Security Threats and Solutions in Cloud Computing

Hanım Eken
Institute of Information
Gazi University
Ankara, Turkey
eken.hanim@gmail.com

Abstract— **Information Technology infrastructure continues to grow with evolving technology. The invention of the Internet has increased the use of computer and the mobile device. Nowadays, many people in the world use these devices. As a result, a large amount of data stored device and each device in the Internet were required to be connected each other because of sharing information. New business model has emerged with the increase of data and the development of Internet and mobile technology. This new business model is referred to as cloud computing. The cloud computing offers many advantages, but there are also many disadvantages. The advantages are flexibility and scalability and better security and large enterprises.**

This paper identifies security threats focused on cloud computing which is an essential part of the companies that want to use cloud computing services. The fundamental risk factors particular to the cloud are elaborated.

Finally, this paper provides some solutions about security threats for enterprise and service provider for the cloud computing deployment in order to provide the security of information. This paper does not mention new idea or innovation about cloud computing. Purpose of this study is intended to be a guide for people who is interested in cloud computing and want to take advantage of the cloud computing services.

Keywords- Cloud computing, Cloud computing security, Risk management, Information Security, Critical infrastructures

I. INTRODUCTION

Internet was introduced in 1982 after TCP/IP was standardized and consequently, the concept of TCP/IP network announced. Internet started to make huge impact on world with electronic mail, instant messaging, VoIP, video calls and especially World Wide Web with its social networking, blogs, online shopping sites and discussion forums. Increasing amount of data is transmitted at high speeds due to networking developments (fiber optics). In the year 1993, only %1 of information flows through two-way telecommunication networks. It increased to %57 by 2000 and %97 by 2007 [1].

Nowadays, the Internet continues to grow and greater amount of information is being transferred. Adding smart phones and tablet pc's to this environment. As a result, data and application in Internet and mobile have continuously increased. Thus, data must be stored and achieved. All these technological developments provide new business model which is cloud computing. Cloud computing is an important solution and cost effective model in order to facilitate companies' computing needs and accomplish business objectives [2].

In this paper, firstly gives information about cloud computing, then mentions security threats of cloud computing. After all, talking about how to mitigate security threats and give recommendations to mitigate security threats.

II. WHAT IS CLOUD COMPUTING

Cloud computing supplies a shared pool of configurable IT resources such as network, software and database. Customers are able to use virtualization resources very easily by a scalable and elastic cloud computing service. Cloud computing can also be defined as the collection of technologies and a means of supporting the use of large scale Internet services for the remote applications with good quality of service (QoS) levels [3].

The first standardized definition of "Cloud Computing" done by Forrester Research was:

"A standardized IT capability (services, software or infrastructure) delivered via Internet technologies in a pay-per-use, self-service way." [4].

The most recent and accepted definition done by the National Institute of Standards and Technology (NIST) is:

"Cloud computing is a model for enabling ubiquitous, 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. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models." [5]. In additon Figure 1 shows services in the cloud computing [6].

Figure 1: Services in the Cloud

The term "Cloud Computing" dates back to the 1950s. There are four milestones in the history of cloud computing. These happened at 1950's, between 1960's- 1970's, 1990's and after 2000.

At the beginning of 2000, Amazon made a huge impact by modernizing their data centers. Until that time they were using %10 of their capacity and leaving the rest as insurance. New cloud architecture gave opportunity to add new features faster and easily. This resulted Amazon to provide their new product called, Amazon Web Services (AWS) to external customers in year 2006. The aim of the service is providing a large computing capacity faster and cheaper than building a physical server farm [7].

Cloud computing includes three basic cloud-computing models that service providers can offer; IaaS (Infrastructure as a Service), PaaS, (Platform as a Service) and SaaS (Software as a Service) [8] In 2012 NaaS (Network as a Service) and CaaS (Communication as a Service) were officially included by ITU (International Telecommunication Union) as part of the basic cloud computing models [9]. Also, Figure 2 represents Cloud Computing Models.

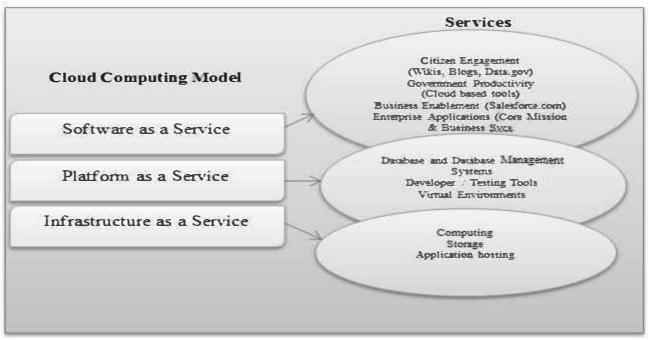

Figure 2: Cloud Computing Models (Cloud Computing Security Issues and Access Control Solutions)

Infrastructure as a Service (IaaS) is main cloud service model. IaaS offer computers and other resources like virtual machines, servers, storage, load balancers and network. Computers can be physical or virtual machines [10]. Amazon EC2, HP Cloud, Joyent, Linode, Rackspace, Google Compute Engine, Windows Azure Cloud Services and ReadySpace Cloud Services are main examples of IaaS.

Platform as a Service (PaaS) provides a higher level of abstraction then IaaS to make a cloud easily programmable [8]. This platform enables developers to use execution runtime, database, web server and development tools. AWS Elastic Beanstalk, Windows Azure Cloud Services, OrangeScape, Heroke and Jelastic are examples of PaaS.

Software as a Service (SaaS) provides users to access to application software and databases. Cloud users don't need to install and run the application on their own computers. Maintenance and support becomes much easier by this way [11]. Google Apps, Microsoft Office 365, GT Nexus, Marketo, Salesforce, Rally Software are some examples of SaaS.

There are four deployment models, which describes the environment of where cloud applications and services can be installed for consumers to use. These are; public cloud, private cloud, hybrid cloud and community cloud.

Public cloud is an open model which including applications and storage are rendered over a network. Public cloud is open for public use and cost effective service for application hosting [12]. Examples include the Amazon AWS, Microsoft and Google.

Private cloud is appropriate for a single organization. This infrastructure managed internally by the organization or by a third-party and can be hosted internally or externally [5].

Hybrid cloud is a combination of public and private clouds in order to perform various functionalities within the same organization.

Community cloud is used in order to provide cloud-computing solutions for individuals or organizations concerning regulatory compliance or performance requirements [5].

In recent years, cloud computing has a very important role in information technology in the world because of development of the cloud. Cloud computing has advantages and disadvantages. Disadvantages of cloud computing are security threats for cloud computing customers. Disadvantages are generally about security. This paper gives disadvantages of cloud computing then identifies recommendations to mitigate the security threats.

III. SECURITY THREATS IN CLOUD COMPUTING

Security threats in cloud computing are important issue for cloud service providers and cloud service customers. Threats usually are related information security because of data and applications. Cloud computing service has wide variety of

threats because of being combination of several technologies. If a candidate for cloud computing users wants to use cloud computing service, customer is being aware of security threats. In the section has identified security threats and effect of data security.

A. Information Security

Information security has an important significance in the cloud. Cloud computing is a combination of several different technologies. Thus, cloud computing faces just as much security threats. These threats are lack of cloud provider security, attacks by other customers, physical security, availability and reliability situation, legal and regulatory situation, data loss/leakage, shared technology vulnerabilities [13].

Confidentiality, integrity and *availability* (CIA) security model is basic security element of information security. Therefore, cloud provider must supply this security model for customers. All data and applications being maintained by cloud providers. Provider must supply the security of data.

B. Physical Securtiy

Physical security implies that the data center the cloud is hosted in should be secure against physical threats. This includes not only attempts at penetration by intruders, but also protection against natural hazards and disasters such as floods, and human error such as switching off the air conditioning. For this reason, data center location is important. Cloud computing customers must be careful about location when they choose cloud computing providers. At first data must be protected physically. Cloud computing providers must protect infrastructure and choose special location for data center. Specific entry/exit control techniques are required for physical security. This control should be done in order to identify personal and search individuals, vehicles, and materials [14].

C. Data Location

Most well-known cloud service providers have data centers around the globe. Some service providers also take advantage of their global data centers. However, in some cases applications and data might be stored in countries, which can judiciary concerns [12]. Illegal situations about data, laws of the country where the data is stored implemented. This event can be a big problem to punish the real criminals. Data is not access because of laws of country where the data is stored. If cloud computing customers have sensitive personal data or private data, they prefer cloud computing provider in their country for legal processes. Furthermore, sensitive data must be protected because of homeland security. Data must be stored own country.

D. Data Investigation

Cloud computing consists of many different systems. For that reason, finding information is difficult in cloud environment. When people need data for searching an illegitimate activity, they must have enough time on account of analyzing data. In addition, data for multiple customers may be co-located and may also be spread across multiple data centers. Usually users' knowledge is not enough to using cloud computing environment. Service provider may also impose restrictions on the network security of the service users.

If cloud computing customers have important and sensitive data, they must work with the best cloud computing service providers. Cloud computing service providers must guarantee that would give the necessary information quickly.

E. Data Segregation

Cloud computing providers store different customers' data in same devices. Poor segregation of resources increases the risk of vulnerability. Attackers may be succeeding stealing data. This threat can be overcome by providing complete isolation of customer data on a dedicated physical server. Besides, all data in the cloud must be encrypted with a strong password due to overcome threat. Encrypted data cannot be used even if data is stolen by attackers. However, strong encryption may increase costs. The data may be destroyed by encryption accident.

When service providers change business situations in order to ensure data security, this situation may affect customers adversely. So, the available data is not correctly sent to the customer at all times of need.

F. Data Recovery

All data is stored in cloud computing providers' physical devices. Data is backed up by cloud computing providers. Data and data backup may be stored in same physical devices. This situation is major problem about data security in natural and man-made disasters. However, the cloud is a service aimed at preserving your data, not protecting it. Cloud computing customers discuss these events with cloud providers. Cloud service providers must ensure the data security in natural and man-made disasters. The goal is to minimize a data loss risk and successfully recovering from a loss. In the case of any such unwanted event, provider must do a complete and quick restoration [14].

G. Secure Data Transfer

All of the traffic is between cloud computing customers and cloud provider network. All data travels through the Internet. There are many threats to the data being transferred. If attacker leaks network, he/she manages to listen to all of the data flow. If you are not satisfied security measures, it is big trouble for customers. Thus, service providers make sure data

always travels on a secure channel. When data is transferred, data must be encrypted.

H. User Access Control

Firstly, user access control is enough to provide security for sensitivity of the data in cloud. Because data for multiple customers may be co-located in cloud, other people may be access other customers' data. It is an important risk for sensitive data. Cloud service vendors must provide best access management for cloud customers. Access management is to allow accesses to cloud facilities only to authorized users. Additional requirements are to:

- cloud management personal have not unrestricted access
- multi-factor authentication for example password and fingerprint
- accounts do not shared for example admin
- provide white-listing of IP addresses for remote actions

IV. MITIGATION OF SECURITY THREATS

There are several types of security threats to which cloud computing is vulnerable. These threats damage *confidentiality, integrity* and *availability* (CIA) security model. Accordingly, solutions of security threats aim to protect (CIA) security model. Many recommendations which are solved security issues will be offered in these sections.

Firstly, cloud computers' customers find the best cloud provider. Each cloud service provider has different data security and data management. Hence, customer determines requirements for cloud services then choose right cloud provider. Also, cloud provider must have experience, standards and regulation about cloud service.

Data transfer between customers' network and cloud in the Internet. Therefore, data must be always travelling on a secure channel. HTTP is insecure due to send data all as plain text. Attackers gain access to website accounts and sensitive information with man-in-the-middle and eavesdropping attacks. Connect to browser with HTTPS. Because everything in the HTTPS message is encrypted with SSL. Also, standard protocols should be used for authentication [14].

User access control is important in cloud computer because of sensitive and private data. Only authorized persons should see the information and persons should be authorized until they need it. Customers to ask service providers for specifics about the people who manage their data and the level of access they have to it.

All systems and network components' log must be stored and monitored so as to analyze unwanted events. Logging and monitoring events is the process of auditing. Auditing is important for analyzing events. Auditing is necessary to provide security. Cloud computing customers discuss cloud provider about monitoring logs day-to-day. In addition, the audit log should be centrally preserved. Authentication and authorization should be done for people to monitor the audit log.

Unfortunately, auditing is a passive defense because of becoming aware of critical security event after the occurrence of the event. Auditing help people to response to unwanted-event quickly. Thus, cloud provider may improve process that including a cloud-wide intrusion and anomaly detection system. The intrusion detection systems may be installed an infrastructure for security.

Besides, security testing is important to provide security in cloud computing. Security tests should be performed for software before deployment in infrastructure of cloud. Software patches should be tested for security before software patches to install. Additionally, security testing should be realized continuously to identify vulnerabilities in the cloud system. On the risk assessment, some of these tests may be performed by third parties. There should also be a process to resolve identified vulnerabilities.

If all systems in the data center are synchronized to the same clock, this is helpful both to ensure correct operation of the systems, as well as to facilitate later analysis of system logs. If time zone is different, it is big problem for logs and synchronizes systems. Data has needed to analyze the event such as the time when a problem about security-related events.

In a cloud, with shared storage, encryption is a key technology to ensure isolation of access. The cloud infrastructure needs to provide secure facilities for the generation, assignment, revocation, and archiving of keys. It is also necessary to generate procedures for recovering from compromised keys.

Policies, standards and guidelines should be developed, documented, and implemented. Cloud computing providers must be up to this standards and policies. To maintain relevancy, these policies, standards, and guidelines should be reviewed at regular intervals or when significant changes occur in the business or IT environment [15].

Trainings or programs should be developed that provide a baseline for providing fundamental security and risk management skills and knowledge to the cloud computing providers, the security team and their internal partners [15].

Security in cloud computing is very important topic which will be certainly discussed in the upcoming years of cloud computing. Based on IDC survey [16] the security and vulnerability market should exceed revenue of $4.4 billion by the end of 2013, with a climbing annual growth rate resulting in a compound annual growth rate (CAGR) of 10.8%. This

survey shows that products that fall within the security and vulnerability management market will remain in high demand [15].

V. CONCLUSION

In recent years, the use of cloud computing has begun to spread in the world. It has matured over the years. Cloud computing is a good opportunity for enterprises to cost savings and computing requirements. However, security threats are a major problem for enterprises. For that reason, cloud computing customers must explore all cloud computing providers when they decide to take cloud computing service. So, this paper identifies being aware of the risks in the cloud computing environment.

In this paper purpose is to serve as an introductory exploration of the security threats. The threats are related to information security and *confidentiality, integrity* and *availability* (CIA) security model. Security threats about cloud computing are discussed. Additionally, companies are looking for cloud computing services have informed about the security threats in this paper. Finally, recommendations that mitigate security threats are presented.

Also, this paper is to provide a fundamental step towards the development of guidelines and standards for secure cloud computing environments. This paper does not mention new idea or innovation about cloud computing. Purpose of this study is intended to be a guide for people who is interested in cloud computing and want to take advantage of the cloud computing services. The researcher is able to ensure that innovation about cloud computing, after researcher read this paper.

REFERENCES

[1] History of The Internet, http://en.wikipedia.org/wiki/History_of_the_Internet/,2013. (Access date:15.08.2013).

[2] "The benefits and challenges of cloud computing", http://www.moorestephens.com/cloud_computing_benefits_challenges.aspx/, 2013. (Access date: 21.08.2013).

[3] G. Kulkarni & J. Gambhir, T. Patil, A. Dongare, "A Security Aspects in Cloud Computing", 978-1-4673-2008-5/12 ©2012 IEEE

[4] J. Staten, T. Schadler, J. R. Rymer, and C. Wang (2009, August 14). Q&A: By 2011, CIOs Must Answer The Question, "Why Not Run In The Cloud?". (S. Leaver, & A. Viglianti, Interviewers)

[5] P. Mell & T. Grance, (2011), "The NIST Definition of Cloud Computing. National Institute of Standards and Technology.", US: National Institute of Standards and Technology.

[6] Hosted Cloud Computing, http://www.alchemysys.net/solutions/hosted-cloud-computing/,2013. (Access date: 24.08.2013).

[7] Amazon. (2006). About AWS, http://aws.amazon.com/about-aws/,2013. (Access date: 15.08.2013).

[8] Voorsluys. (2011), "Cloud Computing: Principles and Paradigms." (R. Buyya, J. Broberg, & G. Andrzej, Eds.) New-York, USA: Wiley Press.

[9] ITU, International Telecommunication Union, http://www.itu.int/ITU-T/newslog/Cloud+Computing+And+Standardization+Technical+Reports+Published.aspx,2013. (Access date: 16.08.2013).

[10] A. Amies, H. Sluiman, Q. Tong, & G. Liu, 2012, "Infrastructure as a Service Cloud Concepts"

[11] M. Hamdaqa, T. Livogiannis, & L.Tahvildari, 2011," A Reference Model For Developing Cloud Applications", 1st International Conference On Cloud Computing and Services Science (pp. 98-103). Ontario: SciTePress.

[12] M. Hamdaqa & L. Tahvildari, (2012), "Advances In Computers" (Vol. 86), Ontario: Elsevier.

[13] Cloud Security Alliance Congress 2010, Orlando, FL, November, 2010

[14] N. Brender, I. Markov, "Risk perception and risk management in cloud computing: Results from a case study of Swiss companies", International Journal of Information Management 33 (2013) 726– 733

[15] K. Popović, Ž. Hocenski, "Cloud computing security issues and challenges", MIPRO 2010, May 24-28, 2010, Opatija,Croatia

[16] International Data Corporation, Worldwide Security and Vulnerability Management 2009–2013 Forecast and 2008 Vendor Shares, http://vulnerabilitymanagement.com/docs/IDC_MA_2009.pdf/,2013.(Access date:16.08.2013).