International Journal on Emerging Technologies (Special Issue on ICRIET-2016) **7**(2): 269-274(2016)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Security Issues in Cloud Computing: A Review

Sapna Parma and Gangambika Mangane
Department of Electronics and Communication Engineering,
BKIT Bhalki, INDIA-585328

(Corresponding author: Sapna Parma)

(Received 28 September, 2016 Accepted 29 October, 2016)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: In traditional computing, we install software programs on system (computer) update the hardware as per our requirements. Documents we create or save are stored in our computer. Documents are accessible on our own network, but they can't be accessed by computers outside the network. Using of cloud computing, the software programs aren't run from one's personal computer, but are rather stored on servers accessed via the Internet. Cloud Computing provides resources and capabilities of Information Technology (e.g., applications, storages, communication, collaboration, infrastructure) via services offered by CSP (cloud service provider). Cloud Computing has various characteristics as shared infrastructure, self-service, pay-per use model, dynamic and virtualized, elastic and scalable. Cloud computing in academic environment will be benefitted by every student and staff where lots of collaboration and safety of data is needed in academic. Academic has various departments and many semesters where lots of students need to access the computing a need for highly available up-to-date software and hardware is must. Cloud computing has the capacity of scaling and elasticity which is perfect for such an environment.

Keywords: Cloud Computing, Web service, Virtualization, Grid Computing, Virtual Computing Lab, higher education institutions

I. INTRODUCTION

Cloud computing growth has taken all the attention of various communities like researches, student, business, consumer and government organization The teaching method from black board to online is growing faster than ever With the increasing number in receiving education, a series of new problems have emerged. For example: As teaching methods change, the existing teaching-learning methods cannot meet demand; and with the constant expansion of education, the existing teaching facilities also need to constantly update. When Cloud Computing appears, it provides a new solution to establish a unified, open and flexible is provide a global forum for educators, researchers and IT professionals from education industry to pursue cloud computing initiatives, develop skill and share best practices for reducing operating costs while improving quality and access to education. In this way users do not need to buy a server, only need to purchase related "services" can create an efficient network teaching platform. Using of cloud computing in academicians in universities are not aware of benefits and characteristic of minimizing the cost of cloud computing. From an IT-management view, it radically reduces resource management costs —including electric power, cooling and system management personnel, while driving up the utilization of servers and software licenses, which in turn reduces purchasing requirements. The storage security at the cloud service providers data centres are also directly linked with the security of the cloud services. All the traditional security risks are thus applicable with added degree of potency in a cloud infrastructure which makes the ongoing success of cloud computing a quite challenging one. Confidentiality, availability and integrity are the generalized categories into which the security concerns of a cloud environment falls. Threats for a cloud infrastructure are applicable both to data and infrastructure .Different modes of data transfer and communication means (e.g. satellite communication) might need to take into account. Huge amount of data transfer is a common anticipation in a cloud environment, the communication technology used along with the security concerns of the adapted communication technology also becomes a security concern for the cloud computing approach. The broadcast nature of some communication technology is a core concern in this regard. Cloud environment is associated with both physical and virtual resources and they pose different level of security issues – having no sophisticated authentication mechanism to fully address the security threats is an existing problem for cloud computing. It has mainly resulted in the situations where grid computing has been taken as an embedded part of cloud computing. As the virtualized resources are highly coupled with a cloud infrastructure, intrusion related security concerns are of utmost priority as part of security issues.

Arbitrary intermittent intrusion needs to be monitored in the operational context of a cloud computing infrastructure where the severity of possibility for a virtual machine to be compromised is to be taken into account. Some authors have argued that using Internet technologies is not a must for cloud computing but the cost efficiency and globalization trends will enforce and motivate almost all the businesses to admit Internet and associated technologies to be the ultimate means towards cloud computing approach. As a result, total Internal related security concerns are anticipated to be automatically added on top of the cloud-specific security issues. Bringing portability is one of the Figure 2 illustrates the hierarchical arrangement based on which a cloud is perceived in the form of IaaS, PaaS and SaaS from any cloud end-user's viewpoint.

The security challenges for cloud computing approach are somewhat dynamic and vast. Data location is a crucial factor in cloud computing security Location transparency is one of the prominent flexibilities for cloud computing, which is a security threat at the same time – without knowing the specific location of data storage, the provision of data protection act for some region might be severely affected and violated

Benefits of Cloud Computing:

- Reduced implementation and maintenance costs
- Increased mobility for a global workforce
- Flexible and scalable infrastructures
- Quick time to market
- IT department transformation (focus on innovation vs. Maintenance and implementation)
- "Greening" of the data centre
- Increased availability of high-performance applications to small/medium-sized businesses

Cloud Platforms and Service Deployment Models

A. Essential Cloud Characteristics

- On-demand self-service
- Broad network access
- Resource pooling
- Location independence
- Rapid elasticity
- Measured service

B. Cloud Service Models

- Software as a Service (SaaS)
- Use provider's applications over a network
- Platform as a Service (PaaS)
- Deploy customer-created applications to a cloud
- Infrastructure as a Service (IaaS)
- Rent processing, storage, network capacity

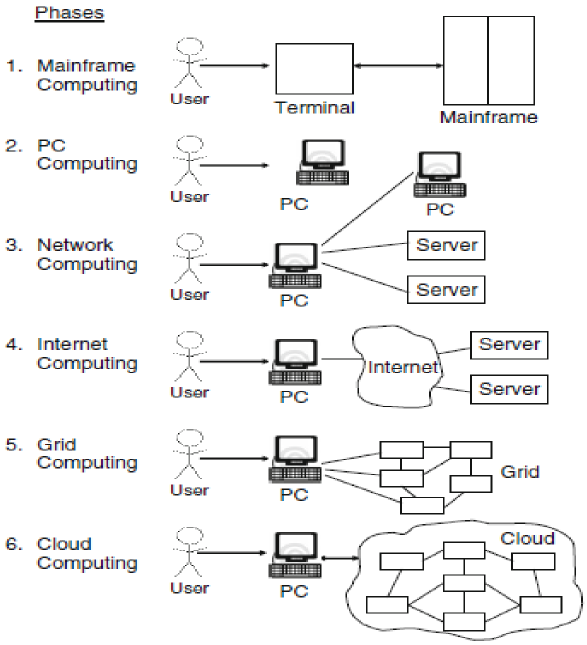


Fig. 1. Six paradigms phase.

C. Cloud Deployment Models:

- Public-Sold to the public, mega-scale infrastructure
- Private-enterprise owned or leased
- Hybrid-composition of two or more clouds
- Community-shared infrastructure for specific community

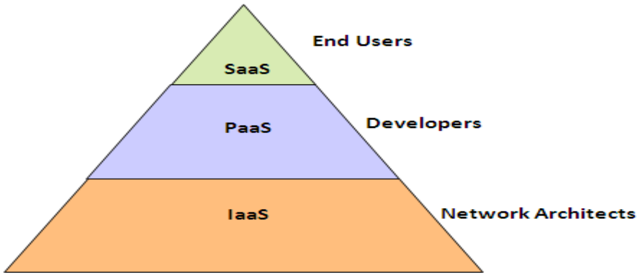
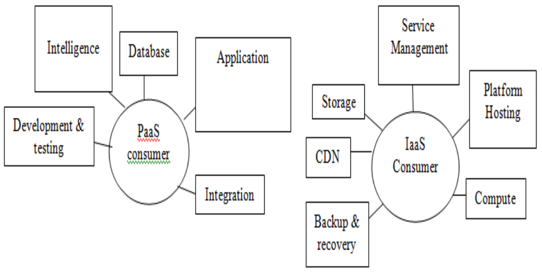
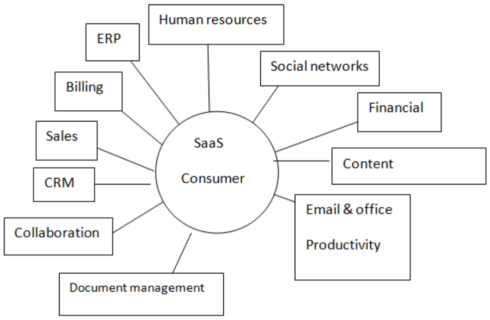


Fig. 2. Cloud computing service model.





Advantages of cloud computing:

(i) Lower cost computers for users: The high powered computer to run cloud computing web-based applications. Because the application runs in cloud, not on the desktop PC, that desktop PC does not need the processing power or hard disk demanded by the traditional desktop software. Hence the client computers in cloud computing can be lower priced, with smaller hard disks , less memory, more efficient processors. In fact ,a client computer in this scenario would not need a CD or DVD Drive, because no software program have to loaded and no document files need to saved.

(ii) Improved performance: lets look further at what results when a desktop PC does not have store and run a ton of software- based applications. With fewer bloated programs hogging the computer's memory users will see better performance for their PCs. Put simply; computers in cloud computing system will boot up faster and run faster because they will have fewer programs and processes loaded into memory.

(iii) Lower IT infrastructure costs: In a larger organization, the IT department could also see lower costs from the adoption of the cloud computing paradigm. Instead of investing in larger number of more powerful servers, the IT staff can use the computing power of the cloud to supplement or replace internal computing resources. Those companies that have peak needs no longer have to purchase equipment to handle the peaks are easily handled by computers and server in the cloud.

(iv) Fewer Maintenance Issues: Speaking of maintenance costs, cloud computing greatly reduces both hardware and software maintenance of organizations of all sizes, with less hardware necessary in the organization, maintenance costs are immediately lowered. As to software, maintenance, remember that all cloud apps are based elsewhere, so there's no software on the organizations computers for the IT staff to maintain. Its that simple

(v) Lower software costs: Then there's the issue of software cost, Instead of purchasing separate software packages for each computer in the organization, only those employees actually using an applications need access to that application in the cloud. Even if it costs the same to use web-based applications as it does similar desktop software, IT staffs are saved the cost of installing and maintain those programs on every desktops in the organizations.

(vi) Instant software updates: Another software-related advantage to cloud computing is that users are no longer faced with the choice between obsolete software and high upgrade costs. When the app is web-based, updates happen automatically and are available the next time the user locks into the cloud. Whenever you access a web based application, you're getting the latest version without needing to pay for or download an upgrade.

(vii) Storage capacity: Similarly, the cloud computing offers virtually limitless storage capacity. Consider that when your desktop or laptop PC is running out of storage space. Your computer's hard drive is peanuts compared to the hundreds of peta bytes (a million gigabytes) available in the cloud.

(viii) Latest version availability: Here another document-related advantage of cloud computing. When you edit a document at home, that edited version is what you see when you access the document at work, the cloud always hosts the latest version of your documents.

Disadvantages:

(i) Requires a constant internet connection: Cloud computing is, quite simply, impossible if you cannot connect to the internet, because you use the internet to connect to both your applications and documents, if you don't have an internet connection, you cannot access anything, even your documents. A dead internet connection means no work, period and in areas where internet connections are fewer or inherently unreliable, this could be a deal breaker, when you are offline cloud computing just work. These might be more significant disadvantage than you might thing. Sure you are used to a relative consistent internet connection both at home and at work, but where else do you like to use your computer? If you are used to working on documents on your deck, are while you are at a restaurant for lunch, or in your car, you won't be able to access your clouds based documents and applications-unless you have a strong internet connection at all those locations, of course, a lot of what is nice about portable computing becomes problematic when you are depending on web-based application.

(*ii*) Does not work will with low-speed connections: similarly, a low-speed internet connection, such as that found with dial-up services, makes cloud computing painful at best and often impossible, web-based apps often requires a lot of bandwidth to download, as do large documents. If you are laboring with low speed dial-up connection, it might take seemingly forever just to change for page to page in a document, a let alone launch feature rich cloud service.

(iii) Can be slow: Even on a fast connection, web-based application can sometimes slower that access a similar software program on your desktop PC, that is because everything about the program for the interface to the document you are working on, as to be send back and for your computers in the cloud, if the cloud servers happen to be backed up had that moment, or if the internet is having a slow day, you won't get the instantaneous access you are used to with desktop apps.

9vi) Store data might not be secure: it cloud computing all your data is stored on the cloud that is all well and god but how secure is the cloud? Can other, unauthorized users gain access to your confidently data? These are all important questions, and will worth further examination, to that end, read a head to the "The Security Conscious".

Security Issues in Cloud:

Cloud computing comes with numerous possibilities and challenges simultaneously. Of the challenges, security is considered to be a critical barrier for cloud computing in its path to success MK. Environment in terms of the customers' personal or business data security, the strategic policies of the cloud providers are of highest significance as the technical security solely is not adequate to address the problem. Trust is another problem which raises security concerns to use cloud service for the reason that it is Cloud users' personal data security is thus a crucial concern in a cloud computing directly related to the credibility and authenticity of the cloud service providers. Trust establishment might become the key to establish a successful cloud computing environment. The provision of trust model is essential in cloud computing as this is a common interest area for all stakeholders for any given cloud computing scenario .Trust in cloud might be dependent on a number of factors among which some are automation management, human factors, processes and policies . Trust in cloud is not a technical security issue, but it is the most influential soft factor that is driven by security issues inherent in cloud computing to a great extent DDoS (Distributed Denial of Service) attack is one common computing. Any security tools or other kinds of software used in a cloud environment might have security loopholes which yet major attack for cloud computing infrastructure well considered as part of security concerns for cloud in turn would pose security risks to the cloud infrastructure itself. The problem with third party APIs as well as spammers are threats to the cloud environment. As cloud computing normally means using public networks and subsequently putting the transmitting data exposed to the world, cyber attacks in any form are anticipated for cloud computing. The existing contemporary cloud based services have been found to suffer from vulnerability issues with the existence of possible security loopholes that could be exploited by an attacker. Security and privacy both are concerns in cloud computing due to the nature of such computing approach. The approach by which cloud computing is done has made it prone to both information security and network security issues. Third party relationship might emerge as a risk for cloud environment along with other security threats inherent in infrastructural and virtual machine aspects. Factors like software bugs, social engineering, human errors make the security for cloud a dynamically challenging one. Intrusion detection is the most important role in seamless network monitoring to reduce security risks. If the contemporary IDSs (Intrusion detection Systems) are inefficient, the resultant consequence might be undetected security breach for cloud environment .The facets from which the security threat might be introduced into a cloud environment are numerous ranging from database, virtual servers, and network to operating systems, load balancing, memory management and concurrency control. Data segregations and session hijacking are two potential and unavoidable security threats for cloud users. One of the challenges for cloud computing is in its level of abstraction as well as dynamism in scalability which results in poorly defined security or infrastructural boundary. Privacy and its underlying concept might significantly vary in different regions and thus it may lead to security breach for cloud services in specific contexts and scenarios. Data loss and various bonnets can come into action to breach security of cloud servers. Besides, multi-tenancy model is also an aspect that needs to be given attention when it comes to security. Security in the data-centres of cloud providers are also within the interests of security issues, as a single physical server would hold many clients' data making it a common shared platform in terms of physical server or operating system.

Major challenges faced by cloud computing:

The specific challenges differ for the three cloud delivery models, but in all the cases the difficulties are created by the very nature of utility computing, which is based on resource sharing and resource virtualization and requires a different trust model than the ubiquitous user-centric model we have been accustomed to for a very long time. The most significant challenge is security, gaining the trust of a large user base is critical for the future of cloud computing.

It is unrealistic to expect that a public cloud will provide a suitable infrastructure, healthcare applications, and others will most likely to be hosted by private clouds .many real time applications will probably still be confined to private clouds. Some applications may be best served by a hybrid cloud setup; such applications could keep sensitive data a on a private cloud and use a public cloud for some of the processing. The Saas model faces similar challenges as other online services required to protect private information, such as financial or healthcare services. Data in storage is most vulnerable to attack, so special attention should be devoted to the protection of storage servers. Data replication necessary to ensure continuity of service in case of storage system failure. Data encryption may protect data in storage, but eventually data must be decrypted for processing, and then it is exposed to attack. The IaaS model is far the most challenging to defend against attacks. The next major challenge is related to resource management on a cloud and about the interoperability and standardization. Any systematic rather than ad hoc resources management strategy requires the existence of controllers tasked to implement

Algorithms

An Approach For Data Storage Security In Cloud Computing

Cloud computing is the most demanding and emerging technology throughout the world. Cloud computing is an internet based technology. Cloud computing is a new paradigm that combines several computing concepts and technology of the internet creating a plot form for more agile and cost effectively business applications and IT infrastructure.

Cloud computing unavoidably posses' new challenging security threats for number of reasons.

(i) Unauthenticated person do not attack the authorized file

(ii) Avoids Collusion attacks

(iii) A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against malware or bypass access controls. There are several different types of spoofing attacks that malicious paries can use to accomplish this.

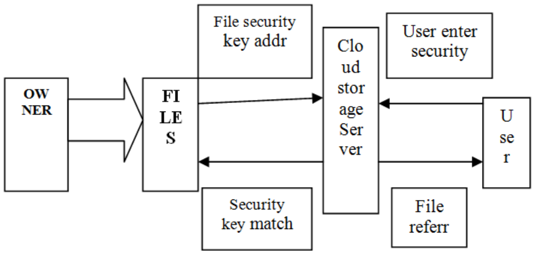
Problem Statement

Cloud computing unavoidable poses new challenging security threats for number of reasons.

(i) Data stored on cloud servers is not completely secure from infection. While popular cloud services such as Google Docs are equipped with virus scanning software, there is still the possibility of an internal or external attack affecting your data.

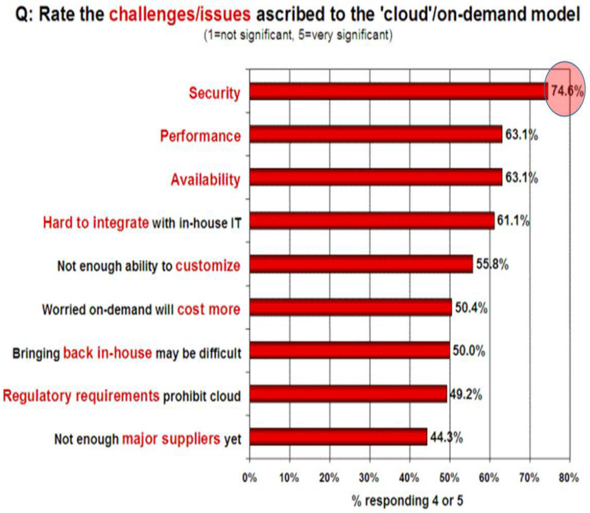
(ii) The data stored in the cloud may be frequently updated y the users, including insertion, deletion, modification, appending, recording, etc. to ensure storage correctness under dynamic data update, distributed protocol is used.

Fig. shows architecture of secured data storage. Data storage in a cloud is a process where owner stores his data and files through a cloud storage provider into a set of cloud servers. At the time of file storage security key is used to secure the data and file from the unauthorised persons and then safely stored in the cloud. File cannot be accessed by any unauthorised person or the person who entering unmatching security key.



A Security Approach For data Migration In Cloud Computing:

Cloud computing is now days emerging field because of its performance, high availability, low cost. Data storage is the main future that cloud service provides to the companies to store huge amount of storage capacity. But still many companies are not ready to implement cloud computing technology due to lack of proper security control policy and weakness in protection which lead to many challenge in cloud computing. Main objective of this paper are 1) To prevent the data access from unauthorized access. 2) Proposed scheme perfectly stores the data and identifies the any tamper at the cloud server. 3) It performs some of the tasks like data updating, deleting, appending. This paper also provides a process to avoid Collusion attacks of server modification by unauthorized user.Data migration to a cloud computing environment is in many ways +an exercise in risk management. Both qualitative and quantitative factor apply in an analysis. Data security is another important research topic in cloud computing. Since server providers typically do not have access to the physical security system of data centres. Remote attestation typical requires a Trusted Platform Module (TPM) to generate non-forgeable system summary as the proof of system security. Recent has been devoted to designing efficient protocols for trust establishment and management.



VI. CONCLUSION

Cloud computing can be utilized for many applications and it has the capability to deliver the data to users any time irrespective of where the data are stored actually. Securing the data is the important concept as sometimes the data may be more private.

In this paper we have discussed some of the security issues and data migration approaches in the cloud computing. The data needs more sufficient protocols to provide security to the private data.

REFERENCE

[1] Virendra Singh Kushwah*, Aradhana Saxena "A Security approach for Data Migration in Cloud computing", *International Journal of Scientific and Research Publications,* Volume **3**, Issue 5, May 2013 1 ISSN 2250-3153

[2] Deepanchakaravarthi Purushothamanand Dr.Sunitha Abburu, "an Approach for Data Storage Security in CloudComputing", *IJCSI International Journal of Computer Science* Issues, Vol. **9**, Issue 2, No 1, March 2012ISSN (Online): 1694-0814.

[3] Kamal SrivastavaAtul Kumar,"A New Approach of CLOUD: Computing Infrastructure on Demand"

[4] Monjur Ahmed1 and Mohammad Ashraf Hossain, "Cloud computing and security issues in theCloud", *International Journal of Network Security & Its Applications (IJNSA),* Vol. **6**, No.1, January 2014.

[5]Ajith Singh. N, M. Hemalatha,**"**Cloud Computing for Academic Environment", *International Journal of Information and Communication Technology Research,* Volume **2** No. 2, February 2012 ISSN 2223-4985.