2. Cloud Computing Security

Prof. Salunke Ravindra B.
Head, Department of Computer Application,
Dada Patil Mahavidyalaya, Karjat, Dist Ahmednagar.

Abstract

It is no secret that cloud computing is becoming more and more popular today and is ever increasing in popularity with large companies as they share valuable resources in a cost effective way. This paper primarily aims to highlight the major security issues existing in current cloud computing environments and ways in which security threats can be a danger to cloud computing and how they can be avoided.

Keywords- Cloud Computing, Security, threats, danger, valuable, effective

1. Introduction

Cloud computing is internet based where shared resources; software and information are provided to computers and other devices on-demand. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are both well known examples. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. Downtime of Amazon's S3 is such an example. [1] the basis for this infrastructure software. Some PaaS offerings have a specific programming language or API. For example, Google AppEngine is a PaaS offering where developers write in Python or Java. EngineYard is Ruby on Rails. Sometimes PaaS providers have proprietary languages like force.com from Salesforce.com and Coghead, now owned by SAP. Infrastructure as a Service (IaaS) is the delivery of hardware (server, storage andnetwork), and associated software (operating systems virtualization technology, file system), as a service. It is an evolution of traditional hosting that does not require any long term commitment and allows users to provision resources on demand.

2. Method

Cloud computing paradigm also introduces some key security challenges. Some of these key security challenges are:

2.1 DDOS (Distributed denial of service): Cloud computing and web services run on a network structure so they are open to network type attacks. If a user could hijack a server then the hacker could stop the web services from functioning and demand a ransom to put the services back online. To stop these attacks the use of syn cookies and limiting users connected to a server all help stop a DDOS attack. Another such attack is the man in the middle attack. If the secure sockets layer (SSL) is incorrectly configured then client and server authentication may not behave as expected therefore leading to man in the middle attacks. [3]

2.2 Network sniffing: With a packet sniffer an attacker can capture sensitive data if unencrypted such as passwords and other web service related security configuration such as the UDDI (Universal Description Discovery and Integrity), SOAP (Simple Object Access Protocol) and WSDL (Web Service Description Language) files. Port scanning is also another threat which can be used by an attacker. Port 80 is always open due to it being the port that the web server sits on. However this can easily be encrypted andas long as the server software is configured correctly then there should be no intrusion. [4]

2.3 SQL injection: In this a hacker can use special characters or terms to return unintended data For example, strings that may end up in a WHERE clause of an SQL statement may be tricked into including more information. For instance a parameter value of X' or 1=1 may cause a whole table to be returned as 1=1 is always seen as true.

2.4 Cross site scripting: In this technique inserting code into a field or URL that gets executed hands over control or sensitive data to the attacker. Successful cross site scripting attacks can lead to buffer overflows, DOS attacks, inserting spyware and malicious code into visiting browsers and violation of user privacy. [4]

2.5 Compromised Servers: In a cloud computing environment, users do not even have a choice of using physical acquisition toolkit. In a situation, where a server is compromised; they need to shut their servers down until they get a previous backup of the data. This will further cause availability concerns.

3. Result

Cloud computing environment is generally assumed as a potential cost saver as well as provider of higher service quality. Security, Availability, and Reliability are the major quality concerns of cloud service users. Gens et. al. [5], suggests that security in one of the prominent challenge among all other quality challenges.

3.1 Loss of Governance: in using cloud infrastructures, the client necessarily cedes control to the Cloud Provider (CP) on a number of issues which may affect security. At the same time, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defence.[6]

3.2 Lock-In: there is currently little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability. This can make it difficult for the customer to migrate from one provider to another or migrate data and services back to an in-house IT environment. This introduces a dependency on a particular CP for service provision, especially if data portability, as the most fundamental aspect, is not enabled.[6]

3.3 Data Protection: cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated clouds.

4. Disscussion

Cloud computing is no doubt a fantastic technology and continues to grow in popularity and more and more companies are investing in a cloud for their company. Cloud computing presents IT organizations with a fundamentally different model of operation, one that takes advantage of the maturity of web applications and networks and the rising interoperability of computing systems to provide IT services.

To secure the structure that is to be implemented we need to come up with a security analysis process. This will include what type of assets there are to be protected from a company point of view, what threats can be run against a company, what countermeasures can be put in place to stop these attacks from taking place. When dealing with assets we need to look at what assets are we trying to protect and what properties of these assets must be protected. For dealing

with threats we must look at what kind of attacks can be launched against a company with this type of structure Few security measures that can be adopted are:

4.1 Long-term Viability: Service providers must ensure the data safety in changing business situations such as mergers and acquisitions. Customers must ensure data availability in these situations. Service provider must also make sure data security in negative business conditions like prolonged outage etc.

4.2 Regulatory Compliance: Traditional service providers are subjected to external audits and security certifications. If a cloud service provider does not adhere to these security audits, then it leads to a obvious decrease in customer trust.

4.3 Recovery: Cloud service providers must ensure the data security in natural and man-made disasters. Generally, data is replicated across multiple sites. However, in the case of any such unwanted event, provider must do a complete and quick restoration.

5. Conclusion

In an emerging discipline, like cloud computing, security needs to be analyzed more frequently. With advancement in cloud technologies and increasing number of cloud users, data security dimensions will continuously increase. Cloud computing offers real alternatives to IT departments for improved flexibility and lower cost. Markets are developing for the delivery of software applications, platforms, and infrastructure as a service to IT departments over the "cloud". These services are readily accessible on a pay-per-use basis and offer great alternatives to businesses that need the flexibility to rent infrastructure on a temporary basis or to reduce capital costs. Open source clouds such as the Ubuntu cloud offer smaller businesses the chance to try out the benefits of cloud computing. Once cloud computing technology has been improved and network technology has also been improved a real golden opportunity exists for the future. Each cloud solution must however be tailored to each company but they can all benefit from the numerous advantages the technology brings to the table. The technology is still in early days but already there is much hype surrounding the technology and with impressive results so far this will continue to grow. [7]

6. Acknowledgement

I convey my honest thanks to MrsSudhalakshmiIyer Lecturer of Arihant Education Foundtion, Pune for providing me the leadership and conveniences for this paper I also extend