Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 87 (2016) 246 – 251

Procedia Computer Science

2016 International Conference on Computational Science

Security Issues In Service Model Of Cloud Computing Environment

B. Hari Krishna[a], Dr.S. Kiran[b], G. Murali[a,b,*], R. Pradeep Kumar Reddy [a,b,*]

[a]Ph.D Research Scholar, YSREC Of Yogi Vemana University, Proddatur, A.P ,India

[b]Assistant Professor, YSREC of YVU, Proddatur, A.P, India

[a,b,*]Assistant Professor& HOD CSE, JNTUAC of Engineering (Autonomous), Pulivendula, A.P, India

[a,b,*]Assistant Professor, YSREC of YVU, Proddatur, A.P ,India

Abstract

Cloud computing is becoming increasingly fashionable in distributed computing environment. Processing and Data storage use cloud environment is becoming a movement universal. Software as a Service (SaaS) has on many business applications as well as in our day to day life, we can simply say that this disruptive technology. Cloud computing can be seen since Internet-based computing, in which shared resources, software, and information are made available to devices on demand. It allows resources towards leveraged on per-use basis. It diminishes cost and complexity of service providers by means of assets and operational costs. It allows users to access applications tenuously. On behalf of user, this construct directs cloud service provider to feel software updates and cost of servers etc. For both, cloud providers and consumers; availability, integrity, authenticity, confidentiality, and privacy are important concern. Infrastructure as a Service (IaaS) serves as base layer for many other release models and Platform-as-a-Service (PaaS) clouds. Security of PaaS clouds is considered from multiple perspective including access control, service continuity and privacy while protecting together the service provider and the user. Security problems of PaaS clouds are explored and classified. In this paper we are going to some major security issues of current cloud computing environments.

Peer-review under responsibility of the Organizing Committee of ICRTCSE 2016

Keyword- cloud computing; deployment model; service level agreement; utility computing; privacy; platform as a service; software as a service; infrastructure as a service;

I. Introduction

In the progressively prevalent cloud computing, datacentres play an ultimate role as the major cloud infrastructure providers, for example Microsoft Azure, Amazon, and Google. Datacentres position for the utility computing service to software service providers who auxiliary provide the application service to end users over Internet. The later service has wide been termed “Software as a Service (SaaS)”, and the prior service has newly been called “Infrastructure as a Service (IaaS)”, everywhere the software service provider is also mentioned to as cloud service provider. To yield advantage of computing and storage assets providing by

* Corresponding author. Tel.:9014834561;E-mail address: *haribommala@gmail.com; rkirans125@gmail.com; muralig521@gmail.com; pradeepmadhavi@gmail.com.*

Peer-review under responsibility of the Organizing Committee of ICRTCSE 2016
doi:10.1016/j.procs.2016.05.156

cloud infrastructure providers, data owners outsource gradually data to the datacentres concluded cloud service providers, e.g., the online storage facility provider, which are not completely trusted by data owners. As a general data structure to define the relation between entities, the graph has been increasingly used to model complicated organisations and schema less data, such as the personal social network (the social graph), the relational data base, Considered for the protection of users' privacy, these sensitive data have to be encrypted before outsourcing to the cloud. Furthermore, nearly data are invented to be shared among trusted partners to all organizations. There have stayed revealed attacks on cloud computing providers and this paper discusses recommended steps to handle cloud security, issues to illuminate before adopting cloud computing, the need for a governance strategy and good governance technology, cloud computing strengths, faults, analyzes the profits and cloud computing information security management. This paper has discussed approximately of the services being provided.

II. Cloud Computing Architecture

There are several major cloud computing providers with Amazon, Salesforce, Google, Yahoo, Microsoft and others that are providing cloud computing services. Cloud computing providers provide a variety of services to the customers and these services include e-mails, storage, infrastructure-as-a-services, software-as-a-services etc.

The attractiveness of cloud computing is not only to large enterprises but also startups, entrepreneurs, medium companies and small companies would benefit greatly and they will have a opportunities and alternative that is not available to them in the past that would save them billions of dollars because with cloud computing they will have the choice to only rent the necessary computing power, communication capacity and storage space from a large cloud computing provider that has all of these assets connected towards the Internet. In practice, cloud service providers tend to offer services that can be grouped into three categories: infrastructure as a service, platform as a service, and software as a service. These categories group together the countless layers illustrated in Figure, with approximately overlap.

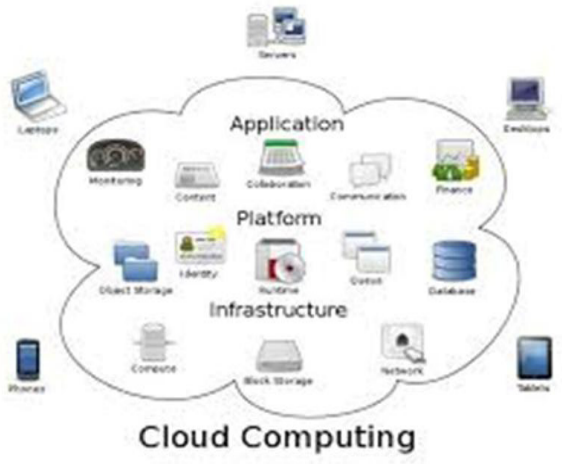

Fig 1. (a)

2.1. *Software as a Service (SaaS)*

If provide software services on demand. The use of single occurrence of the application runs on the cloud services and multiple end users or client organizations. The most usually known example of SaaS is salesforce.com, though many other examples have revive market, including the Google Apps offering of basic corporate services including email and word processing. Even though salesforce.com led the definition of cloud computing by a limited years, it now operates by leveraging its companion force.com, which can be

demarcated by way of a platform as a service.

2.2. *Platform as a service (PaaS)*

Platform as a service condenses a layer of software and make available it as a service that can be used to build higher level services. There are at least two perspectives on PaaS provisional on the perspective of the producer or consumer of the services:

• Someone producing PaaS potency produce a platform by participating an OS, middleware, application software, and even a development environment that is before provided to a customer as a service. For example, somebody developing a PaaS offering might base it on a set of Sun™ xVM hypervisor virtual machines that include a NetBeans™ integrated development environment, a Sun GlassFish™ Web stack and support for additional programming languages such as Perl or Ruby.

• Someone using PaaS would see an summarized service that is presented to them through an API. The customer interacts by the platform through the API, before the platform does what is necessary to manage and scale itself to provide a specified level of service. Virtual appliances can be hush-hush as instances of PaaS. A content switch appliance, for example, would have all of its component software unseen from the customer, and only an API or GUI for configuring and deploying the service provided to them. PaaS assistances can provide for every phase of software development and testing, or they can be specialized everywhere a particular area such as content management. Commercial examples of PaaS include the Google Apps Engine, which assists applications on Google's infrastructure. PaaS services such as these can provide a powerful origin on which to deploy applications, however they may be forced by the capabilities that the cloud provider indicates to convey.

2.3. *Infrastructure as a service (IaaS)*

Infrastructure as a service delivers basic storage and compute capabilities as consistent services over the network. Servers, storage systems, switches, routers, and other systems are united and made available to holder workloads that range from application components to high performance computing applications. Commercial samples of IaaS include Joyent, whose main product is a line of virtualized servers that afford a highly available on demand infrastructure.

III. Threats Now Cloud Computing

3.1 Threats

Cloud computing faces just as much security threats that are at present found in the existing computing platforms, networks, intranets, internets in enterprises. These threats, risk susceptibilities come in many forms.

The Cloud Security Alliance (Cloud Computing Alliance, 2010) did a research on the threats roughcast cloud computing and it identified the flowing major threats:

- Attacks by Other Customers
- Shared Technology Vulnerabilities
- Failures in Provider Security
- Availability and Reliability Issues
- Integrating Provider and Customer Security Systems
- Legal and Regulatory Issues
- Insecure Application Programming Interfaces
- Perimeter Security Model Broken
- Data Loss/Leakage
- Malicious Insiders
- Unknown Risk Profile
- Account, Traffic Hijacking & Service

IV. Cloud Computation Implementation Guidelines

4.1 Steps to Cloud Security

Edwards (2009) stated that, with the security risk and susceptibility in the enterprise cloud computing that are being exposed enterprises that want to ensue with cloud computing should, use the following steps to substantiate and understand cloud security providing by a cloud provider:

- Understand: the cloud by appreciating how the cloud's uniquely loose structure affects the security of data sent into it. This can be done by consuming an in-depth understanding of how cloud computing transmit and handles data.
- Demand Transparency: by constructing sure that the cloud provider can hoard detailed information on its security architecture and is agreeable to accept regular security audit. The regular security appraisal should be from an independent body or centralised agency.
- Reinforce Internal Security: by making sure that the cloud provider's internal security technologies and practices with firewalls and user access controls are very strong and can lattice very well through the cloud security measures.
- Contemplate the Legal Implications: by significant how the laws and regulations will affect what you lead into the cloud.
- Pay attention: by constantly observing any development or changes in the cloud technologies and practices that may impression your data's security.

4.2 Information Security Principles

A I C (Availability, Integrity, Confidentiality)

- Availability

Certify information is available when needed

- Integrity

Sanctuary information integrity

- Confidentiality

Prevent unauthorized disclosure

- Client Computing Devices

Integrity, Confidentiality, and availability.

4.3 Identify Assets & Principles

- Customer Data

Integrity, Confidentiality, and availability.

- Customer Applications

Confidentiality, integrity, and availability.

V. **Issues Of Security To Clarify Before Adopting Cloud Computing**

The world's important information technology, advisory company, research and has identified seven security apprehensions that an enterprise cloud computing user should discourse with cloud computing providers (Edwards, 2009) before approving.

- Regulatory Compliance: Create sure your provider is willing to submit to external Audits and security certifications.
- User Access. Ask providers for unambiguous information on the hiring and oversight of privileged administrators and the controls concluded their access to information. Major Companies should demand and enforce their own hiring principles for personnel that will operate their cloud computing environments.
- Data Segregation: Realize what is done to segregate your data, and probe for proof that encryption schemes are deployed and are effective.
- Data location: Enterprises should necessitate that the cloud computing provider store and process data

in specific jurisdictions and should follow the privacy rules of those Jurisdictions.

- Disaster Recovery. Ask the provider for a contractual commitment to sustenance specific types of investigations, such as the research involved in the discovery phase of litigation, and verify that the provider has successfully supported such activities in the past. Deprived of evidence, don't assume that it can do so.
- Disaster Recovery Verification. Know what will happen if adversity strikes by asking whether your provider will be capable of utterly restore your data and service, and find out how long it will take.
- Long-term Viability: Ask forthcoming providers how you would get your data back if they were to fail or be assimilated, and find out if the data would be in a arrangement that you could easily import into a replacement application.

VI. Solution Of Security Issues

6.1. Discovery Key Cloud Provider

First solution is of verdict the right cloud provider. Different vendors have dissimilar cloud IT security and data management. A cloud vendor should be well established, have experience, principles and regulation. So there is not some chance of cloud vendor closing.

6.2. Clear Contract

Contract with cloud vendor should be clear. So if cloud vendor closes earlier contract, enterprise can claim.

6.3. Recovery Facilities

Cloud vendors ought to provide very good recovery facilities. So, if data are fragmented or lost because of certain issues, they can be recovered and continuity of data can be managed.

6.4. Enhanced Enterprise Infrastructure

Enterprise requisite have infrastructure which enables installation and configuration of hardware components such as firewalls, routers, software, servers and proxy servers such as operating system, thin clients, etc. Similarly ought to have infrastructure which prevents from cyber-attacks.

6.5. Use of Data Encryption for security purpose

Developers should develop the solicitation which provides encrypted data for the security. So further security from enterprise is not crucial and all security burdens are placed on cloud vendor. IT leaders must define approach and key security components to know where the data encryption is needed.

6. 6. Organise chart apropos data flow

There should be a chart apropos the tide of data. So the IT managers can have idea where the data is on behalf of all the times, where it is being stored and where it is being united. There shou*ld* be total exploration of data.

VII. Conclusion

Cloud computing has a probable for cost savings to the enterprises but the security risk are also gigantic. Enterprise considering into cloud computing technology as a tactic to cut down on cost and increase profitability should seriously analyser the security risk of cloud computing. The asset of cloud computing in information risk management is the facility to manage risk more effectively from a integrate point. Although Cloud computing can be seen as a new marvel which is set to reform the way we use the Internet, there is much to be thoughtful about. There are many new technologies emerging at an express rate, each with technological developments and with the potential of making human's lives at ease. However, one must be very careful to appreciate the security risks and challenges stood in exploiting these technologies. Cloud computing is no exception. In this paper Security issues in Service Model of Cloud computing Environment which are currently handled in the Cloud computing are highlighted. Cloud computing has the possible to become a favourite in stimulating a secure, virtual and economically possible IT solution in the forthcoming. We tried to solve many issues. In our future work, we will include the different cryptographic-algorithms by solving the security in cloud computing.

Acknowledgment

The authors would like to acknowledge with thanks the financial assistance from JNTUCEP of AP.

References

[1] Buyya R, Chee Shin Y, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems; 2009; 25(6):599–616.

[2] Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A View of Cloud Computing. Communications of the ACM ; 2010; 53(4):50–58.

[3] Subashini S, Kavitha V. A survey on security i issues in service delivery models of cloud computing. Journal of Network and

mputer Applications; 2011; 4(1):1–11.
[4]Takabi H, Joshi J B D, Ahn G. Security a and privacy challenges in cloud computing environments. IEEE Security & Privacy;2010;8(6) :24–31.
[5] Sangroya A, Kumar S, Dhok J, Varma V. Towards analyzing data security risks in cloud computing environments. Communications in Computer and Information Science; 2010; 54 :255–265.
[6]Boss G, Malladi P, Quan D, Legre gni L, Hall H. Cloud computing, 2009. h ttp://www.ibm.com/developerswork/websphere /zones/hipods/ library.html.
[7]Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing (Draft). NIST. 2011. http://www.production scale.com/home/2011/8/7/the-nist-definition-of-cloud-computingdraft.html#axz z1X0xKZRuf.
[8] Cloud Security Alliance. Security gui dance for critical areas of focus in cloud computing(v2.1). Decemeber, 2009.
[9] Pearson, S. and Azzedine Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing" in 2010 IEEE Second International Conference Cloud Computing Technology and Science (CloudCom),Nov 30-Dec 3,2010, page(s): 693-702.
[10] Jinzhu Kong, "A Practical Approach to Improve the Data Privacy of Virtual Machines" 2010 IEEE 10th International Conference on Computer and Information Technology (CIT), June 29 -July 1 ,2010, pp. 936-941.
[11] Esteves, R.M. and Chunming Rong, "Social Impact of Privacy in Cloud Computing" in 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), N ov. 30-Dec. 3 ,2010, pp. 593-596
[12] Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online Michael Miller
[13] Cloud Application Architectures: Building Applications and Infrastructure in the Cloud (Theory in Practice) by George Reese.
[14] Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice) by Tim Mathe
[15] Dot Cloud: The 21st Century Business Platform Built on Cloud Computing Peter Fingar
[16] Ramanujam, S., Gupta, A., Khan, L., & Seida, S(2009). R2D: Extracting relational structure from RDF stores. In Proceedings of the ACM/IEEE International Conference on Web Intelligence, Milan, Italy
[17] Smith, S., & Weingart, S. (1999). Building a high performance, programmable secure coprocessor [Special Issue on Computer Network Security]Computer Networks, 31, 831–860. doi:10.1016 S1389-1286(98)00019-X
[18] Teswanich, W., & Chittayasothorn, S. (2007). ATransformation of RDF Documents and Schemascto Relational Databases. IEEE Pacific Rim Conferences on Communications, Computers, and Signal Processing, 38-41.