IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 05-10
www.iosrjournals.org

Cloud Computing Security Disputes, Defies and Elucidations

Venugopal S. Narsingoju[1], Dr. S. B. Kishor[2]
[1]*venu.narsingoju@gmail.com,Research Scholar,Gondwana University, Gadchiroli, India*
[2]*s.b.kishor.spc@gmail.com, Head Dept. of Computer Science,Sardar Patel Mahavidyalaya, Chandrapur,India*

Abstract: *Cloud computing is an up going technology now a days where shared resources, software's and information are provided to computers and devices. Security in respect to cloud computing is an important and critical aspect, and has numerous issues and problem related to it. Since cloud computing uses distributed resources in open environment, thus it is important to provide the security and trust to share the data for developing cloud computing applications. Cloud service provider and the cloud service consumer should make sure that the cloud is safe enough from all the external threats so that the malicious user can penetrate the cloud by impersonating a legitimate user, thus infecting the entire cloud and affects many customers who are sharing the infected clouds. In this paper we show the desired implementation of cloud computing in an enterprise requires proper planning and understanding of emerging risks, threats and possible countermeasures. It also shows how we secure the cloud security, privacy and reliability when a third party is processing sensitive data, we also discussed security risks and concerns in cloud computing and progressive steps that an enterprise can take to reduce security risks and protect their resources. We also emphasis on strengths, weakness and applicable area in information risk management.*

Keywords- *Cloud Computing, Risk Utility Commuting, Virtual Machine Layer*

I. Introduction

In the increasingly prevalent cloud computing, datacenters play a fundamental role as the major cloud infrastructure providers, such as Amazon, Google, and Microsoft Azure. Datacenters provide the utility computing services to software service providers who further provide the application service to end users through Internet. Many companies developing and offering cloud computing products and services but have not properly consider the implications of processing, storing and accessing data in a shared and virtualized environment. To take advantage of computing and storage resources provided by cloud infrastructure providers, data owners outsource more and more data to the datacenters through cloud services providers, e.g., the online storage service provider, which are not fully trusted by data owners. Cloud computing is sharing of resource on a larger scale which is cost effective and location independent. Resources on the cloud can be used by the client and deployed by the vendor such as amazon, google etc. It also shared necessary software's and on demand tools for various IT Industries. Benefits of clod Computing are enormous. The most important one is that customers don't need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money. Cloud is not only for multinational companies but it's also being used by small and medium enterprises [7].As a general data structure to describe the relation between entities, the graph has been increasingly used to model complicated structures and schema less data, such as the personal social network (the social graph), the relational data base, For the protection of users' privacy, these sensitive data have to be encrypted before outsourcing to the cloud. Moreover, some data are supposed to be shared among trusted partners to all organizations. There have been revealed attacks on cloud computing providers and this paper discusses recommended steps to handle cloud security, issues to clarify before adopting cloud computing, the need for a governance strategy and good governance technology, cloud computing strengths, weaknesses, analyzes the benefits and cloud computing information security management. This paper has discussed some of the services being provided

II. Cloud Computing Architecture

There are several major cloud computing providers including Amazon, Google, Salesforce, Yahoo, Microsoft and others that are providing cloud computing services (Figure1. shows current cloud providers).Cloud computing providers provide a variety of services to the customers and these services include e-mails, storage, software-as-a-services, infrastructure-as-a-services etc.

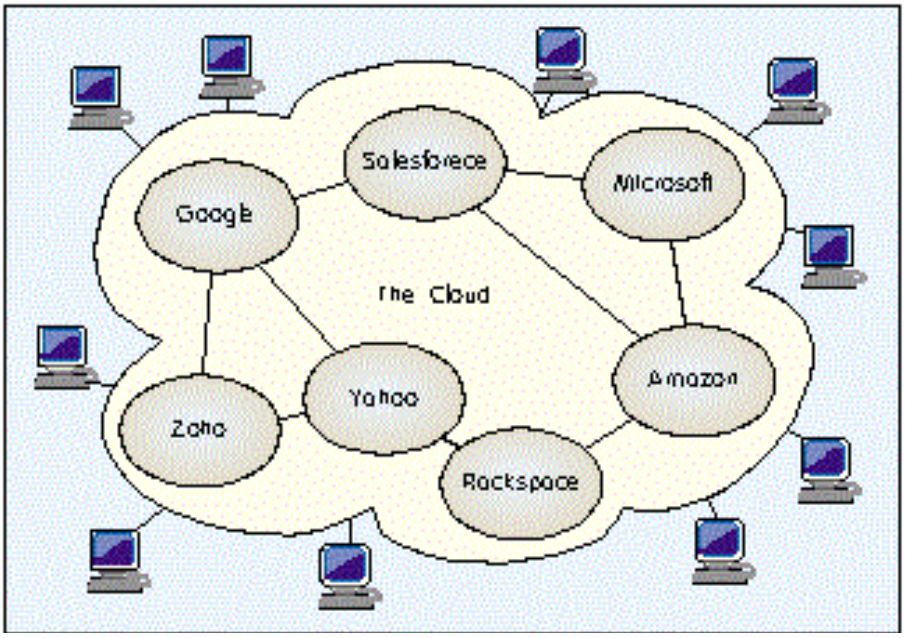

Fig1: Cloud Computing Architecture

The desirability of cloud computing is not only to large enterprises but also entrepreneurs, startups, medium companies and small companies would benefit greatly and they will have a new alternative and opportunities that is not available to them in the past that would save them millions of dollars because with cloud computing they will have the choice to only rent the necessary computing power, storage space and communication capacity from a large cloud computing provider that has all of these assets connected to the Internet. In practice, cloud service providers tend to offer services that can be grouped into three categories: software as a service, platform as a service, and infrastructure as a service. These categories group together the various layers illustrated in Figure2, with some overlap.

2.1 Software as a Service (SaaS)

If provide software services on demand. The use of single instance of the application runs on the cloud services and multiple end users or client organizations. The most widely known example of SaaS is salesforce.com, though many other examples have come to market, including the Google Apps offering of basic business services including email and word processing. Although salesforce.com preceded the definition of cloud computing by a few years, it now operates by leveraging its companion force.com, which can be defined as a platform as a service. Figure 2 Cloud Services and Application

2.2 Platform as a service (PaaS)

Platform as a service encapsulates a layer of software and provides it as a service that can be used to build higher-level services. There are at least two perspectives on PaaS depending on the perspective of the producer or consumer of the services: • Someone producing PaaS might produce a platform by integrating an OS, middleware, application software, and even a development environment that is then provided to a customer as a service. For example, someone 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 encapsulated service that is presented to them through an API. The customer interacts with the platform through the API, and the platform does what is necessary to manage and scale itself to provide a given level of service. Virtual appliances can be classified as instances of PaaS. A content switch appliance, for example, would have all of its component software hidden from the customer, and only an API or GUI for configuring and deploying the service provided to them. PaaS offerings can provide for every phase of software development and testing, or they can be specialized around a particular area such as content management. Commercial examples of PaaS include the Google Apps Engine, which serves applications on Google's infrastructure. PaaS services such as these can provide a powerful basis on which to deploy applications, however they may be constrained by the capabilities that the cloud provider chooses to deliver.

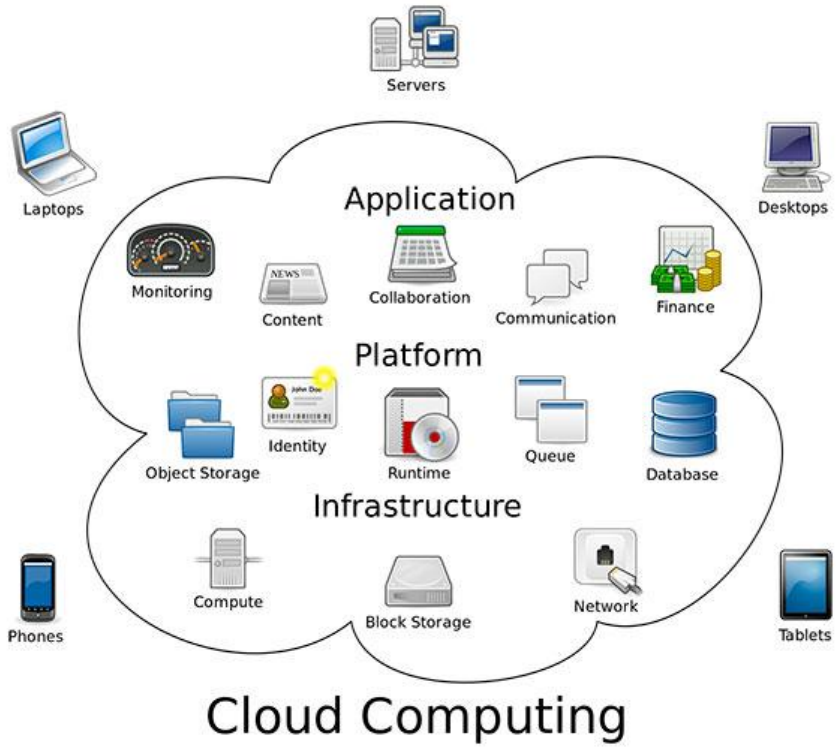

Fig2: Cloud Computing Services

2.3 Infrastructure as a service (IaaS)

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

III. Extortions In Cloud Computing

Cloud computing faces just as much security threats that are currently found in the existing computing platforms, networks, intranets, internets in enterprises. These threats, risk vulnerabilities come in various forms. The Cloud Security Alliance (Cloud Computing Alliance, 2010) did a research on the threats facing cloud computing and it identified the flowing major threats:

- ✓ Disasters in Provider Security
- ✓ Outbreaks by Other Customers
- ✓ Availability and Reliability Issues
- ✓ Legal and Regulatory Issues
- ✓ Perimeter Security Model Broken
- ✓ Integrating Provider and Customer Security Systems
- ✓ Abuse and Despicable Use of Cloud Computing
- ✓ Insecure Application Programming Interfaces
- ✓ Malevolent Insiders
- ✓ Shared Technology Vulnerabilities
- ✓ Data Loss/Leakage
- ✓ Account, Service & Traffic Hijacking
- ✓ Unknown Risk Profile

IV. Cloud Computation Implementation Guidelines 4.1

4.1 Levels to Cloud Security

Edwards (2009) stated that, with the security risk and vulnerability in the enterprise cloud computing that are being discovered enterprises that want to proceed with cloud computing should, use the following steps to verify and understand cloud security provided by a cloud provider:

- Understand the cloud by realizing how the cloud's uniquely loose structure affects the security of data sent into it. This can be done by having an in-depth understanding of how cloud computing transmit and handles data.
- Demand Transparency by making sure that the cloud provider can supply detailed information on its security architecture and is willing to accept regular security audit. The regular security audit should be from an independent body or federal agency.
- Reinforce Internal Security by making sure that the cloud provider's internal security technologies and practices including firewalls and user access controls are very strong and can mesh very well with the cloud security measures.
- Consider the Legal Implications by knowing how the laws and regulations will affect what you send into the cloud.
- Pay attention by constantly monitoring any development or changes in the cloud technologies and practices that may impact your data's security.

4.2 Information SecurityIdeologies

C I A (Confidentiality, Integrity, Availability)

- Confidentiality- Prevent unauthorized disclosure
- Integrity- Preserve information integrity
- Availability- Ensure information is available when needed

4.3 Categorize Assets &Ideologies

- Customer Data- Confidentiality, integrity, and availability.
- Customer Applications- Confidentiality, integrity, and availability.
- Client Computing Devices- Confidentiality, integrity, and availability.

V. Disputes To Illuminate Before Implementing Cloud Computing

The world's leading information technology research and advisory company, has identified seven security concerns that an enterprise cloud computing user should address with cloud computing providers (Edwards, 2009) before adopting:

- User Admittance- Ask providers for specific information on the hiring and oversight of privileged administrators and the controls over their access to information. Major Companies should demand and enforce their own hiring criteria for personnel that will operatetheir cloud computing environments.
- DirectingAcquiescence- Make sure your provider is willing to submit to external Audits and security certifications.
- Data position- Enterprises should require that the cloud computing provider store and process data in specific jurisdictions and should obey the privacy rules of those Jurisdictions.
- Data Isolation- Find out what is done to isolate your data, and ask for proof that encryption schemes are deployed and are effective.
- CatastropheSalvage Verification- Know what will happen if disaster strikes by asking whether your provider will be able to completely restore your data and service, and find out how long it will take.
- CatastropheSalvage- Ask the provider for a contractual commitment to support specific types of investigations, such as the research involved in the discovery phase of a lawsuit, and verify that the provider has successfully supported such activities in the past. Without evidence, don't assume that it can do so.
- Longstanding Viability- Ask prospective providers how you would get your data back if they were to fail or be acquired, and find out if the data would be in a format that you could easily import into a replacement application.

VI. Illumination Of Security Disputes

6.1 Discover Key Cloud Provider

First solution is of finding the right cloud provider. Different vendors have different cloud IT security and data management. A cloud vendor should be well established, have experience, standards and regulation. So there is not any chance of cloud vendor closing.

6.2 Strong Contract

With cloud vendor should be clear. So if cloud vendor closes before contract, enterprise can claim.

6.3 Regaining Facilities

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

6.4 Improved Enterprise Infrastructure Enterprise

Must have infrastructure which facilitates installation and configuration of hardware components such as firewalls, routers, servers, proxy servers and software such as operating system, thin clients, etc. Also should have infrastructure which prevents from cyber-attacks.

6.5 Usage of Data Encryption for security determination

Developers should develop the application which provides encrypted data for the security. So additional security from enterprise is not required and all security burdens are placed on cloud vendor. IT leaders must define strategy and key security elements to know where the data encryption is needed.

6.6 Formulate chart regarding data flow

There should be a chart regarding the flow of data. So the IT managers can have idea where the data is for all the times, where it is being stored and where it is being shared. There should be total analysis of data.

VII. Conclusion

Cloud computing is a mishmash of several key technologies that have grown and matured over the years. Cloud computing has a probable for cost savings to the enterprises but the security hazard are also massive. Enterprise looking into cloud computing technology as a way to cut down on cost and riseeffectiveness should utterly analyze the security risk of cloud computing. The asset of cloud computing in information risk management is the ability to manage risk more effectively from a integrate point. Although Cloud computing can be seen as a new spectacle which is set to develop the way we use the Internet, there is much to be guarded about. There are many new technologies emerging at anexpress rate, each with technological progresses and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and tasks posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a leader in promoting a secure, virtualand economically viable IT solution in the future. We tried to solve many issues. In our future work, we will include the developing of testing of data flow and security in cloud computing.

VIII. Future Work

We are considering in the cloud security management problem. Our objective is to block the hole ascend in the security management processes of the cloud clients and the cloud benefactors from adopting the cloud model. To be able to resolve such problem we need to capture different shareholders security necessities from different perceptions and different levels of details map security necessities to the cloud architecture, security patterns and security solicitation mechanisms and Deliver feedback about the current security status to the cloud providers and consumers. Weadvise to adopt an adaptive model-based method in attacking the cloud security management problem. Models will help in the problem intellection and the seizing of security requirements of different stakeholders at different levels of details. Addictiveness will help in delivering an integrated, energetic and enforceable cloud security model. The response loop will measure the security status to help cultivating the current cloud security model and keeping cloud consumers attentive with their assets' security status.

REFERENCES

Books

[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 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 nd 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, Legregni L, Hall H. Cloud computing, 2009.http://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-cloudcomputingdraft.html#axz z1X0xKZRuf.
[8]. Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing (v2.1). December, 2009.
[9]. Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online Michael Miller
[10]. 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
[11]. Dot Cloud: The 21st Century Business Platform Built on Cloud Computing Peter Fingar

Journal Papers

[12]. Pearson, S. and AzzedineBenameur, "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.
[13]. 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.
[14]. Esteves, R.M. and ChunmingRong, "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
[15]. Cloud Application Architectures: Building Applications and Infrastructure in the Cloud (Theory in Practice) by George Reese.
[16]. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice) by Tim Mathe
[17]. 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
[18]. Teswanich, W., &Chittayasothorn, S. (2007). A Transformation of RDF Documents and Schemas to Relational Databases. IEEE Pacific