computing security.

I. Introduction :

Several trends are opening up the era of cloud computing, which is an internet based development and use of computer technology. Security is considered a key requirement for cloud computing. This viewpoint is shared by many distinct groups, including academia research business decision makers and government organizations. The many similarities in these perspectives indicate a grave concern on crucial security and legal obstacles for cloud computing, including service availability, data confidentiality, provider lock-in and reputation fate sharing. These concerns have their origin not only on existing problems, directly inherited from the adopted technologies, but are also related to new issues derived from the composition of essential cloud computing features like scalability, resource sharing and virtualization. The distinction between these classes is more easily identifiable by analysing the definatation of the essential cloud computing characteristics proposed by the NIST definition of cloud computing, which also introduces the SPI model for services and deployment. Due to the ever growing interest in cloud computing, there is an explicit and constant effort to evaluate the current trends in security for such technology, considering both problems already identified and possible solutions. An authoritative reference in the area is the risk assessment developed by ENISA not only does it list risks and vulnerabilities, but it also offers a survey of related works and research recommendations. A similarly work is the security guidance provided by the Cloud Security Alliance (CSA), governance and compliance to virtualization and identity management. Both documents present a plethora of security concerns, best practices and recommendations regarding all types of services in NIST's SPL model, as well as possible problems related to cloud computing, encompassing from data privacy to infrastructural configuration. Albeit valuable, these studies do not focus on quantify the main security concerns and solutions associated to cloud computing, helping in the task of pinpointing the concerns that remain unanswered. Aiming to organize this information into a useful tool for comparing, relating and classifying already identified this information into a useful tool for comparing, relating and classifying already identified concerns and solutions as well as future ones, we also present a taxonomy proposal for cloud computing security. We focus on issues that are specific to cloud computing, without losing sight of important issues that also exist in other distributed systems. This article extends work presented in providing an enhanced review of the cloud computing security taxonomy previously presented, as well as a deeper analysis of the related work by discussing the main security frameworks currently available; in addition, we discuss further the security aspects related to virtualization in cloud competing, a fundamental yet still underserved field of research.

II. Cloud Computing Security (CSA)

CSA security guidance and top threats analysis the cloud competing that required further studies for being appropriately handled and, consequently, for enhancing technology acceptance and adoption. Emphasis is given to the distinction between services in the form of software , platform and infrastructure which are commonly used as the fundamental basis for cloud service classification. However, no other methods are standardized or even employed to organize cloud computing security aspects apart form cloud deployment models, service types or traditional security models. Aiming to concentrate and organize information related to cloud security and to facilitate future studies, in this section we identify the main problems in the area and group them into a model composed of seven categories, based on the aforementioned references. Namely, the categories are network security, interfaces, data security, virtualization, governance, compliance and legal issues. Each category includes several potential security problems, resulting in a classification with subdivisions that highlights the main issues identified in the base references.:

- **Security Challenges**

In spite of all the many advantages, due issues such as lack of standardization, there are unfortunately some drawbacks and security issues that can arise from using

cloud computing and SaaS services (Software-as-a-service). This paper describes some of the major security risks facing cloud providers and mentions several recognized by the Cloud Security Alliance (CSA). We focus on the following threats:

1. Cyber attacks and hacking of sensitive information.
2. Illegal local network access from cloud services.
3. Stolen information from cloud computing employees.
4. Attacks from other customers.
5. Adherence and compliance of providers to security standards.
6. Data loss.
7. Data Segregation from other customers.
8. Security culture among providers.
9. Evolving threats that may target clouds.
10. Privacy concerns.

SaaS undeniably provides savings and other advantages for end users but we now endeavor to address its risks and possible solutions to make it more secure for customers.

A) Network Security : Problems associated with networks communications and configurations regarding cloud computing infrastructures. The ideal network security solution is to have cloud services as an extension of customers' existing internal networks, adopting the same protection measures and security precautions that are locally implemented and allowing them to extend local strategies to any remote resource or process.

- Firewall
- Security configuration
- Transfer security

B) Interfaces : concentrates all issues related to user, administrative and programming interfaces for using and controlling clouds,

- API
- User interface
- Authentication

C) Data security : protection of data in terms of confidentiality, availability and integrity

- Redundancy
- Cryptography
- Disposal

D) Virtualization : isolation between VMs, hypervisor vulnerabilities and other problems associated to the use of virtualization technologies.

- Hypervisor Vulnerabilities
- Isolation
- Data Leakage
- VM identification
- Cross-VM attacks

E) Governance : Issues related to administrative and security controls in cloud computing solutions.

- Data Control
- Security Control
- Lock-in

F) Compliance :

- Service Level Agreement (SLA)
- Loss of service
- Audit
- Service Conformity

G) Legal Issues : Aspects related to judicial requirements and law, such as multiple data locations and privilege management.

- Data location
- E-Discovery
- Provider privilege
- Legislation

III. Commercially Available Cloud Services

A) Google: The core of Google's business is all in Cloud Computing. Services delivered over network connections include search, e-mail, online mapping, office productivity (including documents, spreadsheets, presentations, and databases), collaboration, social networking and voice, video, data services. Users can subscribe to these services for free or pay for increased levels of service and support.

B) Amazon: As the world's largest online retailer, the core of Amazon's business is ecommerce. While ecommerce itself can be considered Cloud Computing, Amazon has also been providing capabilities which give IT department's direct access to Amazon compute power. Key examples include S3(Simple Storage Services) and EC2. Any internet user can access storage in S3 and access stored objects from anywhere on the Internet. EC2 is the Elastic Compute Cloud, a virtual computing infrastructure able to run diverse applications ranging from web hosts to simulations or anywhere in between. This is all available for a very low cost per user.

C) Microsoft: Traditionally Microsoft's core business has been in device operating systems and device office automation software. Since the early days of the Internet Microsoft has also provided web hosting, online e-mail and many other cloud services. Microsoft now also provides office automation capabilities via a cloud ("Office Live") in an approach referred to as "Software Plus Services" vice "Software as a Service" to allow synchronous/asynchronous integration of online Cloud documents with their traditional offline desktop-resident versions.

D) Salesforce.com: The core mission of Salesforce.com has been in delivery of capabilities centered on customer relationship management. However, in pursuit of this core Salesforce.com has established themselves as thought leaders in the area of Software as a Service and is delivering an extensive suite of capabilities via the Internet. A key capability provided is the site Force.com, which enables external developers to create add-on applications that integrate into the main Salesforce.com application and are hosted on the infrastructure Salesforce.com.

E) VMware: Provides several technologies of critical importance to enabling cloud computing, and has also started offering its own cloud computing on demand capability called vCloud. This type of capability allows enterprises to leverage virtualized clouds inside their own IT infrastructure or hosted with external service

IV. Security Culture Among Providers:

In a survey conducted by the Phenom institute, many Cloud providers that participated felt that the customer was more responsible for security in the cloud than the provider. other findings include that Cloud Security Providers feel the main advantages they offer users are reduced costs and savings, that few of them (26%of participants in the USA) have full time cloud security personnel and many Cloud providers (over 65%) do not encrypt their customers data. while many of the participants do have features like firewalls and antivirus security risks like unauthorized customer logins are not as closely monitored by some Cloud providers. A few Cloud Security providers do claim to offer the highest level of security for their customers with about 10% stating that they offer Security as a Service in the Cloud. Security as a Service is the concept of outsourcing security needs to an outside party and is likely to see much growth in the cloud especially for users who feel unable to safeguard their networks to the highest level. Figure 3 shows the percentages of responsibility for ensuring the security of Cloud resources by Cloud providers.

V. Conclusion:

There is no dedicated legislation for cloud computing in India. In nutshell, Although cloud computing in India is growing in higher pace, but still not trusted. The basic reason for this condition is absence of dedicated legal framework for cloud computing in India, missing privacy law, absence of data protection laws in India and inadequate data security. There are various technological perspectives for cloud analytics and various cloud services that can be envisaged in future, as the development of cloud computing technology is still at an early stag

REFERENCES :

[1] CSA : Security Guidance of Critical Areas of Focuses in Cloud Computing. 2009. Tech. Rep., Cloud Security Alliance 16 Hubbard D, Jr LJH, Sutton M: Top Threats to Cloud Computing.
[2] http://www. Nist.gove/itl/cloud/upload/-def-v15.pdf technical report 15, national institute of standards and technology
[3] cloud computing security: an emerging technology, by Dr. Shipra Singam, proceeding national conference libraries and social responsibilities in the democratic world information deeksha for all.
[4] Janakiram MSV Cloud Computing Strategist; (2010), "Demystifying the Cloud An introduction to Cloud Computing", Version 1.0
[5] Tompkins D: Scurity for Cloud-based Enterprise Applications. http://blog.dt.org/index.php/2009/02/security-for-cloud-base-enterprise-applications/
[6] Gennovese s: Akamai introductes Cloud-Based Firewall2009. http://cloudcomputing.syscon.com/node/12190023
[7] http://www.csoonline.com/article/658121/cloudpassage-aims-to-ease-cloud-server-securitymanagement
[8] http://www.coloudcomputingtechnlogies.com
[9] Carlin, S. and K. Curran, "Cloud Computing Security," International Journal of Ambient Computing and Intelligence, Vol. 3, No. 1:14-19, 2011
[10] Gobjuka and K. Ahmat, WiNV: A Framework for Web-based Interactive Scalable Network Visualization,in Proc. IEEE INFOCOM Demo Session, 2010.