INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY STUDIES
SPECIAL ISSUE ON ADVANCEMENT IN FIELD OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

Vol. 4, Special Issue 8, February, 2018 ISSN (Online): 2454-8499
Impact Factor: 1.3599(GIF), 0.679(IIFS)

A Study of Cloud Computing and Security Concerns

[1]Prof. Alka B. Mhetre, [2]Prof. Deepali D.Chaudhari
[1, 2]Rajmata Jijau ACS College,LandewadiBhosari,Pune-39
alkamhetre@gmail.com, deep.d.chaudhari@gmail.com

Abstract :

Cloud computing is currently the axiom in IT industry, and many are curious to know what cloud computing is and how it works.

It is very stimulating and tempting technology which contributes multiple services to users over internet. It's a distributed resource environment and it is used to store the data, due to that security becomes main hurdle in deployment of cloud environment. In this paper we discussed various security concerns like Data Breaches, Hijacking of accounts, Insider Threat, Abuse of cloud services, Data loss, Malware Injection.

Keywords: Cloud Computing, Security, Hijacking of accounts, Insider Threat, Abuse of cloud services, Data loss, Malware Injection.

Introduction:

Cloud Computing can be defined as delivering computing power(CPU, RAM, Network Speeds, Storage OS software) a service over a network (usually on the internet) rather than physically having the computing resources at the customer location.

Cloud computing Uses:

- Create new apps and services
- Store, back up and recover data
- Host websites and blogs
- Stream audio and video
- Deliver software on demand
- Analyse data for patterns and make predictions
- Lower IT infrastructure and computer costs for users
- Improved performance
- Fewer Maintenance issues
- Instant software updates
- Improved compatibility between Operating systems
- Performance and Scalability
- Increased storage capacity
- Increase data safety

Types of Clouds

There are four different cloud models that you can subscribe according to business needs:

1. **Private Cloud:** Here**,** computing resources are deployed for one particular organization. This method is more used for intra-business interactions. Where the computing resources can be governed, owned and operated by the same organization.
2. **Community Cloud:** Here**,** computing resources are provided for a community and organizations.
3. **Public Cloud:** This type of cloud is used usually for B2C (Business to Consumer) type interactions. Here the computing resource is owned, governed and operated by government, an academic or business organization.

Vol. 4, Special Issue 8, February, 2018 ISSN (Online): 2454-8499
Impact Factor: 1.3599(GIF), 0.679(IIFS)

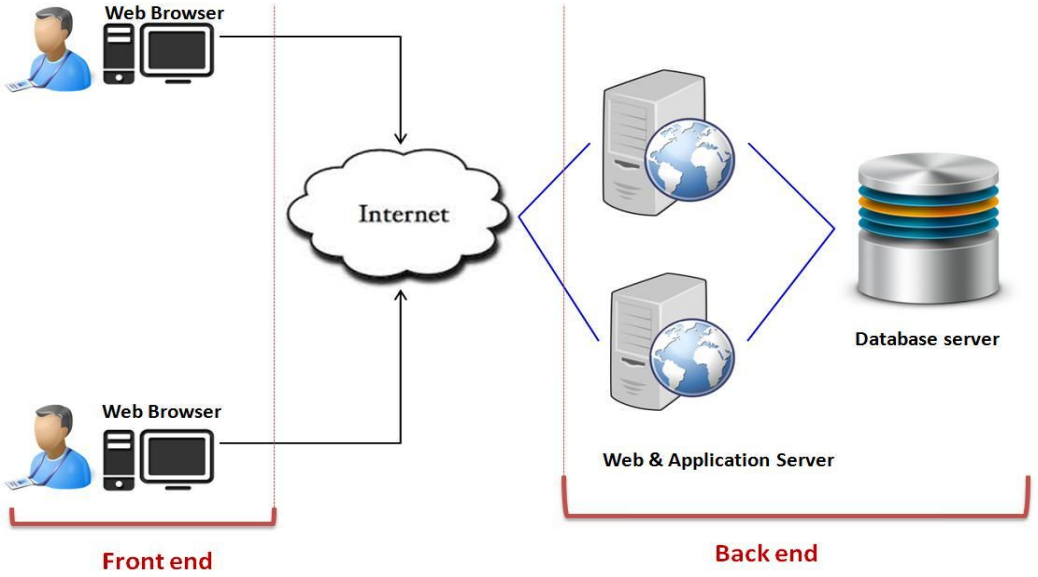
4. **Hybrid Cloud:** This type of cloud can be used for both type of interactions - B2B (Business to Business) or B2C (Business to Consumer). This deployment method is called hybrid cloud as the computing resources are bound together by different clouds.

Cloud Computing Services

The three major Cloud Computing Offerings are

- **Software as a Service (SaaS)**
- **Platform as a Service (PaaS)**
- **Infrastructure as a Service (IaaS)**

Cloud Computing Architecture



Cloud computing architecture refers to the components and **subcomponents** required for cloud computing. These components typically consist of a front end platform (fat client, thin client, **mobile** device), back end platforms (servers, storage), a cloud based delivery, and a network (Internet, Intranet, **Intercloud**).

Cloud Computing Security Concerns:

1. Hijacking of Accounts

Attackers now have the ability to use your (or your employees') login information to remotely access sensitive data stored on the cloud; additionally, attackers can falsify and manipulate information through hijacked credentials.Other methods of hijacking include scripting bugs and reused passwords, which allow attackers to easily and often without detection steal credentials.

2. Insider Threat

An attack from inside your organization may seem unlikely, but the insider threat does exist. Employees can use their *authorized* access to an organization's cloud-based services to misuse or access information such as customer accounts, financial forms, and other sensitive information.

3. Abuse of Cloud Services

The expansion of cloud-based services has made it possible for both small and enterprise-level organizations to host vast amounts of data easily. However, the cloud's unprecedented storage

Vol. 4, Special Issue 8, February, 2018 ISSN (Online): 2454-8499
Impact Factor: 1.3599(GIF), 0.679(IIFS)

capacity has also allowed both hackers and authorized users to easily host and spread malware, illegal software, and other digital properties.

In some cases this practice affects both the cloud service provider and its client. For example, privileged users can directly or indirectly increase the security risks and as a result infringe upon the terms of use provided by the service provider.

These risks include the sharing of pirated software, videos, music, or books, and can result in legal consequences in the forms of fines

4. Data Loss

Data on cloud services can be lost through a malicious attack, natural disaster, or a data wipe by the service provider. Losing vital information can be devastating to businesses that don't have a recovery plan. Amazon is an example of an organization that suffered data loss by permanently destroying many of its own customers' data in 2011.

Google was another organization that lost data when its power grid was struck by lightning four times. Securingdata means carefully reviewing provider's back up procedures as they relate to physical storage locations, physical access, and physical disasters.

5. Malware Injection

Malware injections are scripts or code embedded into cloud services that act as "valid instances" and run as SaaS to cloud servers. This means that malicious code can be injected into cloud services and viewed as part of the software or service that is running within the cloud servers themselves.Once an injection is executed and the cloud begins operating in tandem with it, attackers can eavesdrop, compromise the integrity of sensitive information, and steal data.

Conclusion:

Cloud computing is modern technology that is being widely used all over the world.

Once theorganization takes the decision to move to the cloud, itloses control over the data. Thus, the amount of security needed to secure data. Securityof theCloud relies on trusted computing and cryptography.

In this paper, we have discussed the issues related to security. There is no doubt that cloud computing has bright future. The simple conclusion is that the cloud comes with a unique set of characteristics that make it more vulnerable.

References:

1. www.incapsula.com
2. A review of cloud computing security issues ISSN: 22311963 @AJAET
3. www.guru99.com