ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

Emerging Technologies and Protecting Methods in Cloud Computing Environments

N. Thenmozhi [1], S.Gandhimathi[2]

Research Scholar, Dept. of CS, PGP College of Arts & Science, Namakkal, Tamilnadu, India[1]

HOD/Associate Professor, Dept. of CS, PGP College of Arts & Science, Namakkal, Tamilnadu, India[2]

ABSTRACT: Cloud Computing is a set of IT Services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. It advantages to mention but a few include scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment. This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types.

KEYWORDS: cloud storage server, cloud computing, TPA

I. INTRODUCTION

The advancements in Information Technology (IT) demand a new computing paradigm that supports delivery of computing services on minimal charges without installing them at local sites. Cloud computing offers the same model having above describe properties in which services are delivered over internet in an on-demand elastic way for which the charges are paid at release time of resources. In general, cloud is a multifarious technological paradigm that is an extension of many existing technologies viz. parallel and distributed computing, Service Oriented-Architecture (SOA), virtualization, networking etc. The distributed computing, virtualization and internet works as indispensable building blocks of the cloud computing. It is a highly sharable computing paradigm where processing, storage, network, applications etc. are shared. The objective of the cloud computing is to provide secure, qualitative, scalable, quick, more responsive, on demand, cost-efficient and automatically provisioned services viz. computation services, storage services, networking etc. being provided in a transparent way (location independent). Cloud computing can help to improve business performance while making a contribution to control the cost of delivering IT resources to any organization. The fundamental idea of cloud computing was pronounced way back in 1960 by Professor John McCarthy, as; "If comps of the kind I have advocated become the comps of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility. The computing utility could become the basis of a new and important industry". Douglas Parkhill first explored the characteristics of cloud computing in 1966 in his book "The Challenge of the Computing Utility".

Cloud computing can be thought as an extension of Virtual Private Network (VPN) over network infrastructure which is used in telecommunication world. Initially, telecommunication service providers delivered dedicated point-to-point circuit which was the wastage of the bandwidth; the problem was solved by using VPN services where traffics could be switched to balance the utilization of the overall network. Cloud computing was a buzz word for many years and it turned into reality in 2007 when IT giants Google and IBM announced a collaboration in this domain followed by "Blue Cloud" announcement by IBM. According to blog, the prediction of IT advisory company Gartner says that cloud computing business will surpass $148 billion mark by 2014 while its competitor, Forrester, says it will reach $118 billion. Another Gartner's Survey says that the investment on services in public cloud is expected to increase 18.6% in 2012 to $110.3B that achieves a 17.7% Compound Annual Growth Rate (CAGR) from

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

2011 through 2016 [1]. In general, the total market is likely to increase to $210B in 2016 from $76.9B in 2010. Figure 1 gives a glimpse of the distribution of workloads in cloud and a traditional data centre that shows that popularity of cloud will be grow with a very fast rate. Therefore, cloud computing area looks very promising for researchers and businesses. On the other hand, its realization brings many challenging issues that need to be carefully addressed. The organization of remaining paper is as follows. Section 2 presents an overview of cloud computer, its essential characteristics, different deployment models and service models. Section 3 describes the advantages and disadvantages of cloud. Section 4 describes various issues and challenges of cloud computing that are necessary to address in order to adopt this technology. Finally, section 5 concludes the papers.

II. LITERATURE SURVEY

Gartner 2008 identified seven security issues that need to be addressed before enterprises consider switching to the cloud computing model. They are as follows:(1)privileged user access-information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications first to test the water, (2) regulatory computer - clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by 3rd party organizations that check levels of security and providers that don't (3) data location - depending on contracts, some clients might never know what country or what jurisdiction their data is located (4) data segregation - encrypted information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be deployed by the provider. (5) recovery - every provider should have a disaster recovery protocol to protect user data investigative support - if a client suspects faulty activity from the provider, it may not have many legal ways pursue an investigation long-term viability - refers to the ability to retract a contract and all data if the current provider is bought out by another firm.

The Cloud Computing Use Case Discussion Group discusses the different Use Case scenarios and related requirements that may Kuyoro S. O., Ibikunle F. & Awodele O. International Journal of Computing Networks (IJCN), Volume (3): Issue (5): 2011 249 exist in the cloud model. They consider use cases from different perspectives including customers, developers and security engineers. ENISA investigated the different security risks related to adopting cloud computing along with the affected assets, the risks likelihood, impacts, and vulnerabilities in the cloud computing may lead to such risks. Balachandra et al, 2009 discussed the security SLA's specification and objectives related to data locations, segregation and data recovery. Kresimir et al, 2010 discussed high level security concerns in the cloud computing model such as data integrity, payment and privacy of sensitive information.

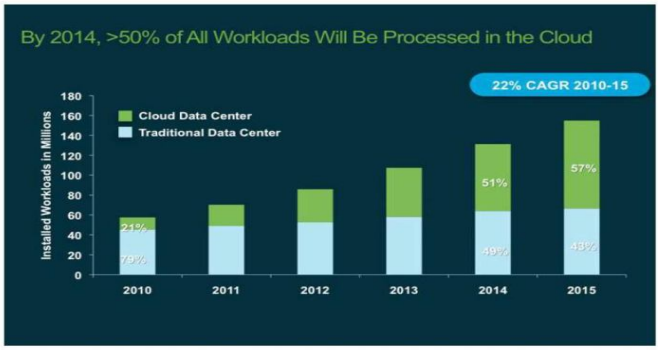

Fig 1.Workload distribution in cloud and traditional data centers

A recent survey by Cloud Security Alliance (CSA)&IEEE indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers. It also details that cloud computing is shaping the future of IT but the absence of a compliance environment is having dramatic impact on cloud computer growth. Several studies have been carried out relating to security issues in cloud computing but this work presents a detailed analysis of the cloud computing security issues

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

and challenges focusing on the cloud computing deployment types and the service delivery types.

III. CLOUD COMPUTING TECHNICAL ASPECT

To properly understand cloud, it is important to know what it is, some essential characteristics that a system must possess to qualify as a cloud along with various services that can be offered using it through various deployment models.

Five Essential Characteristics

The cloud computing must have some characteristics in order to meet expected user requirements and to provide qualitative services. According to NIST, these five essential characteristics can be classified as:

On-demand self-service:

A consumer can access different services viz. computing capabilities, storage services, software services etc. as needed automatically without service provider's intervention.

Broad network access:

To avail cloud computing services, internet works as a backbone of cloud computing. All services are available over the network and are also accessible through standard protocols using web enabled devices viz. computers, laptops, mobile phones etc.

Resource pooling:

The resources that can be assigned to users can be processing, software, storage, virtual machines and network bandwidth. The resources are pooled to serve the users at a single physical location and/or at different physical location according to the optimality conditions (e.g. security, performance, consumer demand). The cloud gives an impression of resource location independence at lower level (e.g. server, core) but not at the higher level (e.g. datacenter, city, country).

Rapid elasticity:

The beauty of cloud computing is its elasticity. The resources appear to users as indefinite and are also accessible in any quantity at any time. The resources can be provisioned without service provider intervention and can be quickly scale in and scale out according to the user needs in a secure way to deliver high quality services.

Measured service:

A metering capability is deployed in cloud system in order to charge users. The users can achieve the different quality of services at different charges in order to optimized resources at different level of abstraction suitable to the services (e.g. SaaS, PaaS and IaaS).

Issues And Challenges Of Cloud Computing

The existing computing paradigms via distributed computing, SOA, networking etc. are building blocks of cloud computing. There are numerous issues associated with theses computing paradigms and some new challenges emerged from cloud computing are required to be addressed properly in order to realize the cloud to its full extent. Current cloud adoption is associated with numerous challenges as shown in Figure 2 and 3 depicting the specific business risk of adopting cloud services and biggest barriers. Therefore, these issues must be addressed in order to provide high quality services to the users while computing with the service provider's needs. The issues can be organized into several different categories varying from security, protection, identity management, resource management, power and energy management, data isolation, availability of resources, heterogeneity of resources. Although, there are several issues that demand attention but the following could be treated as of prime concern.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

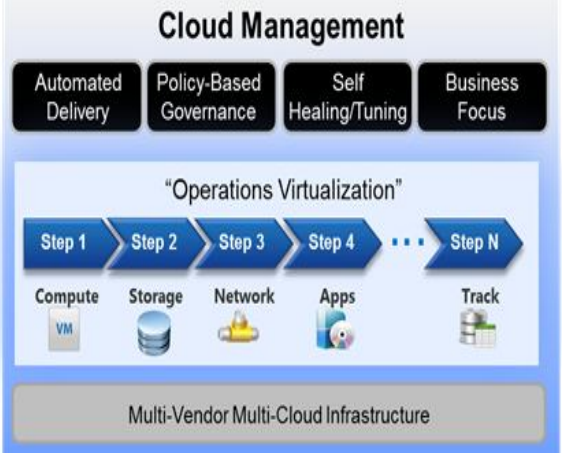

Fig 2.Cloud Management

IV. SECURITY ISSUES FACED BY CLOUD COMPUTING

The vendor for Cloud must make sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud thus affecting many customers who are sharing the infected cloud. Some of the problem which is faced by the Cloud computing.

1. Data Integrity
2. Data Theft
3. Privacy issues
4. Infected Application
5. Data loss
6. Data Location
7. Security on Vendor level
8. Security on user level

Data Integrity

When a data is on a cloud anyone from any location can access those data's from the cloud. Cloud does not differentiate between a sensitive data from a common data thus enabling anyone to access those sensitive data's. Thus there is a lack of data integrity in cloud computing.

Data Theft

Most of the cloud Vendors instead of acquiring a server tries to lease a server from other service providers because they are cost affective and flexible for operation. The customer doesn't know about those things, there is a high possibility that the data can be stolen from the external server by a malicious user.

Privacy Issues

The Vendor must make sure that the Customer Personal information is well secured from other operators. As most of the servers are external, the vendor should make sure who is accessing the data and who is maintaining the server thus enabling the vendor to protect the customer's personal information.

Infected Application

Vendor should have the complete access to the server for monitoring and maintenance, thus preventing any malicious user from uploading any infected application onto the Cloud which will severely affect the customer.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

Data Loss

Data loss is a very serious problem in Cloud computing. If the vendor closes due to financial or legal problems there will be a loss of data for the customers. The customers won't be able to access those data's because data is no more available for the customer as the vendor shut down.

Data Location

When it comes to location of the data nothing is transparent even the customer don't know where his own data's are located. The Vendor does not reveal where all the data's are stored. The Data's won't even be in the same country of the Customer, it might be located anywhere in the world.

Security on Vendor level

Vendor should make sure that the server is well secured from all the external threats it may come across. A Cloud is good only when there is a good security provided by the vendor to the customers.

Security on User level

Even though the vendor has provided a good security layer for the customer, the customer should make sure that because of its own action, there shouldn't be any loss of data or tampering of data for other users who are using the same Cloud.

Protecting the Cloud

A Secure cloud is always a reliable source of information thus protecting the cloud is a very important task for security professionals who are in charge of the cloud. Some of the ways by which a cloud can be protected are Protection of data, making sure data is available for the customers, delivering high performance for the Customers, using Intrusion Detection System on Cloud to monitor any malicious activities, to make sure the application used by the customer is safe to use, Vendors must provide a support system for the customer, customer should be able to recover any loss of data in the cloud.

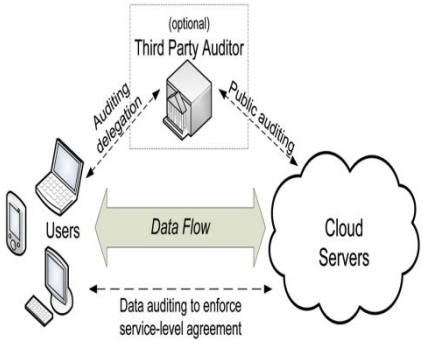

Fig 3.System Overview

V. TCLOUD: A TRUSTED STORAGE ARCHITECTURE FOR CLOUD COMPUTING

The cloud storage provides a least cost means of data storage for the small and large enterprises across the globe. But the main barricade to wide spread adoption of cloud storage is the lake of trust in the technology by its user. The data is stored on multiple servers and the location is concealed from the customers and they are no more in control of the data. This distinctive feature of the cloud storage presents many security and trust challenges. In this paper we present a trusted architecture of cloud data storage. The architecture presents a unique way of secure storage and accessing of data from the cloud data center. It also ensured that only authorized user will be able to access the data. Additionally, if there is any violation of the security parameter at the data center, the data will still be safe i.e. the data will be stored in encrypted form.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

VI. FUTURE OF THE TECHNOLOGY

As cloud computing is a relatively new delivery model it's future is not fully known but seeing as its popularity and excitement around the technology is constantly growing, it's safe to say that cloud computing is here to stay. Short-term forecasts predict that in 2012 80% of new commercial enterprise apps will be deployed on cloud platforms, which illustrates that cloud adoption is set to rise exponentially this year. In the long-term technology experts and stakeholders say they expect they will 'live mostly in the cloud' in 2020 and not on the desktop, working mostly through cyberspace- based applications accessed through networked devices.

The many stakeholders and enthusiasts of the technology see it as the next step in computing, with many businesses and individual users in the future using cloud technology in some shape of form. Using cloud technologies will become even more popular as our network infrastructure is improved allowing less latency and quicker connections to the content on the cloud. Cloud computing technologies are for everyone as it benefits the common user as much as it benefits stakeholders, business leaders and academics as cloud computing has the potential to reduce cost and risk, increase revenue, and enhance total customer experience for everyone. There are a number of trends that have been projected such as that integrated public and private cloud infrastructure will become possible 2012, and many will take advantage of it. This will be possible with emerging technologies such as vCloud Connector 1.5, which lets users running workloads on internal VMware infrastructure slide all or part of those workloads into a leased public cloud running the same infrastructure allowing communication between private and public clouds. Businesses will want to share their information, services and infrastructure with other clouds that means that clouds are going to move towards a cloud network. This will facilitate collaboration for projects or engagements across enterprises and enabling conference calls including temporary, controlled access to internal information systems, knowledge bases or information distribution systems which usually are only accessible to employees.

All the common problems outlined in the previous section will have to be addressed with security being the largest challenge as it can influence the cloud market and also drive trends. There is a concern about cyber gangs hacking into commercial and military systems, which leads to a worldwide trend that temporarily reduces public cloud adoption and in order to protect against these negative trends security and standards must not be ignored.

VII. COMPUTATION

It is clear that cloud computing is here to stay for the foreseeable future, as the topic has had buzz around it for years now and it is finally being adopted by many with more to follow. The key concepts, terminologies and underlying technologies of cloud computing that were outlined should clarify and aid in the understanding of this complex topic. Through identifying the current challenges that cloud computing technologies are experiencing it allows cloud service providers to act upon them and also give consumers a better understanding of the problems which can affect them when migrating to cloud environments. In order for cloud technologies to be fully adopted by everyone the challenges in standards, consumer confidence, data governance and most importantly security must be addressed. The future of cloud computing is not definite but by analyzing the trends it seems that cloud technology will play a large part in our day to day lives. In the future business and consumers will benefit from higher interoperability between clouds and maybe even a cloud network which will improve sharing of resources and information. There are many uses for this technology and it is surely going to change the way in which we handle our data, services and access/store our digital content but for its full potential to be unlocked a broader understanding, appreciation and investment in cloud computing technologies is required.

REFERENCES

1. Marshall, D. "Microsoft: 2012 – The Year Cloud Moves from a Buzzword to Reality" [on-line] available from: http://vmblog.com/archive/2011/12/12/microsoft-2012-the-year-cloud-moves-from-a-buzzword-to-reality.aspx
2. Rajan, S. & Jairath, A. (2011) "Cloud Computing: The Fifth generation of Computing, 2011 International Conference on Communication Systems and Network Technologies (2011) Volume: 15, Issue: 4, Publisher: Ieee, Pages: 665-667
3. Mell, P. & Grance, T. (2011) "The NIST Definition of Cloud Computing (Draft)", Publisher: U.S. Department of Commerce
4. Weiss, A. (2007) "Computing in the Clouds", Networker Volume: 11, Issue: 4, ACM, Pages: 16-25

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

5. Xu, D. (2010) "Cloud Computing: an Emerging Technology", 2010 International Conference On Computer Design And Appliations (ICCDA 2010), IEEE, Pages 100-104
6. Gong,C., Liu, J., Zhang, Q., Chen, H. & Gong, Z (2010) "The Characteristics of Cloud Computing", Parallel Processing Workshops (ICPPW), 2010 39th International Conference, IEEE, Pages 275 -279
7. IBM, "IBM Cloud Computing: PaaS–United States" http://www.ibm.com/cloud-computing/us/en/paas.html
8. Creeger, M. (2009) "Cloud Computing: An Overview", Magazine Queue - Distributed Computing Queue Homepage archive Volume 7 Issue 5, June 2009, ACM
9. Vouk, M.A. (2008) "Cloud Computing Issues, Research and Implementations", Information Technology Interfaces, 2008. ITI 2008. 30th International Conference, Pages 31 - 40 ISSN: 2089-3337ρ IJ-CLOSER Vol. 1, No. 2, June 2012: 59 – 65 64
10. Armbrust, M. (2009) "Above the Clouds: A Berkeley View of Cloud Computing", Publisher: UC Berkeley Reliable Adaptive Distributed Systems Laboratory
11. Mahjoub, M., Mdhaffar, A., Halima, B. R. & Jmaiel, M (2011) "A comparative study of the current Cloud Computing technologies and offers", Network Cloud Computing and Applications (NCCA), 2011 First International Symposium, Publisher: IEEE, Pages: 131 – 134
12. Linthicum, D. (2010) "The cloud's three key issues come into focus", [on-line] available from: http://www.infoworld.com/d/cloud-computing/clouds-three-key-issues-come-focus-164?page=0,0
13. Dillon, T., Wu, C., & Chang, E. (2010) "Cloud Computing: Issues and Challenges", 2010 24th IEEE International Conference on Advanced Information Networking and Applications (2010), Pages: 27-33
14. Zhen, J. (2008) "Five Key Challenges of Enterprise Cloud Computing", http://cloudcomputing.syscon.com/node/659288
15. Mikkilineni, R. & Sarathy, V. (2009) "Cloud Computing and the Lessons from the Past", Enabling Technologies: Infrastructures for Collaborative Enterprises, 2009. WETICE '09. 18th IEEE International Workshops, pp: 57 – 62.