International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 22 Issue 1 –MAY 2016.

CLOUD COMPUTING: SERVICES AND TRUST MODELS

A.Mary Odilya Teena[#1] I.Roseline Jecintha[#2] and A.Isabella Amali[#3]

[#] *Assistant Professor, St. Joseph's College of Arts & Science (AUTONOMOUS), Cuddalore-607001.*

***Abstract*— A new technological trend called Cloud Computing portends a major change in the way of using computer and internet in the world today. Everything is hosted in the cloud and accessed uniquely. This paper exhibits the important key concepts of Cloud Computing. The First Section deals with the definition of Cloud Computing and the Second Section explains about Cloud Services, Cloud Deployment model presented in Section 3 , Cloud Service Provider in Section 4, and Security is discussed in the last section.**

***Index Terms*— Cloud Computing, Cloud Components, Pros and Cons of Cloud Computing, Cloud Services, Cloud Deployment Models, Cloud Service Provider, Security.**

I. INTRODUCTION

Cloud computing also known as the cloud, is a distributed computing that provides a virtualized environment to the cloud users for accessing and exchanging their applications and data through Internet [1,2]. Cloud Computing is a document centric. Because the document what we create are stored in the collection of servers accessed via the Internet.

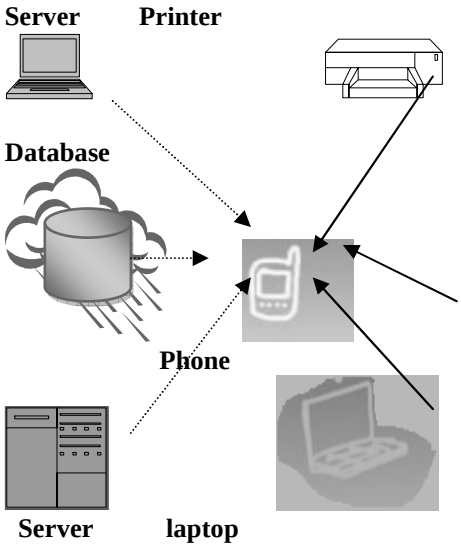

Figure 1: Cloud Overview

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction[1] " – defined by NIST(National Institute of Standards and Technology). European Community for Software and Software Services (ECSS) quoted "Cloud as the delivery of computational resources from a location other than your current one".[3,4,5]

Internet based Cloud computing has become a part of the competitive market today. The most and best examples of cloud computing applications today are the Google family of applications. IBM, Sun systems and other big companies are developing cloud-based applications and storage devices. Cloud Computing has as its antecedents both client/server computing and peer-to-peer computing.

A. Cloud Entity

Cloud entity refers to an entity in the cloud, such as a cloud provider (CSP - one who manages and offers services on the cloud), a cloud user (CU – one who makes use of services from the cloud), a cloud broker (CB – manages the usage, performance and delivery of cloud services and discussed relationships between CSPs and CUs) and a cloud auditor. Trust evaluation depends on cloud service provider and cloud broker, Cloud broker and cloud user.

B. Cloud Components

Clients, Datacenter and distributed servers are the Components of Cloud Computing [6]. Each element plays a specific role in delivering a functional Cloud based application. Clients are the devices that the end users interact with to manage their information on the cloud. The three categories of Clients are,

i) Mobile (Mobile devices include PDAs or Smart Phone or an iphone),
ii) Thin (No internal hard drivers)
iii) Thick (Regular computer using a web browser like Firefox or Internet Explorer).

The datacenter is a collection of servers where the application to which you subscribe is housed. Distributed Servers gives the service provider more flexibility in options and security.

C. Pros and Cons of Cloud Computing

The pros and cons of Cloud Computing are listed below.

Advantages
Cost Efficient.

Improved Performance
Lower IT Infrastructure costs
Unlimited Storage Capacity
Fewer maintenance issues
Lower Software Costs
Backup and Recovery
Easy access to information
Instant Software updates
Increased Computing power
Increased Data Safety
Easier Group Collaboration

DisAdvantages
Connections and can be slow
Features might be limited
Stored data might not be secure
Doesn't work well with Low speed

II. CLOUD SERVICES

Cloud Services (CS) are the services available in the cloud. Cloud Service Level Agreement (SLA) is the legal contract between the Cloud Service Provider and Cloud user. It is important in cloud services. It gives a clear idea about the cloud service providers. It monitors the service quality, performance, priority and responsibility from service point of view. Customer based SLA, Service based SLA, Multilevel SLA, Customer level SLA and Service level SLA are the five types of SLA.

Cloud Computing Services are broadly classified in three different types namely, Infrastructure as a Service (IaaS) , Platform as a Service (PaaS), Software as a Service (SaaS) called as Cloud Service Models[7,8,9,10]

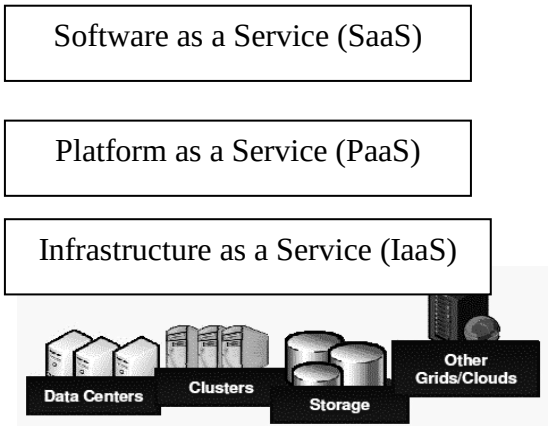

Figure 2: Cloud Services

A. Infrastructure as a Service (IaaS):

IaaS is the first layer of Cloud Services. In this model, the user manages data, operating system, middleware and runtime. The service provider manages virtualization, servers, networking and storage. It provides highest level of flexibility and management control in IT resources and similar to existing IT resources. So many IT departments and developers are familiar with today.

Amazon EC2 is the best known IaaS provider. AWS, Windows Azure, Rackspace, Red Hat, VMvare and Google Compute Engine are some of the well known providers of IaaS. It is also described as a set f infrastructure capabilities such as operating system, network connectivity, CDNs and few other key infrastructure services. NaaS involves the optimization of resource allocations and resource computing in the network. VPN, and bandwidth on demand are the common example of NaaS [10,11,12,13].

1) Advantages of IaaS:

1. It is easily scalable. Resources are available on demand as and when the user requires it.
2. No investment in hardware for the users.
3. Saves the implementation cost and time of execution.
4. Charges based on the compute power that is utilized.
5. The service can be accessed from any location through Internet connection. So, it is location independent.
6. Cloud provider provides physical security of user's data. So the time required to give security to data is saved.
7. The chance of system failure is less. If failure occurs, it will be smoothly handled by the service provider. So it is fault tolerant.

B. Platform as a Service (PaaS):

It is the middle layer of cloud computing service model. In this model, the providers deliver applications over the Internet and host user's hardware and software on their applications. One popular example is Google App Engine. It takes advantage of dynamic scalability, automated database backups, and other platform services without the need to specifically code for it. For this reason PaaS adds support a specific set of programming languages or developing environments.

PaaS supplies all the resources required to build applications and services completely from the Internet without having to download or install software. In this model, Cloud Service Providers provides a platform which includes operating system, programming language execution environment, database, and web server. The users can use these services to develop and deploy their own applications.

The main disadvantage of this model is lack of interoperability and portability among providers. Data security, backup and recovery are the major security issues.

AWS Elastic Beanstalk, Cloud Foundry, Heroku, Force.com, OrangeScape are some examples of well known PaaS providers.

In PaaS services the user has to pay for a subscription basis and charged just for what they use.[10,11,12,13,14]

1) Benefits of PaaS:

1. It includes application design, development, testing,

deployment and hosting.

2. No need to invest for physical infrastructure as it will be provided by IaaS on demand. It gives fully mobility to focus on the development of applications.

3. Application development is simple. The application can be developed by less technical knowledge by using web browser.

4. PaaS Services charges on monthly basis.

5. Allows developers to frequently change or upgrade Operating System feature if required.

6. The services are not isolated, application specific or location dependent. The users in various locations can work together and connected through a communication medium.

C. Software as a Service(SaaS) :

The third layer of the cloud service model is Software as a Service. It is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. All programs are running in the cloud, managed by cloud vendor. Service provider is responsible for the software installation and operation, which is already available by using IaaS and PaaS. Users doesn't pay for owning the software, they can only pay for using it.

One of the well known example is SalesForce.com. Other popular examples are Microsoft Office365, Jira, Box.net, Basecamp, Onlive, GT Nexus, Marketo, and TradeCard and google apps. These applications are hosted in "the cloud" and can be used for a wide range of tasks for both individuals and organizations [14,15,16,17].

1) Benefits of SaaS:

1. Need not pay for extra licensing fees.

2. The user has to pay for software not for infrastructure or platform setup.

3. We can add new users easily.

4. All users will have the same version of software. So, compatibility is good and easier collaboration.

5. Application development is simple in SaaS.

6. Automatic updates.

7. Global accessibility.

8. The services are not isolated, application specific or location dependent.

9. No initial setup costs required with SaaS.

III. CLOUD DEPLOYMENT MODELS

Cloud Computing are classified into Cloud computing service models and cloud computing deployment models.

A. CLOUD DEPLOYMENT MODEL

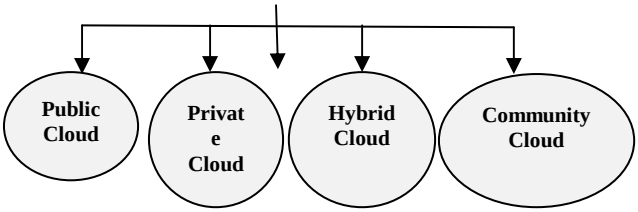

Figure 3 : Cloud Deployment model

1) Cloud hosting deployment models represent the exact category of cloud environment and are mainly distinguished by the proprietorship, size and access. It tells about the purpose and the nature of the cloud. On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured service are the five essential characteristics of cloud model.
2) Public Cloud (External Cloud), Private Cloud (Internal Cloud), Community Cloud(Grouped Cloud), Hybrid Cloud(Mixed Cloud) are the four different types of Cloud Deployment Models[17-21].
3) The most popular model of public cloud model provides cloud services in a virtualized environment accessible via Web applications or Web services through Network. It renders services and infrastructure to various clients. It is suitable for business requirements. There was a slight or no difference between private and public cloud structure except in the level of security offered for various cloud services. Google is an example of a public cloud. The service can be provided by a vendor free of charge or on the basis of a pay-per-user license policy.

A private cloud also known as internal cloud which provides a distinct and secure cloud based environment in which only the authentic users within an organization can access.

A community cloud is a type of cloud hosting that provides a distinct and secure environment where organizations with similar requirements share a common cloud infrastructure. It can be managed by third party provider. It can be hosted externally or internally. The cost is shared by the specific organizations within the community hence it helps to reduce cost as compared to a private cloud.

A hybrid cloud provides an integrated environment accessible to both private and public cloud functionalities. It permits the user to increase the capacity or the capability by aggregation, assimilation or customization with another cloud service. This model is also used for handling cloud bursting.

To provide high quality of service to customers, CSP uses individual cloud providers that work collaboratively to form a federation of clouds. It involves multiple clouds that are tied together to build a larger one. It is used in Real time online interactive applications, weather forecasting and research, etc.

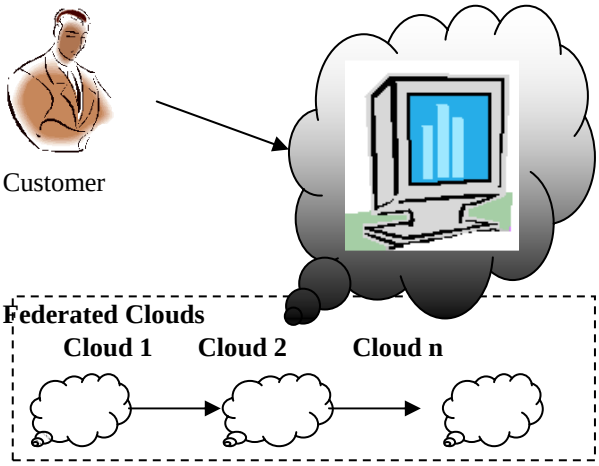

Figure 4 : Federated Clouds

IV. CLOUD SERVICE PROVIDERS

A Cloud Service Provider (CSP) or Cloud Provider is a company that offers Cloud Services such as Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) to other businesses or individuals.

Cloud providers host their resources on the internet on virtual computers and make them available to multiple clients. Multiple virtual computers can run on one physical computer sharing the resources such as storage, memory, the CPU and interfaces giving the feeling to the client that each client has his own dedicated hardware to work on.

Cloud service providers are making a substantial effort to secure their systems, in order to minimize the threat of insider attacks, and reinforce the confidence of customers [22]. Cloud Service Providers (CSP) are the utility computing provider organizations that delivers cloud computing based services and solutions to the cloud users. The services includes Virtual infrastructure, computing platforms and applications software.

CSP delivers cloud services through On-Demand, pay-as-use systems as a service to cloud users. Users access cloud resources through web based applications. A user will choose a good cloud service provider based upon the services, platforms, Infrastructure details and user interfaces.

Amazon, Google, IBM, Microsoft, and Yahoo are the forerunners that provide cloud computing services. Other companies such as Apple, Cisco, Citrix, Joyent, Google, Microsoft, Rackspace, Salesforce.com and Verizon/Terremark also begin to provide all kinds of cloud computing services for the Internet users.

V. TRUST MECHANISMS

Several trust mechanisms are used are computed to ensure the security and privacy of the users accessing the services. Reputation based trust, SLA verification based trust, Policy based trust, Evidence based trust are the some of the existing trust mechanisms in the cloud. Policy based trust is a real formal trust mechanism used in Public Key Infrastructure (PKI). Trust and Reputation are different, but related.

The Reputation Based Trust is the basic element of trust computation. The reputation of an entity is the aggregated opinion of a community towards that entity. It is further classified into Direct trust and Indirect trust. Direct trust is the most contributing factor for trust computation. In this trust mechanisms are widely used in e-commerce and P2P networks. A Service Level Agreement(SLA) is a legal contract between a cloud user and cloud service provider. It is an important basis of trust management for cloud computing. In Evidence based trust, the expected behavior on the evidence about the trustee's attributes of Competency, goodwill and integrity.

VI. TRUST MODELS

The general term in Cloud trust means "security" and "privacy". Expectance, Belief, Willingness to take risk are the most important state of a trust. Cloud shared many kinds of distributed resources to different organizations, hence establishing trust between Cloud users and Cloud Service Providers is a very big issue in a Cloud Environment. To solve these issues a number of tools and models have been proposed and used in distributed systems. Some of the commonly used trust models are Cuboid Trust, Eigen Trust, Bayesian Network based Trust Management (BNBTM), Group Rep, AntiRep, Semantic Web Global trust, Peer trust, etc. But due to lack of standardization and interoperability these models are not widely accepted by the industry. Comprehensive research about the trust model would help the user in the selection of an appropriate model according to their security and functional requirement. Trust models are used to measure the security strength and computes trust value based on the attributes. And also Cloud Security Alliance(CSA) service challenges are used to assess security of a service and validity of the model.

VII. CONCLUSION

Security is the active area of research. In this paper focus only the key concepts of Cloud Computing. In future work, we have performed in depth analysis of the existing trust models in the cloud.

REFERENCES

[1] Francesco M.A and Gianni F. "An approach to a cloud Computing network", IEEE, August 2008, pp113-118
[2] Huaglory Tianfield,"Cloud Computing Architectures",978-1-4577-0653-/11/©2011 IEEE.
[3] Wikipedia, http://en.wikipedia.org/wiki /Cloud_Computing
[4] Rafael Moreno-Vozmediano,Rubén S. Montero, Ignacio M.Llorente," Key Challenges in Cloud Computing -Enabling the Future Internet of Services", Published by the IEEE Computer Society 1089-7801/13/ © 2013 IEEE, IEEE internet computing
[5] M.Rajendra Prasad, R. Lakshman Naik, V.Bapuji," Cloud Computing : Research Issues and Implications ", International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.2, No.2, April 2013, pp. 134~140 ISSN: 2089-3337.
[6] Cloud Computing:A Practical Approach by Anthony T.Velte, Toby J.Velte and Robert Elsenpeter.

[7] Xu Xiaoping, Yan Junhu," Research on Cloud Computing Security Platform", 978-0-7695-4789-3/12 © 2012 IEEE DOI 10.1109/ICCIS.2012.238.
[8] Dimitrios Zissis , Dimitrios Lekkas, "Addressing cloud computing security issues", 0167-739X/ © 2010 Elsevier B.V. All rights reserved.doi:10.1016/j.future.2010.12.006.
[9] "Understanding Cloud Computing Vulnerabilities", by the ieee computer and reliability societies 1540-7993/11/ © 2011 IEEE march/april 2011.
[10] Hassan Takabi , James B.D. Joshi, Gail-Joon Ahn, "Security and Privacy Challenges in Cloud Computing Environments", by the ieee computer and reliability societies ,1540-7993/10/ © 2010 IEEE , november/december 2010.
[11] Zhifeng Xiao and Yang Xiao, Senior Member, IEEE," Security and Privacy in Cloud Computing", IEEE communications surveys & tutorials, VOL. 15, NO. 2, second quarter 2013, 1553-877X/13/ c_ 2013 IEEE.
[12] Peter Mell," What's Special about Cloud Security? ", IT Pro July/August 2012, P u b l i s h e d by t h e I E E E Comp u t e r S o c i e t y, 1520-9202/12/ © 2012 IEEE.
[13] Jianhua Che, Yamin Duan, Tao Zhang, Jie Fan," Study on the security models and strategies of cloud computing", 1877-7058 © 2011 Published by Elsevier Ltd. doi:10.1016/j.proeng.2011.11.2551.
[14] Xue Jing, Zhang Jian-jun2. "A Brief Survey on the Security Model of Cloud Computing" 978-0-7695-4110-5/10 © 2010 IEEE DOI 10.1109/DCABES.2010.103
[15] Engr: Farhan Bashir Shaikh, Sajjad Haider," Security Threats in Cloud Computing", 978-1-908320-00-1/11@2011 IEEE
[16] H.Sato,et al., "A Cloud Trust Model in a Security Aware Cloud", SAINT2010, pp.121-124.
[17] Mladen A. Vouch, "Cloud Computing Issues, Research and Implementations|", Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246.
[18] Latifa Ben, Arfa Rabai , Mouna Jouini, Anis Ben Aissa , Ali Mili," A cybersecurity model in cloud computing environments", 1319- 1578 ª 2012 King Saud University. Production and hosting by Elsevier B.V. All rights reserved.http://dx.doi.org/10.1016/j.jksuci.2012.06.002
[19] M. Mackay, T. Baker, A. Al-Yasiri," Security-oriented cloud computing platform for critical infrastructures", 0267-3649/ 2012 M. Mackay, T. Baker & A. Al-Yasiri. Published by Elsevier Ltd. All right reserved.http://dx.doi.org/10.1016/j.clsr.2012.07.007.
[20] S. Subashini , V.Kavitha," A survey on security issues in service delivery models of cloud computing", 1084-8045/ 2010 ElsevierLtd. All rights reserved. doi:10.1016/j.jnca.2010.07.006.
[21] Y. Jianfeng, C. Zhibin. "Cloud Computing Research and Security Issues" CISE 2010. Dec, 2010
[22] T. R. Peltier, J. Peltier, and J. Blackley. Information SecurityFundamentals. Auerbach Publications, Boston, MA, USA, 2003.