Research Article Impact Factor: 0.621 ISSN: 2319-507X
Jayashree Chirde, IJPRET, 2014; Volume 2 (8): 162-172 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

CLOUD COMPUTING-ARCHITECTURE, SECURITY ISSUES

JAYASHREE S. CHIRDE, P. H. PAWAR

ME Student, Department of CSE, Babasaheb Naik College of Engg, Pusad (INDIA)

Accepted Date: 15/02/2014 ; Published Date: 01/04/2014

Abstract: Cloud computing was define as a computing environment where computing needs by one party can be outsourced to another party and when need be arise to use the computing power or resources like emails, they can be access them via internet. Cloud computing facilitates its consumers by providing virtual resources via internet. General example of cloud services are Google apps, business application provided by Google and Microsoft SharePoint. The rapid growth in field of “cloud computing” also increases severe security concerns. Security has been remained a constant issue for Open Systems and internet, when we are talking the about security cloud really suffers. The wide acceptance www has raised security risks along with the not countable advantages, so is the case with cloud computing. The cloud computing has lots of security challenges for the consumers and service providers. How the users of cloud computing know that their information is not having any availability and security issues? Every one poses, Is their information secure? This study aims to identify the most assailable security threats in cloud computing, which will enable both end users and sellers. In our work we discussed what is the architectural design of cloud computing and security issues in it.

Keywords: Cloud Computing; Issues; Architecture; Cloud Computing Security

Corresponding Author: Ms. JAYASHREE S. CHIRDE

Access Online On:

www.ijpret.com

How to Cite This Article:

Jayashree Chirde, IJPRET, 2014; Volume 2 (8): 162-172

PAPER-QR CODE

INTRODUCTION

Cloud computing is a especially used to describe a variety of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. Cloud computing deals with computation, data access and storage services that may not require end-user knowledge of the physical location and the configuration of the system that is delivering the services. Cloud computing is a recent trend in the IT that transfer computing and data away from desktop and portable PCs into large data centers [4] Besides, Resources of cloud computing are dynamic and scalable. Cloud computing is independent computing it is totally different from grid and utility computing. Google Apps, Sales force, Microsoft Azure are the paramount examples of Cloud computing, it enables to services for accesses via the browser and deployed on millions of machines over the Internet. Resources are accessible from any place across the globe using the internet. Cloud computing is low cost than other computing models; it required no maintenance cost is involved since the service provider is responsible for the availability of services and clients are free from maintenance and management problems of the resource machines. Due to this feature, the cloud computing is also known as utility computing, or IT on demand‘. Scalability is key attribute of cloud computing and is achieved through server virtualization. This fresh, web-based generation of computing uses remote servers placed in extremely safe and secure data centers for storage of data and management, so organizations do not need to pay for and look after their internal IT solutions. After creation of a cloud, Deployment of cloud computing differs with reference to the requirements and for the purpose it will be used.

I. CLOUD COMPUTING ARCHITECTURE

Cloud computing system can be divided into two sections: the front end and the back end [5]. They both are connected with each other through a network, usually the internet. Front end is what the client (user) sees whereas the back end is the

cloud of the system, which stored data. Front end has the client's computer and the application required to access the cloud and the back has the cloud computing services like various computers, servers and data storage. Monitoring of traffic, administering the system and client demands are administered by a central server. It follows certain rules i.e., protocols and uses a special software called the middleware [5]. Middleware allows networked computers to communicate with each other.

A. Layers and Services of Cloud Computing

Architecture

Client
Application
Platform
Infrastructure
Sever

The above diagram shows the different layers of cloud computing architecture [6]. A cloud client consists of computer hardware and/or computer software which relies on cloud computing for application delivery, or that is specifically designed for delivery of cloud services [7].

The principal service model are:

1. Software as a Service (SaaS)

2. Platform as a Service (PaaS)

3. Infrastructure as a Service (IaaS)

1. Software as a Service(SaaS)

A cloud application delivers "Software as a Service (SaaS)" over the internet, thus eliminating the need to install and run the application on the users system [7]. Important characteristics of this are: [7] Network-based access and management of commercially available software that are managed from centralized locations and enabling customers to access these applications remotely through the internet. Examples of the key providers are SalesForce.com (SFDC), NetSuite, Oracle, IBM and Microsoft [8]. Google Apps is the most widely used SaaS. No Software as a service sometimes referred to as "software on demand," is software that is deployed for the internet and/or is deployed to run behind a firewall on a local area network or personal computer.

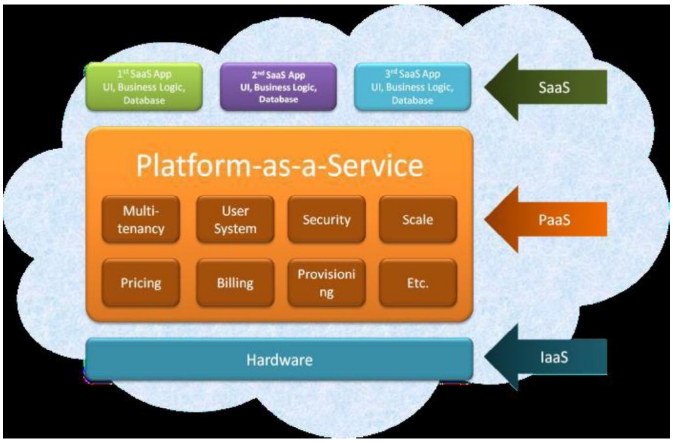

Fig 1: Cloud Computing Services

2. Platform as a Service (PaaS)

Platform services "Platform as a Service (PaaS)" gives a computing platform using the cloud infrastructure. It has all the application typically required by the client deployed on it. Thus client need not go through the hassles of buying and installing the software and hardware required for it. Through this service is developers can get a hold of all the systems and environments required for the life cycle of software, be it developing, testing, deploying and hosting of web applications. Key examples are GAE, Microsoft's Azure [8].PasS has several benefit for developers. With PaaS, operating system features can be changed and upgraded frequently.

3. Infrastructure as a Service (IaaS)

Infrastructure-as-a-Service like Amazon Web Services provides virtual server instances with unique IP addresses .Infrastructure services "Infrastructure as a Service (IaaS)" provides the required infrastructure as a service. Client need not purchase the required servers, data center or the network resources. Also the key advantage here is that customers need to pay only for the time duration they use the service. As a result customers can achieve a much faster service delivery with less cost. Examples are GoGrid,

Flexiscale, Layered Technologies, Joyent andMosso/Rackspace [8].

Figure shows the conceptual diagram of Cloud Computing

[6]:

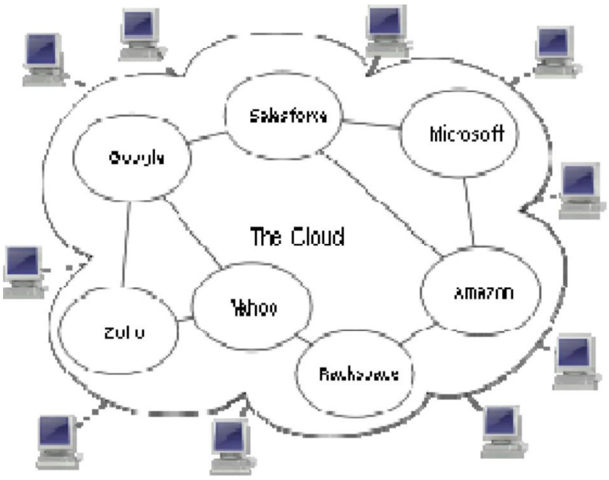

Fig 2: conceptual diagram of Cloud Computing

Server consists of the characteristic computer hardware and/or software required for the delivery of the above mentioned services. Figure2 shows the various cloud computing services with their examples.

B. Deployment a/Cloud Computing Service

For deploying a cloud computing solution, the major task is to decide on the type of cloud to be implemented. Presently three types of cloud deployment takes place - public cloud, private cloud and hybrid cloud Figure below shows the overview of the deployment of these three clouds [11 :

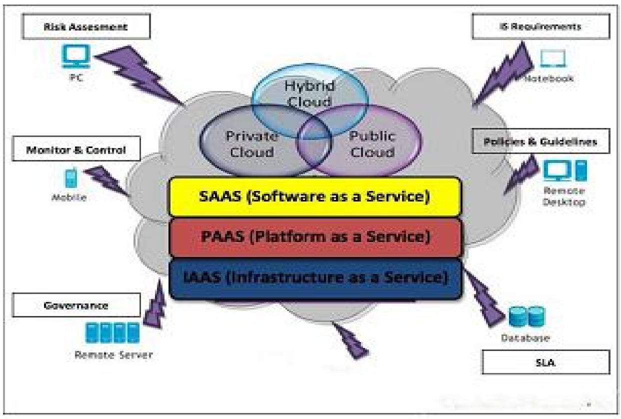

Fig 3: overview of cloud computing.

a) Public Cloud

Public cloud allows users' access to the cloud via interfaces using web browsers. Users need to pay only for the time duration they use the service, i.e., pay-per-use. This can be compared to the electricity system which we receive at our homes. We are pay only for the amount of that we use. The same concept used here. This helps in reducing the operation of costs on IT expenditure. However public clouds are less secure compared to other cloud models as all the applications and data on the public cloud are more prone to malicious attacks. The solution to this can be that security checks be implemented through validation on both sides, by the cloud vendor as well as the client. Also both the parties need to identify their responsibilities within their boundaries of operation.

b) Private Cloud

A private clouds operation is within an organization's internal enterprise data center. The main advantage here is that it is easier to manage security, maintenance and upgrades and provides more control over the deployment and use. Private cloud can be compared to the intranet. Compared to public cloud where all resources and applications were managed by the service provider, in private the cloud these services are pooled together and made available for the users at the organizational level . A community cloud may be established where several organizations have similar requirements and seek to share infrastructure so as to realize some of the benefits of cloud computing. The resources and applications are managed by the organization itself. Security is enhanced here as only the organizations' users' have access to the private cloud.

c) Hybrid Cloud

It is a combination of public cloud and private cloud. In this model a private cloud is linked to one or more external cloud services. It is more secure way to control data and applications and allows the party to access information over the internet. It enables the organization to serve its needs in the private cloud and if some occasional need occurs it asks the public cloud for intensive computing resources[2].

d) Community Cloud

When many organization jointly construct and share a cloud infrastructure, their requirements and policies then such a cloud model is called as a community cloud. The cloud infrastructure could be hosted by a third-party provider or within one of the organizations in the community[2].

II. LITERATURE REVIEW

Rongxing et al [9] in this paper gave a new security and provenance proposal for data forensics and post examination in cloud computing. According to them their proposed system is typified, the proposed system can provide the privacy and security on secret documents/files that are piled up in the cloud. It also provides secure authentication mechanism to control unauthorized user access, and provides track mechanism to resolves disputes of data. Their proposed secure provenance scheme is working on the bilinear pairing method and they have claimed it as the necessary building blocks of data forensics and post examination in cloud computing environment. Using provable security techniques, they have formally verified that there proposed scheme is safe and sound in the standard model. There proposed secure rovenance system for cloud computing includes five parts: [9] “Setup, KGen, AnonyAuth, AuthAccess, and ProveTrack”. Due to theample security features, the scheme proposed produces reliable facts for data forensics in cloud computing. They claim that their proposed system can be a cause to move forward for the wide recognition of cloud computing.

The advantages of their work is the proposed secure system and disadvantages of their work is that their proposed scheme is difficult to implement as it is based on complex mathematical model which is very difficult to understand and they discussed problem of Data Forensics and post investigation in cloud computing.

La‘Quata Sumter et al. [10] says: The rise in the scope of “cloud computing” has brought fear about the “Internet Security” and the threat of security in “cloud computing” is continuously increasing. Consumers of the cloud computing services have serious concerns about the availability of their data when required. Users have server concern about the security and access mechanism in cloud computing environment. To assure users that there information is secure, safe not accessible to unauthorized people, they have proposed the design of a system that will capture the movement and processing of the information kept on the cloud. They have identified there is need of security capture device on the cloud, which will definitely ensure users that their information is secure and safe from security threats and attacks. The proposed implementation is based on a case study and is implemented in a small cloud computing environment. They have claimed that there proposed security model for cloud computing is a practical model cloud computing.

The benefit of their work is assurance of security to the end users of cloud. The limitation of this study is there proposed framework is not feasible for large scale cloud computing environments and they discussed problem of Security Risk and Security assurance to cloud user.

Mladen [11] states that “Cloud” computing is a recent field, which came into existence after Years of research in networking and different types of computing. It uses a SOA, that minimized the information technology operating and maintenance cost for the clients, it offers greater flexibility, reduces capital costs, provides required services are along with many other characteristics. This study discusses issues associated with cloud computing along with Virtualization, Cyber infrastructure; Service oriented Architecture and end users. Implementation, research and security issues are studied in detail and key concerns have been identified. The study ranked security as the primary challenge in cloud computing. It is being observed that the users of cloud computing services are not satisfied with the current security mechanism in cloud computing. Service providers must assure the availability and reliability of services to the consumers available anytime, anywhere using internet, plus security, safety, data protection and Privacy is also exercised. The study further emphasizes that further research on security of cloud computing is required.

The advantages of this study is the identification of issues related with security and implementation. The drawback of this work is the study is based on theoretical concepts nothing practical found in this study. This work could have contributed more if practical things were discussed and they discussed problem of SSH tunnels and VLANs, variable integrity and end-to-end service isolation through VPN

Wenchao et al. [12] in this paper have taken alternative perspective and proposed data centric view of cloud security. They have explored the security properties of secure data sharing among the applications hosted on clouds. They have discussed the data management issues in distributed query processing, Forensic and system analysis and query correction assurance. They have proposed a new security platform for cloud computing, which is named as Declarative Secure Distributed Systems (DS2). According to them the DS2 platform includes the functionality essential for their proposed data security methods. In DS2, the network protocol and security policies are specified Via Secure Network Data log (SeNDlog) a Language which is normally rooted in Datalog that merges declarative networking and logic-based access control Specifications. In this paper they have developed DS2 prototype using the Rapid Net declarative networking engine They have added provenance support to the DS2 platform because they believe that the distributed Provenance is significant step towards a secure cloud data management infrastructure.

The benefit of their work is the proposed tool for data centric security which provides secure query processing, seamless integration of declarative access control policies, system analysis and forensics, efficient end-to-end verification of data. Limitations are not worth mentioning. There work needs to be validated from cloud computing vendors and discussed the problem of Secure Query processing and data Shearing system anlysis and forensics.

Soren et al [13] in this paper they mentioned that benefits of clouds are shadowed with the security, safety and privacy challenges and due to these challenges the adoption of cloud computing has been inhibited to a great extent. It is stated that highly flexible but very complex cloud computing services are configured using web interface by use but wrong configuring of cloud computing by users may lead to vulnerable security threats and can cause security incidents. In this paper an approach has been presented for analyzing security at client side and server side. Amazon‘s Elastic Compute Cloud (EC2) has been chosen for this assessment. The primary aim is to focus on the accessibility, vulnerabilities in the entire cloud infrastructure of cloud computing. They have been implemented the security analysis model & weigh up it for realistic environments. A specialized query policy language for assessment has been proposed in this paper, which is used to get handy into the arrangement and to state required and not required configurations .That they claim that their approach they have used effectively allows remediate current security issues by validating configurations of complex cloud Infrastructures. Security assessment has been implemented in Python and weigh up was calculated on Amazon EC2. Breaches in the weaknesses of security policies are Identified and probable attack trails are informed to the administrators of the system in order to ensure concerned services are checked and action is taken to make them secure.

The benefit of this work is their proposed tool which provides Strong analysis of security attacks and vulnerabilities, this will helps vendors to improve their security policies the drawback is that their proposed framework is specific to Amazon. This study contributed more if it would have been general instead of specific to Amazon and discussed the problem of reach ability Audit of Amazons Security Groups & security Graphs.

III. FUTURE WORK

Cloud computing is not totally secure and we needs explored. After our study we claiming that security is the most important part to both the users and the vendors of cloud computing. Vendors, Researchers and are working on security issues associated with cloud computing. Different models and tools have been proposed but still nothing fruitful found. While doing the research on security issues of cloud computing we came to know that there are no security standards available for secure cloud computing. In our future work we will work on architecture and security standards for secure cloud computing.

IV.CONCLUSION

In this paper we have discussed a new wave in the field of information technology: cloud computing. We have also described its architecture and security issues. There is no doubt that cloud computing is the development trend for the future. Cloud services are used by both larger and smaller scale organizations. Advantages of Cloud computing are huge. But it‘s a global phenomenon that everything in this world has advantages as well as limitations . Cloud computing is suffering from severe security threats from user point of view, one can say that lack of security is the only worth mentioning disadvantage of cloud computing. Both the Service providers and the clients must work together to ensure safety and security of cloud and data on clouds. Mutual understanding between service providers and users is extremely necessary for providing better cloud security. In this paper we have identified that security is biggest hurdle in wide acceptance of cloud computing. Users of cloud services are in fear of data loss and privacy. Researchers and IT security professionals must come forward and do more to ensure security and privacy to users. Our study identifies security concerns of cloud computing, these concerns are Data loss, Leakage of Data, Client‘s trust, User‘s Authentication, Malicious users handling.

REFERENCES

1. Engr: Farhan Bashir Shaikh, Sajjad Haider“ *Security Threats in Cloud Computing*” 6th international conferences in Abu Dhabi in 2011

2. Yashpalsinh Jadeja, Kirit Modi,” *Cloud Computing - Concepts, Architecture and Challenges*” 2012 international conference in ICCEET.

3. Pankaj Arora, Rubal Chaudhry Wadhawan, Er. Satinder Pal Ahuja, “*Cloud Computing Security Issues in Infrastructure as a Service*” International Journal of Advanced Research in Computer Science and Software Engineering in 2012

4. Marios D. Dikaiakos, George Pall is, Dimitrios Katsaros, Pankaj Mehra, Athena Vakali, "*Cloud computing : Distributed Internet Computing for IT and Scientific Research*", IEEE Internet Computing, Published by the IEEE Computer Society, September/October 2009.

5. Cloud Computing Architecture http://communication.howstuffworks.com/cloudcomptingl.htm

6. http://en.wikipedia.orglwikilCloud_computing

7. Peeyush Mathur, Nikhil Nishchal, "*Cloud Computing: New challenge to the entire computer industry*", 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

8. Bhaskar Prasad Rimal, Eunmi Choi, *"A taxonomy and survey of cloud Computing systems*", 2009 Fifth International Joint Conference on INC, IMS and IDC, published by IEEE Computer Society.

9. Rongxing et al, "*Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing"*, ASIACCS'10, Beijing, China.

10. R. La'Quata Sumter, "*Cloud Computing: Security Risk Classification*", ACMSE 2010, Oxford, USA

11. Mladen A. Vouch, "*Cloud Computing Issues, Research and Implementations*", Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

12. Wenchaoet al, "*Towards a Data-centric View of Cloud Security*", CloudDB 2010, Toronto, Canada

13. Soren Bleikertz et al, "*Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds*", CCSW 2010, Chicago, USA.