



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

To Study the Impact of Security Issues in Cloud Computing

Sonali Nemade¹, Sunayna Shivthare², Deepashree Mehendale³, Reshma Masurekar⁴,

Assistant Professor, Dept. of Computer Science, Dr. D. Y. Patil A.C.S College, Pimpri, Pune, India¹

Assistant Professor, Dept. of Computer Science, Dr. D. Y. Patil A.C.S College, Pimpri, Pune, India²

Assistant Professor, Dept. of Computer Science, Dr. D. Y. Patil A.C.S College, Pimpri, Pune, India³

Assistant Professor, Dept. of Computer Science, Dr. D. Y. Patil A.C.S College, Pimpri, Pune, India⁴

ABSTRACT: Cloud computing is an Internet based computing that provides the capability to user to store and process data in either privately owned or third party data centres. It enables the organizations to manage their business efficiently. Cloud computing framework allows business to save expenses. Cloud computing has played a major role in solving the inefficiencies problem in organizations and increase the growth of business thus helping the organizations to be stable in market. Cloud computing has been considered as an innovative way to improve business. Using Cloud computing cost of hardware and software can be reduced more effectively. Recently, the customers of cloud computing have no source for reliability and authentication of their confidential data. Business organizations need to be alert against the attacks to their cloud storage. This paper discusses about the different delivery and development models, benefits and the security issues of cloud computing.

KEYWORDS: -Cloud computing, business, third party, cloud service, benefits, security.

I. INTRODUCTION

Cloud computing is a new technology. It is a way to increase the capacity and add capabilities dynamically without any investment in new infrastructure. The main objective is to provide secure, quick, convenient data storage and net computing service. It is the development of parallel computing, distributed computing, grid computing, and is the combination and evolution of Virtualization, Utility computing, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). Cloud describes web as a space where computing has been preinstalled and exist as a service; data, operating systems, applications, storage and processing power exist on the web ready to be shared.

Cloud computing provides different activities such as the use of social networking sites and other interpersonal computing. Most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. Different cloud services are available like webmail, online file and business applications. It provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud storage specifies the storage on cloud with almost inexpensive storage and backup option for small enterprise. The actual storage location may be on single storage environment or replicated to multiple server storage based on importance of data. An example of cloud computing is Yahoo email, Gmail, or Hotmail etc. To use this services there is no need of server or a software but the consumer needs only an Internet connection. The server and email management software is all on the cloud (internet) and is totally managed by the cloud service provider.

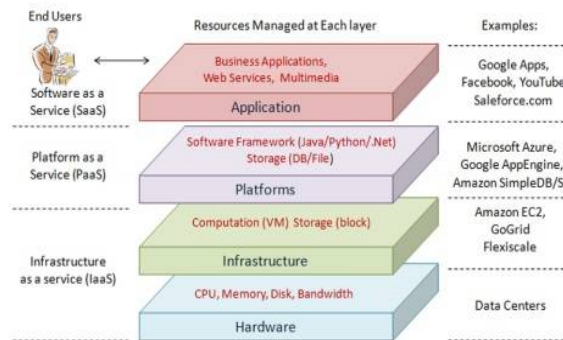
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

II. CLOUD COMPUTING ARCHITECTURE:



Cloud Computing Architecture

2.1 Client Platform:

The cloud clients are the thick, thin and ultra thin clients. The interaction between client platforms and the cloud data storage is via an application (middleware), a web browser.

2.2 Cloud Storage:

Cloud storage is an internet or online storage where data is stored and available to clients. Cloud storage is commonly public cloud, private cloud, community cloud or a hybrid cloud.

2.3 Cloud Delivery Models:

2.3.1 Software as service (SaaS):

Software as service. It is also known as delivery model where the software and the data which is associated with it is hosted over the cloud environment by third party and that third party is called cloud service provider, like Gmail account. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). SaaS provides application services on demand such as email, conferencing software, and business applications such as ERP, CRM, and SCM. SaaS users have less control over security among the three fundamental delivery models in the cloud.

2.3.2 Platform as service(PaaS):

In this, we can use Web-based tools to develop applications so they run on systems software which is provided by another company, like Google App Engine. PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher level services. PaaS facilitates deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers. PaaS depends on a secure and reliable network and secure web browser. PaaS application security comprises of two software layers: Security of the PaaS platform itself (i.e., runtime engine), and Security of customer applications deployed on a PaaS platform.

2.3.3 Infrastructure as service (IaaS):

IaaS provides abundant resources such as servers, storage, networks, and other computing resources in the form of virtualized systems, which are accessed through the Internet. Users are entitled to run any software with full control and management on the resources allocated to them. With IaaS, cloud users have better control over the security compared to the other models as long there is no security hole in the virtual machine monitor. They control the software running in their virtual machines, and they are responsible to configure security policies correctly. The effectiveness provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer has control over operating systems, storage, deployed applications, and possibly limited control of networking components.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

2.4 Cloud Networking

In general, the cloud network layer must offer:

2.4.1 Low latency – Ensuring users have uninterrupted access to data and applications.

2.4.2 Agile network – On-demand availability of resources involves the capability to move rapidly and efficiently among servers and perhaps even within clouds.

2.4.3 Network security – Security is always vital but when you are working with multi-tenancy, it becomes much more crucial because you're now dealing with isolating multiple customers from each other.

III. CLOUD COMPUTING DEVELOPMENT MODELS

3.1 Public model

In public cloud, the services are offered to everyone in general public over Internet. These services are generally free. These services are provided and shared with other organizations by third party service providers. Usually the service providers have their own policy, value, costing. Examples of public cloud services are email services and photo storage services.

3.2 Private Model

The cloud infrastructure is operated for a private organization. It may be managed by the organization or a third party, and may exist on premise or off premise. Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise data centre.

3.3 Hybrid Model

The cloud infrastructure is a composition of two or more clouds (private or public) that remain unique entities, but are bound together by standardized or proprietary technology, that enables data and application portability (e.g., cloud bursting for load balancing between clouds). Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds.

IV. BENEFITS OF CLOUD COMPUTING IN BUSINESS

Cloud computing helps businesses to maximize their IT return on investments. In the last 18 months the number of users using cloud computing has increased with 27%. Businesses use a service that is provided by a third party without building their own infrastructure. The benefits provided are as follows:-

4.1 Cost reduction-Rather than buying expensive systems for businesses the cost can be reduced by using resources of cloud computing service provider.

4.2 Flexibility- Cloud computing allows employees to be more flexible in their work timings. They are able to work from home by making use of virtual office. It also allows flexibility as your needs change.

4.3 Mobility and agility- Users of cloud services can access their accounts from anywhere they want and from number of devices. They have to sign in using their account. This is possible because data that is stored in the cloud is online and they are not bundle on the system where they were created.

4.4 Easier update-The responsibility of the system up gradation is of cloud vendors and not of the customer. New solutions that appear in the market are made available to the customers by the cloud vendors. Because the competition is high, vendors need to find ways of keeping their business up to date with the latest technologies.

4.5 Backup and recovery: Customers can store their data on clouds in low cost. The benefits of using this service are: data is stored in multiple copies; the customer has to pay only for what he is using; data is encrypted for security reasons there are multiple copies of the data; data is kept safe because it is encrypted and it is integrating with the archiving software that already exists.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

4.6 Disaster recovery: The benefits of this service are: data is secured offsite; multiple copies are done automatically; the files are back-up and restore. Development and test is created for customers that need to develop applications and also to test them. The customer that is using this service will have instant access to new resources, the machine used can be configured for the customer's needs and the customer is paying only what he is using.

V. SECURITY ISSUES IN BUSINESS ENVIRONMENT

Organisations use the cloud in a variety of different service models such as SaaS, PaaS, IaaS and different deployment models such as private, public and hybrid. The security issues of cloud fall into two categories viz:- security issues faced by cloud providers and security issues faced by the customers. The provider should make sure that their infrastructure is secure and the clients' data and applications are protected, while the user must focus on use of strong passwords and authentication measures. Some of the security issues faced are as follows:-

5.1 Hacked interfaces and APIs

Practically every cloud service and application relies on APIs. Interfaces and APIs are used to manage and interact with cloud services. The security and availability of cloud services from authentication and access control to encryption and activity monitoring depend on the security of the API. Risk increases with third parties that rely on APIs and build on these interfaces, as organizations may need to expose more services and credentials. Weak interfaces and APIs expose organizations to security issues related to confidentiality, integrity, availability, and accountability.

5.2 Account hijacking: -

Phishing, fraud, and software exploits are still successful, and cloud services add a new dimension to the threat because attackers can monitor on activities, manipulate transactions, and modify data. Attackers may also be able to use the cloud application to launch other attacks. Organizations should prohibit the sharing of account credentials between users and services, as well as enable multifactor authentication schemes where available.

5.3 Malicious insiders

The insider threat has many faces such as a current or former employee, a system administrator, a contractor, or a business partner. In a cloud environment an insider can destroy whole infrastructures or manipulate data. Systems that depend solely on the cloud service provider for security, such as encryption, are at greatest risk.

5.4 Permanent data loss

In the cloud environment reports of permanent data loss due to provider error have become extremely rare. But malicious hackers have been known to permanently delete cloud data to harm businesses, and cloud data centers are as vulnerable to natural disasters as any facility. Cloud providers recommend distributing data and applications across multiple zones for added protection. Adequate data backup measures are essential, as well as adhering to best practices in business continuity and disaster recovery. Daily data backup and off-site storage remain important with cloud environments.

5.5 Shared Technology Shared danger:-

Vulnerabilities in shared technology have a significant threat to cloud computing. Cloud service providers share infrastructure, platforms, and applications, and if a vulnerability arises in any of these layers, it affects everyone.

VI. CONCLUSION

Cloud Computing is an emerging trend of reliable service over the Internet. It has many advantages when used in business environment. In this paper we have discussed the benefits of cloud computing in business environment. With benefits cloud also has some security issues. Both the users and cloud providers are equally responsible for the security breaches. The security issues should be handled by both the providers and users. Some of the security issues discussed



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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

focuses that there is a need to identify and solve the security problems and approaches arising in cloud in terms of loss of control, lack of trust and multi-tenancy problems.

REFERENCES

1. Ricardo vilaca, Rui oliveira 2009. Clouder: A Flexible Large Scale Decentralized Object Store. Architecture Overview. Proceeding of WDDDM '09
2. Michael Miller. 2009. Cloud Computing-Web Based Application that change the way you collaborate online. Publishing of QUE, 2nd print.
3. R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.
4. B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.
5. 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.
6. Chun-Ting Huang, Zhongyuan Qin, C.-C. Jay Kuo., "Multimedia Storage Security in Cloud Computing: an Overview" 978-1-457701434-4/11/\$26.00,IEEE,2011.
7. Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, 16, 108-114. doi:10.1016/j.istr.2011.08.006 [8]
- Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), 257-259.
9. Arshad, J, Townsend, P. and Xu, J. (2013).A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29, 416-428. doi:10.1016/j.future.2011.08.009