CLOUD SECURITY: A CONCERNING ISSUE

Ms.Suman

Institute of Information Technology & Management, New Delhi (India)

Abstract

Cloud computing, a quickly developing information technology, has provoked the anxiety of the whole world. Cloud computing is Internet-based computing, whereby shared resources, software and information, are providing to digital devices and devices on-demand, like the electricity grid [1]. Cloud computing is the creation of the combination of traditional computing technology and network technology like grid computing, distributed computing parallel computing and so on. It purposes to paradigm a perfect structure with powerful computing capability through many relatively low-cost computing entity, and using the advanced business models like SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) to allocate the powerful computing capacity to end users' hands. This papermake known to the background and service model of cloud computing. This article also make known to the existing issues in cloud computing such as security, privacy, reliability and so on. This paperaims to identify the most vulnerable security threats in cloud computing, which will enable both end users and vendors to know about the key security threats associated with cloud computing.

Keywords—Cyber Security, Strategies, Cyber Security Measures

I. INTRODUCTION

Cloud computing is not a total naew concept; it is originated from the earlier large-scale distributed computing technology. However, it will be a subversion technology and cloud computing will be the third revolution in the IT industry, which represent the development trend of the IT industry from hardware to software, software to services, distributed service to centralized service. Cloud computing is also a new mode of business computing, it will be widely used soon. The core concept of cloud computing is reducing the processing burden on the users' terminal by constantly improving the handling ability of the “cloud”, eventually simplify the users' terminal to a simple input and output devices, and busk in the powerful computing capacity of the cloud on-demand. All of this is available through a simple Internet connection using a standard browser or other connection [2]. However, there still exist many problems in cloud computing today, a recent survey shows that data security and privacy risks have become the primary concern for people to shift to cloud computing [3].

II. CRITICAL EVALUATION

This Papercontained comprehensivestudied of research papers related with security and privacy threats in cloud computing. In some papers tools and models are planned to address security and privacy in cloud computing while in others some more security and privacy issues are known. After review the conclusion summarized in the following comparable table.

Lit. Ref	Context of Research	Problem Discuss	Technique Used
1.	Secure Provenance in Cloud Computing	Data forensics and post investigation in cloud computing	Bilinear pairing method
2.	Privacy Manager for Cloud Computing	Security, Privacy and user concerns	Privacy Manger tool developed to address security issues at user level.
3.	Addressing security issues in cloud computing.	Metering problem, Proof of work, Attack scenarios & data Backups	A simulation program that is coded JAVA, the program can simulate 1000 online shops, using different parameters deeds of the cloud computing server and online merchants are simulated. During the process of simulation, it was observed that the cloud computing server misses few inventory parts.
4.	Transparent Cloud Security	Cloud Security vulnerabilities and Security Attacks	The Transparent Cloud Protection System (TCPS)
5.	Implementation and research issues in cloud computing	SSH tunnels and VLANs, verifiable integrity and end-to-end service isolation through VPN	Virtual Computing Laboratory (VCL) Technology, open source
6.	Data Protection Models for Service Provisioning in the cloud	Users Concerns regarding privacy and security of Data	Data Protection Framework
7.	Data-centric cloud security	Secure Query Processing and Data Sharing. System Analysis and Forensics, Query Correctness Assurance.	DS 2 Platform
8.	Security Management of Virtual Machines	Managing virtual machine Images securely, Security Risks in image repository.	Image Management System that uses access control frame work, filters and scanners.

III. CLOUD SERVICES MODELS

A. Cloud Infrastructure as a service(IaaS): In this arrangement of practical environment for their system a supplier must be supply a different computing resources which include loading, processing unit. Client has flexile to achieve and switches a software mutilated to be applied and vary between different applications like operating system etc. There are different issues in IaaS such as [1]:

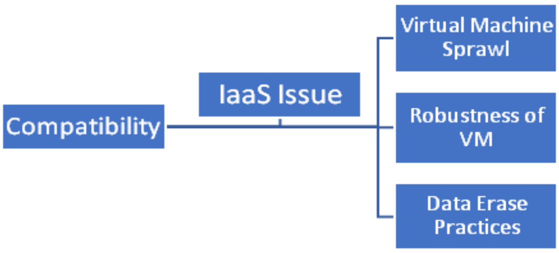

Figure 1: **IaaS Issues**

B. Cloud Platform as a service (PaaS): This software supplies client with the ability to establish and extended applications that are mainly positioned on tackle and programming languages promoted by the suppliers. In this the client has no control over the different association but has control over the extended applications. Examples of this class of services include Google App Engine, Windows Azure Platform and rack space. There are different issues in PaaS such as [1]:

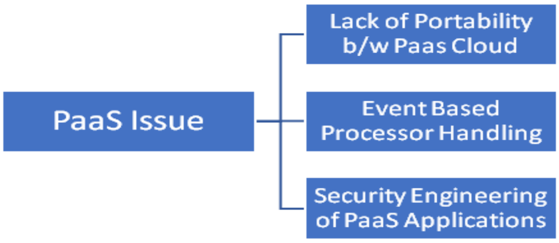
PaaS Issue
Lack of Portability b/w Paas Cloud
Event Based Processor Handling
Security Engineering of PaaS Applications

Figure 2: PaaS Issues

Types of PaaS: There are unlike types of PaaS such as [1]

- Application Delivers Only Environments
- Standalone Developments Environments
- Open Platform & Open Service
- Add on Development Possibility

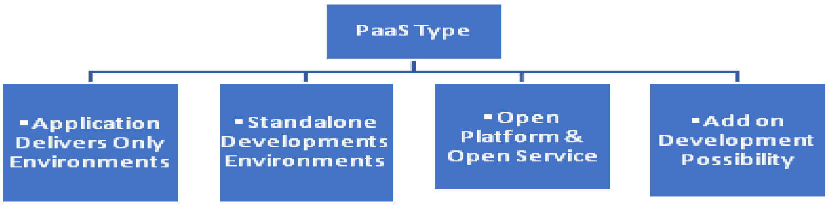
PaaS Type
▪Application Delivers Only Environments
▪Standalone Developments Environments
▪Open Platform & Open Service
▪Add on Development Possibility

Figure 3: PaaS Types

C. Cloud Software as a service (SaaS): This software supplies the ability to usage the applications which executed on cloud association. With the usage of standard interfaces like web browser or online(e-mail) client, these applications are accessible. SaaS applications are obtained from different devices like mobile, workstation from anywhere at any time.

D. Cloud Network as a service (NaaS): NaaS provides the capability to use the network services and inter-cloud network connectivity services. Improvement of possession allocation services include in view of network and computing resources. These types of services involved extensible, improved virtual private network.

IV. CLOUD DEPLOYMENT MODELS

A. Public Cloud: Public cloud describes the predictable meaning of cloud computing that is accessible, actual ways and means, which are accessible on internet from a minor party, which detached assets and charges its clients based on utility. Cloud association is possessed and accomplish by a supplier who suggest its retune to public domain. E.g. Google, Amazon, Microsoft offers cloud services via Internet. There are different benefits of public cloud model. The following figure shows some of those benefits:

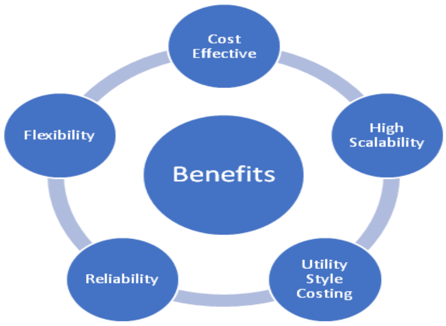

Figure 4: Benefits of Public Cloud

B. Private Cloud: Private cloud is a term used to donate a proprietary computing architecture provisioned services on corporate networks. Big enterprises usually used this type of cloud computing to permit their private network and information Centre administrators to effectively become in-house ‘service providers’ catering to customers within the corporation. Cloud association is establishing for anaggregation and managed by a third party under a service level agreement. Only single association preferred to operate via corporate cloud. There are advantages (benefits) of internal cloud model. The diagram given below depicts a few of these advantages (benefits):

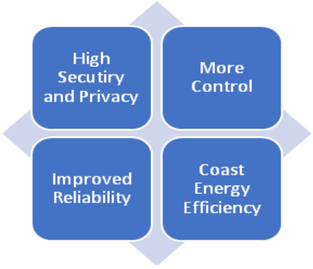

Figure 5: Benefits of Private Cloud

C. Hybrid Cloud: A hybrid cloud comprises assets from both corporate and public providers will become the demanded choice for enterprises. The hybrid cloud is a combination of both corporate cloud and public cloud. For example, for general computing enterprise could selects to make usage of external services, and its own data Centre's comprises it own data Centre's. Hybrid cloud model has number of advantages (benefits). The diagram given below reveals some of those advantages (benefits):

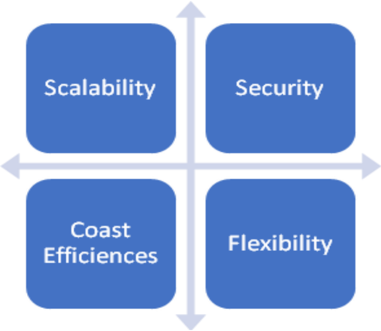

Figure 6: Benefits of Hybrid Cloud

V. SECURITY FEATURE IN CLOUD COMPUTING

There are several main challenges for building a secure band trustworthy cloud system: Outsourcing: Outsourcing brings down both capital expenses and effectiveexpenses for cloud customers. However, outsourcing also means that customers physically lose control on their data and tasks. The loss of control problem has become one of the root causes of cloud insecurity. To address outsourcing security issues, first, the cloud provider shall be trustworthy by providing trust and secure computing and data storage; second, outsourced data and computation shall be verifiable to customers in terms of Privacy, integrity, and other security services. In addition, outsourcing will potentially experience privacy violations, because sensitive data is out of the owner's control. Huge data and intense computation: Cloud computing is capable of handling mass data storage and intense computing tasks. Therefore, traditional security mechanisms may not suffice due to intolerablecalculation or communication overhead. For example, to verify the integrity of data that is remotely stored, it is impractical to hash the entire data set. To this end, new strategies and protocols are expected.

VI. CLOUD SECURITY CHALLENGES

There are some key security [4] challenges are:

A. Authentication: All through the internet data stored by cloud user is available to all unauthorized people. In future, the certified user and assistance cloud must have interchange ability administration entity.

B. Access Control: To check and promote only legalized users, cloud must have right access control policies. Such services must be adjustable, well planned, and their allocation is controlaccessibly. The approach governor provision must be integrated based on Service Level Agreement (SLA).

C. Policy Integration: There are many cloud providers such as Amazon, Google which are accessed by end users. Minimum number of conflicts between their policies because they user their own policies and approaches.

D. Service Management: In this different cloud providers such as Amazon, Google, comprise together to build a new composed services to meet their customers need. At this stage there should be obtain divider to get the easiest localized services.

E. Trust Management: The trust management approach must be developed as cloud environment is service provider and it should include trust negotiation factor between both parties such as user and provider. For example, to release their services provider must have little bit trust on user and users have same trust on provider.

VII. SECURITY ISSUES

The security of corporate data in the cloud is difficult, as they provide different services like Network as a service (NaaS), Platform as a service (PaaS), Software as a service (SaaS), Infrastructure as a service (IaaS). Each service has their own security issues [5]

A. Data Security: Data Security refers as a Privacy, integrity and availability. These are the major issues for cloud vendors. Privacy is defined as a privacy of data. Privacy are designed to prevent the sensitive information from unauthorized or wrong people. In this stores the encryption key data from enterprise C, stored at encrypted format in enterprise D. that data must be secure from the employees of enterprise D. Integrity is defined as the correctness of data, there is no common policies exist for approved data exchanges. Availability is defined as data is available on time.

B. Regulatory Compliance: Customers are eventually liable when the security and completeness of their own data is taken by a service provider. Traditional service providers more prone to outsource surveys and security certification. Cloud computing providers reject to endure the scrutiny as signalling so these customers can only make usage of paltry operations [6].

C. Data Locations: When users use, they probably won't know exactly where their data will have hosted and which location it will stored in. In fact, they might not even know what country it will be stored in. Service providers need to be asked whether they will accomplish to storing and alter data arbitration, and based on their customers will they make a fair accomplishment to follow local privacy requirement [7].

D. Privileged user access: Outside the resource data that is processed contains aninherent risk, as deploy services, avoid the mortal, consistent and human resource manage IT shops works on the house programs.

F. Trust Issue: Trust is also a major issue in cloud computing. Trust can be in between human to machine, machine to human, human to human, machine to human. Trust is revolving around declaration and confidence. In cloud computing, user stores their data on cloud storage because of trust on cloud. For example, people use Gmail server, Yahoo server because they trust on provider.

G. Data Recovery: It is defined as the process of bring back data that has been lost, corrupted or accident.

VIII. CONCLUSION & FUTURE WORK

Cloud computing is latest technology that is being widely used all over the world.Cloud services are used by both larger and smaller scale associations. Advantages of Cloud computing are huge. But it's a global phenomenon that everything in this world has advantages as well as disadvantages. 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 Once the association takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Security of the Cloud relies on trusted computing and cryptography. Number of cloud platforms are available now in educational as well as in enterprises circle. In this paper, it is discussed that issues related to data location, storage, security, availability and integrity. Establishing trust is the way to overcome these security issues as it establishes entities relationship quickly and safely. These issues mentioned above will be the research hotspot of cloud computing. There is no doubt that cloud computing has bright future.

REFERENCES:

[1]. http://www.servicearchitecture.com/articles/cloudcomputing/infrastructure_as_a_service_iaas.html

[2]. "Cloud computing is changing how we communicate".

[3]."How to gain comfort in losing control to the cloud".

[4]. Chandrahasan, R. Kalaichelvi, S. Shanmuga Priya, and L. Arockiam. "Research Challenges and Security Issues in Cloud Computing." International Journal of Computational Intelligence and Information Security 3.3 (2012): 42-48

[5]. B. R kandukuri, R. Paturi V, and A. Rakshit, “cloud security issues”,2009 IEEE International Conference on Services Computing, sep. 21-25, 2009, Bangalore, India, pp. 517-520

[6]. G. Hughes, D. Al-Jumeily & A. Hussain,” Supporting Cloud Computing Management through an Object Mapping Declarative Language”, 2010 Developments in E-systems engineering.

[7]. Feng-Tse Lin, Teng-San Shih, “Cloud Computing: The Emerging Computing Technology,” ICIC Express Letters Part B: Applications (ISSN: 2185-2766), v1, September 2010, pp. 33-38.