Does Cloud Computing pose a serious security threat or not?

Fahad Zahrani[1]

[1.] Computer department in technical institute -Jeddah, Saudi Arabia - email: Fahad-zahrani@hotmail.com

Abstract: The goal of this research paper is to uncover the risks of usage of remote services. General concepts and tasks of cloud computing systems are described. In the main part the threats of cloud computing are revealed along with methods and practical recommendations for avoiding potential pitfalls. Based on the analyzed data, a conclusion is made, stating that ignoring some of the recommendations may present serious security issues in the process of remote systems' usage.

[Fahad Zahrani. **Does Cloud Computing pose a serious security threat or not?** *J Am Sci* 2015;11(1s):40-43]. (ISSN: 1545-1003). http://www.jofamericanscience.org. 6

Keywords: cloud, computing, technologies, security, models, service, resource, analysis.

1. Introduction

Over the last decade the concepts of computing have changed dramatically. Computers were originally popularized as desktop devices for solving vast numbers of problems, but later, when the demand started to lean towards laptops and mobile devices and everyday problems became more and more complicated, remote storage and computing services were introduced. Users no longer need large capacity storage devices or over-the-top CPUs to cope with large amounts of data, manage databases, render animations and perform other resource-consuming activities. Desktop devices, laptops and mobile devices became a gateway to endless computational capabilities that are provided to users remotely. The probability of the appearance of such services was expressed in the 1960s. The idea of organizing computations as a public utility has been expressed many years before it has actually been implemented and metaphorically called "computations in the cloud" or "cloud computing" (Cloud Security Alliance, 2010)

2. Cloud Computing Basics

2.1 Basic concepts

The National Institute of Standards and Technology defines the term "cloud computing" as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [citation]. The standard also defines a number of characteristics, outlining the major features of the remote computation paradigm (Treadway, 2009)

One of the main features is the on-demand structure of providing services. Resources are managed without human interference. Scalability ensures that the system always has enough resources to accomplish the task at hand – additional capabilities are provided at peak moments (e.g. services which have more clients at certain time of the day). Dynamic assignation and scalability lead the way to one of the key principles of remote computation services: for a customer, the capabilities of the system are unlimited and can be purchased and accessed at any time. resources are storage, network bandwidth, virtual achines, processing and memory capabilities. All systems started to evolve from several non-complex bandwidth and storage-sharing solutions towards more sophisticated, problem-specific services, including multithreaded processing systems and virtual environments.

Another characteristic for clouds is the deployment model. It categorizes customers according to the defined rules of shared resources. Clouds may be public (available for all users), private (operating with a single organization), community (owned and operated by several organizations) and hybrid. With the evolution of cloud computing it became vital to distinguish several groups of problem-oriented systems according to the specific features they represent. These groups are better known as "service models".

2.2 Service models

Original and available from the first years of clouds' utilization is a model where software is provided as a service (SaaS model) (Chenette, 2009). The goal of this model is to provide applications which run in the cloud environment and communicate with the customers in ways, common for the majority of users (client interfaces may be accessed by everyone who can operate with personal computers, laptops and mobile devices). Web browsers are among the most common methods to deal with remote software services. In most cases, management of the inner infrastructure of the cloud if fully transparent to

the customers but some applications can be configured by the users and store the options on remote servers (Mell, & Grance, 2011).

Another type of service model is PaaS – Platform as a Service. It is more flexible than the previously described one and allows operating on a "lower level". While Software-as-a-Service model gives the ability to utilize provider's applications, PaaS model works similar to the operating system installed on a typical PC. It gives users the ability to deploy applications they have purchased or created. PaaS providers usually have some cross-platform web-based tools for successful porting and deployment of applications as well as add-ons for simplifying work with common templates (e.g. electronic documents, databases etc.). The majority of operating systems, programming languages and related technologies (such as DBMS) are supported to fit the most exacting customers (Service Level Agreement Advisory Group, 2015).

The Infrastructure-as-a-Service model can be viewed as the most "low-level" approach to cloud computing available. According to this model customers have the ability to set up applications as well as operating systems. Sometimes access to firewalls or other network components are granted to fulfill users' needs. Current model is the most useful for software developing companies, providing cross-platform testing grounds with controlled networking, configurable and constantly monitored environment (Muller, 2015).

All these models have their own levels of implementation but they all share the same cloud computing principles – automatically and transparently deal with the problems, which are not vital to the user on the current level. Scalability, automatic resource allocation and transparent operating mode are the key features and customers can choose between the models depending on how much control they need on the applications running remotely.

3. Analysis of Possible Threats

Like a lot of other IT innovations, cloud computing has always been a subject of numerous discussions in terms of security. Apart from flows and drawbacks of remote computing, direct threats exist and all the potential customers have to be aware of some of the risks, associated with the usage of clouds. Due to a number of reasons, utilizing remote software may sometimes lead to problems with locally installed application and hardware. Furthermore, companies which use clouds to provide their own services have to be well informed about possible attacks, which can harm their customers and therefore their reputation and income.

The threats are generally classified by their nature, impact on data and applications. Lately, the advisory committee of the Cloud Security Alliance has also announced a statistical compilation, in which an attempt was made to classify threats by their severity level for different service models. More generally, a list of threats, common for every customer, is presented giving an overview of the most widespread drawbacks.

3.1 Interfaces

High levels of interactivity of cloud services are available due to the provided convenient application programming interfaces (APIs). These interfaces can be used for many various operations, including low-level resource management and therefore pose a threat if misused. Security often emerges as a drawback in systems, where convenience is made the key feature. Providers often build their applications on a higher level, utilizing basic APIs, related to the inner architecture. This solution is only good when developers are aware of API dependencies, because security maintenance in layered systems may become times more complex than when basic API is used (Hall, 2011). Furthermore, interfaces often deal with delicate data and provide tools for authentication and encryption\decryption. Implemented insecure authentication and transmission schemes and improper memory management may reveal account details, passwords etc.

In the remote systems monitoring and logging mechanisms may also be provided with limited functionality which may provoke related unwanted results.

3.2 Account hijacking

One of the oldest types of attacks, fraud and the usage of credentials is one of the most serious drawbacks in cloud computing as well as in many other spheres. Unauthorized activities can deal a great damage because the attackers have the ability to act on behalf of the account owner – they have the ability to manipulate data and manage your transactions. If the account is shared and trusted by another service(s) the risks grow even more because the attacking side may receive and alter data sent to and from the hacked account (Hinchcliffe, 2008).

The best practices to cope with account hijacking are the usage of well-configured monitoring systems and limitation (or prohibition where possible) of transacting credentials between users and services. When implementing defensive mechanism it is vital to understand the role of each account and provide additional security measures for accounts with elevated rights.

3.3 Data loss

Data loss is one of the most common and simple problems in systems which provide storage as a main distributable remote resource.

Reliability of the most data centers is closely connected with the security of accounts and AAA (authentication, authorization, audit) schemes. Most losses are provoked by improper implementations of backup methods, but one of the most serious problems in data centers is definitely the loss of the key to access encrypted data.

The problem of maintaining data security has to be considered during service's runtime as well as during the design process. Careful choice of tools (such as DBMS), usage of strong algorithms for encryption, key generation, protection and backup are the best practices to deal with data losses.

Data leaking is described as a similar problem, but the origins of this threat lie in the schemes of data disposal. Possible drawbacks are described by persistence and permanence challenges. Resource reallocating mechanisms have destroyed. Disposal politics is often a point of many contractual arrangements and discussions accompanying and supporting service level agreements. to be strong enough to deal with allocation of storage, on which sensitive data was not physically.

3.4 Shared technology risks

Shared technology threats are closely related to IaaS service models. Even minor flaws in scaling-related or monitoring modules may result in the unauthorized access to the data on the physical level (attackers aim for HDD partitions and even CPU cache). A simple overview of this problem suggests that shared technology risks appear when some users get elevated rights to control and access shared resources. The fact that IaaS model implements the lowest (operating system) level of interaction for the users makes it possible to alter configurations using installed applications (TechTarget, 2015).

Strong authentication and monitoring mechanisms are the methods used to reduce the success probability of such attacks. Modern cloud vulnerability checkers also operate in a way, similar to anti-rootkits, designed for personal computers. Logging and keeping audit of configuration changes for the remote infrastructure are effective in unveiling the attacks in progress.

3.5 Insiders

The threat of malicious insiders is an issue, most closely linked to the human factor (after account hijacking). While implementing strong security monitoring the activity of the services' usage by the clients, remote systems do not always pay necessary attention to the process of monitoring the activities of insiders. Many companies providing services in the cloud are more concerned with possible illegal activities performed by users rather than the ones performed by their employees. Even in the systems, where data manipulation is strictly monitored, eavesdropping and data harvesting by insiders can be a powerful tool. Strict hiring policy and defining human resources as a part of any legal contract are the working practices to fight against the insider threat.

4. Inappropriate Usage of Services

From the beginning of the era of cloud computing the remote services were used for inappropriate activities for numerous times. Exploiting the anonymity policy and the lack of standards for authorization policies among different providers, a lot of people use the remote services to test malicious code, send spam and host Trojans and illegal data. It is a known fact that a remote IaaS service has been used to host the famous Zeus botnet and hackers currently predict a "glorious" future of botnets in the clouds.

Another way of inappropriate usage is the provocation of Distributed Denial of Service (DDoS) attack. Intrusion prevention systems proved to be effective in the cases, when attacks have some common distinguishable features. The principles anonymity policy and distribution of data over a vast amount of servers work quite well on hackers' behalf here.

Some information has been published concerning the usage of remote computation for password and key cracking. Virtually unlimited memory and CPU capabilities along with scalability features may become formidable threats to cryptographic algorithms in the nearby future.

5. Summary

It is clearly visible that the conveniences of cloud computing come at a great price. All the positive sides of cloud computing can be quite easily used for illegal and inappropriate activities. The politics of anonymity and simplified authorization schemes are the major drawbacks for the usage of remote services. Lack of standards for authorization, logging, monitoring and auditing scenarios leave malicious users with plenty of ground to experiment. Additionally, remote services themselves are being used by hackers to access sensitive data and perform various kinds of attacks.

The risks can be generally divided in two major groups – design flaws and human interference. This is a conditional distinction because most of the times hackers take advantage of design and API drawbacks (Gorelik, 2010).

Careful reading and understanding of SLA, knowledge of local laws (for servers situated in other countries) secure databases and architecture design, solid authentication, encryption and data transmission protocols, proper data backup and truncation – all of these are the practical recommendation for avoiding certain threats associated with remote computations..

References

1. Cloud Security Alliance. (2010, March). Top Threats to Cloud Computing V1.0. Retrieved from https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.
2. Chenette, S. (2009, March 22). AusCert 2009 – P0wning The Programmable Web. Retrieved from http://securitylabs.websense.com/content/Blogs/3402.aspx.
3. Mell, P., & Grance, T. (2011, September). The NIST Definition of Cloud Computing. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
4. Treadway, J. (2009, July 13). Databases and Cloud Computing Roundup. Retrieved from http://cloudbzz.com/2009/07/13/cloud-dbms-databases-and-cloud-computing/.
5. Muller, M. (n.d.). Guide to SaaS – Software as a Service. Retrieved from http://www.brighthub.com/guides/saas.aspx.
6. Hinchcliffe, D. (2008, April 11). Comparing Amazon's and Google's Platform-as-a-Service (PaaS) Offerings. Retrieved from http://www.zdnet.com/article/comparing-amazons-and-googles-platform-as-a-service-paas-offerings/.
7. Hall, A. (2011, January 6). The Confusions of IaaS, PaaS, and SaaS. Retrieved from http://www.cloudave.com/9239/the-confusions-of-iaas-paas-and-saas/.
8. Tech Target. (n.d.). Cloud Security Resources and Information. Retrieved March 21, 2015 from http://searchcloudsecurity.techtarget.com/resources.
9. Service Level Agreement Advisory Group. (n.d.). Service Level Agreement and SLA Guide: The SLA Toolkit. Retrieved March 21, 2015 from http://www.service-level-agreement.net/.
10. Gorelik, E. (2013, January). Cloud Computing Models. Retrieved from http://web.mit.edu/smadnick/www/wp/2013-01.pdf.

4/16/2015