Indian Journal of Science and Technology, *Vol 9(21), DOI: 10.17485/ijst/2016/v9i21/95282, June 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Analyzing Impacts of Cloud Computing Threats in Attack based Classification Models

R. Kamatchi[1]* and Kimaya Ambekar[2]

[1]Amity University, Mumbai - 410206, Maharashtra, India; kiyer@mum.amity.edu
[2]K. J. Somaiya Institute of Management Studies and Research, Mumbai - 400077, Maharashtra, India; kimaya.ambekar@somaiya.edu

Abstract

Objective: This paper makes an attempt to analyze the threats and vulnerabilities of a cloud based system and propose a threat modeling and process associating with. Different models can help policy makers to evaluate common criteria which in turn can help to create threat specific plan to have a customized solution. **Methods/Analysis:** This paper is an attempt to contribute to the existing research in the area of cloud security. It also analyzes the impact of threats and usage of threat models to improve the security aspects of data in transit and storage. This research uses an analytical research methodology. It tries to analyze various models in terms of their impact and usage to various organizations to combat threats on their data and networks. Existing literature has been studied and analyzed on various parameters to further study the recovery procedures and contingency planning. **Findings:** Different models can help policy makers to evaluate common criteria which in turn can help to create threat specific plan to have a customized solution. **Applications:** Cloud computing is an upcoming technology which is fascinating varied type of organizations. Even though it is widely adopted positively by different set of organizations, it also has its own security issues at different levels. To create a better security plan for an organization, precise calculation of attacks at different levels need to be determined and the impact should be estimated. To enable the same, well-accepted methods are to be determined which can help the users to map their systems with the solutions to have a better visualization.

Keywords: Cloud Computing, Model, STRIDE, Security, Threats

1. Introduction

Technology has evolved tremendously through the past decades. The conscious raise in telecommunication and internet usage resulted with the rapid acceptance of Web 2.0 technologies in many developed as well as developing countries. Web 2.0 came with technologies like social media, blogs and online data sharing. These technologies created a way for huge amount of data handling. On the other hand Grid, cluster and utility computing were also taking good pace. The outsourcing of service paved a way for the introduction of Service oriented architecture. By considering all these cutting edge technologies, the cloud computing technology came alive and became prominent.

The implementation of cloud computing has created a value for the organization which in turn started moving their entire data on cloud. It caused many problems related to data location, control on the data, privacy related problem. It is the need of the hour to focus on these security and privacy related issues.

Security of the cloud can be threatened due to various reasons like loss of control on the data, security related to virtualization etc. At the same time, cloud services can

*Author for correspondence

also be threatened due to privacy related issues like risk of data loss or unauthorized access etc.

For securing the cloud, vulnerabilities available in the system should be identified. From these vulnerabilities, we can analyze threats to the system where attackers can attack. Threat modeling is a process by which we can analyze the vulnerabilities in the system which can lead to threats to the systems. There are several threat classification models available but every model has several distinctive features. Mapping them with various other models may give us a better model which organizations can use while creating security policies.

2. Cloud Computing

As per Gartner, Cloud Computing is an approach of computing in which elastic and scalable IT-enabled necessities are delivered as a service using Internet technologies[1].

In layman's term, cloud computing is a technology in which services and resources from shared pool can be provisioned and released easily[2]. Due to cloud computing, users can reduce the CAPEX (i.e. Capital Expenditure) and can use the finance to improve their core competencies or processes. These services are provided from Cloud Service Provider (CSP) and used by the client through internet from any device. There are three major types of services with respect to service delivery, they are,

- **IaaS (Infrastructure as a Service):** In this service, CSP provides infrastructures like storage, hardware, communication etc.
- **PaaS (Platform as a Service):** In this model, CSP provides database, platforms and frameworks by using which clients can create applications and software.
- **SaaS (Software as a Service):** CSP provides applications or software which is generic in nature and needs no or less customization.

At the same time, according to the deployment, we can categorize cloud computing into four major types:

- **Public cloud:** It is a type of cloud in which services are owned by the CSP and provided to client free or using pay as you go model. Example: Google App is a public cloud in which Google provide services free for some data usage but after that it charges pay as you go model.
- **Private cloud:** In this type of cloud, services are dedicated to a particular organization on site or off site. And it is maintained either by organization or by CSP or by third party.
- **Hybrid cloud:** It can be a combination of more than two deployment models (i.e. public, private, community). It gives advantages of all the models it combined. Example: An organization using private cloud for data storage and networks and using Gmail as mailing server.
- **Community cloud:** This is useful for the organizations whose goal or mission is common. Such organizations can collaboratively use the services given by CSP. These services can be managed by third party or CSP. Example: Educational or healthcare institutes can come together to use private cloud which can be shared by all associated organizations

3. Cloud Security

Cloud computing has various distinctive benefits which organizations especially SMEs, can leverage on it. But like any other technologies it also shows various disadvantages or issues like security, privacy, reliability, availability, governance etc; among which security is of most important to highlight. Need of security for different types of organizations are different. For example, Academic institutes need to impose privacy of data and law/copyrights issues. At the same time if it is a financial institute/organization, security and privacy of the data is the most important. But in general, there are some threats which are common for all, and need to be addressed.

3.1 Attacks, Threats and Vulnerability

While understanding security, we have to understand some basic concepts related to security. It can be explained as follows

3.1.1 Vulnerability

Vulnerability can be explained by NIST in FISMAPEDIA (SP 800-18r1) as "A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy"[3]. Commonly, we can define vulnerability as a defect/flaw in the system which can be utilized by the attacker to attack on the system. This can be seen as weakness in the network and/or devices such as desktops, servers, routers etc.

Vulnerabilities can be seen because of following weaknesses in the system[4].

- Technology weakness.
- Configuration weakness.
- Security policy weakness.

3.1.2 Threats

National Information Assurance Glossary defines threat as: Any circumstance or event with the potential to adversely impact an IS or any organizational operations (including mission, functions, image, or reputation) through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats can be divided into four major categories they are[5,6]

- Structured threats
- Unstructured threats
- External threats
- Internal threats

3.1.3 Attacks

Attack is a technique used by the attacker to exploit vulnerabilities and create threats to the system. Attacks can be divided into many categories like active, passive, distributed, insider, close-in and phishing etc[7].

4. Threat Model

Cloud computing has various distinctive benefits which organizations especially SMEs, can leverage upon. The amount of data and resources can reside on clouds is massive in amount as compared to normal data centers. The scale and pace at which data is manipulated is very high.

Cloud computing can face accidental threats like password sharing or mistakes by some employee etc. It also faces many threats because of its client server as well as multitenant architecture. Some major and dangerous threats can be stealing of misplacing of data, external attacker or simply phishing attacks. And chances become high because of virtualized environment. Security breaches can be seen on various levels. In-depth knowledge of technology is making more room for security attacks. According to the 11th Annual Computer Crime and Security Survey[8], 74.3% of the total losses are caused by: viruses, unauthorized access, laptop or mobile hardware theft and theft of proprietary information[9] and McCue report says that 70% of fraud is perpetrated by insiders rather than by external criminals but that 90% of security controls are focused on external threats[10].

Proposing and implementing security mechanism in cloud computing involves understanding of various threats and vulnerabilities at early stages. Threat modeling is a structured way by which one can identify all possible risks and threats associated with the particular network; and also can suggest some countermeasures for the same. It can also be seen as an attack tree for a piece of software or technology[11]. Threat model looks at the cloud system/services from attacker's point of view which can help designers to design more secure systems and also can answer the questions like what the system is designed to protect and from whom?

5. Threat Modeling Process

Threat modeling is an important process while creating any service/software. It is not a one go process, but it is an iterative process. It is iterative in nature because of two facts. One, identifying threats at one attempt is almost impossible and second we can say that applications/services are no more static and there are tremendous changes in business processes which need to be thought about while creating them.

There is a predefined process for threat modeling to achieve maximum results. It is divided into following six stages:

- **Identify the assets:** In this stage you have to analyze the most valuable assets of your organization which may get damaged and need to be protected by the system.
- **Creating an architecture overview:** First, we need to understand the details of the system/service. Tables, diagrams or simple images of your system will help to understand the system including its boundaries, data flow as well as subsystems.
- **Decompose the application:** In this stage, you have to create fragments of your system including underlying hardware, networks and infrastructure. On the basis of it, we can create a security policy for the system. The security policy should reveal all vulnerabilities which can arise in the system development lifecycle.
- **Identify the threats:** Till this stage we know about the system details, infrastructure details as well as potential vulnerabilities. Now we can identify the threats based on the previous knowledge.
- **Document the threats:** Common threat template can be created for an organization and all the detailed

attributes analyzed for the found threats should be noted down

- **Rate the threats:** In this stage, we need to rate the threats from highest to lowest according to their impact/risk to the system. It should evaluate the probability of the threats against the damage that can cause to the system[12].

6. Threat Classification Method

A threat is a goal of an attacker or what an attacker can does with the system to destroy its functioning. There are two ways an attacker can harm the system. Hence we can divide the threats in two ways:

- Threats based on attack techniques
- Threats based on threat impacts

6.1 Threats based on Attack Techniques

6.1.1 Three Orthogonal Dimensional Model[13]

Lukas Ruf et al devised a model which tried to classify the threats based on three concepts called agent, localization and motivation shown in Figure 1.

- **Agent:** It is an actor who can enforce threat on the system. It can be seen in three ways: human, technology & force measure
- **Motivation:** it can be seen as stimulus for construct the treat on the system which can be divided as accidental and deliberate.
- **Localization:** The origin of the threats can be divided into external and internal.

6.1.2 Hybrid Model

Sandro et al. suggested a model namely the information system security threat cube classification model or C3 model in which he suggested[14]:

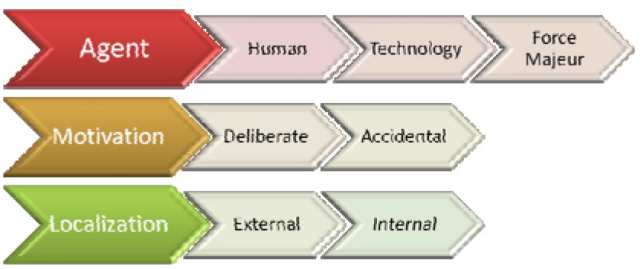

Figure 1. Three orthogonal dimensional models.

- **Security threat frequency:** It describes frequency of the threat which can occur.
- **Area of security threat activity:** it gives the domain which can be affected by the threat or attack. It can be divided into different types of security levels which can be personal security, operational security, data security, physical security, communicational security etc.
- **Security threat source:** type of threat source. It can be divided into nature, technical(technical mistakes, malfunctions, communications errors, radiation), people with attribution of un-attentiality (indiscipline, negligence, inappropriate software, inappropriate organization), people with attribution of attentiality (destruction, sabotage, diversion, espionage, war destruction, fraud, steeling, viruses)

6.1.3 Information security threats classification pyramid model:

In postulated a pyramidal model in which it describes three criteria[15]:

- **Attacker's knowledge about the system:** It gives the knowledge the attacker has about the system.
- **Criticality of the area:** How critical are the system parts which can be harmed by the attack
- **Loss:** All types of losses an organization can bear because of an attack.

6.1.4 Threats based on Attack Impacts

There are various models proposed by many researchers to prove threats based on attack impacts like STRIDE, DREAD, TRIKE, OCTAVE, and ISO etc. but most popular is Microsoft's STRIDE model[16,17].

STRIDE is applied on host, application as well as networks. The STRIDE is an acronym for six different threats which are as follows:

- **Spoofing identity:** In this type of attacks, attacker determines the IP address of network or computer of the authorized user and uses it to harm the system/service. He/she can also steal authentication details of the authorized user to break into the system.
- **Tampering with data:** This attack involves modification or alteration of data maliciously. Data can be modified when is it stored on the cloud storage or it can be modified while transit. Attacker can alter data in such way that it would harm the organization.

- **Repudiation:** Sometimes authorized users can execute an action /event and refuses the fact of doing it. In such situations administrator should have some logs/records to prove the same. Non repudiation is a technique which is a countermeasure for repudiation attacks. This can be done with audits, timestamps or digital signatures etc.
- **Information disclosure:** Information disclosure is a type of threat in which attacker/user is getting access which he/she is not authorized for. Attacker may gain access by various means; it may be password hacking or stealing of data in transit etc.
- **Denial of service:** In this type of attack, services are denied to valid and authorized users. This happens because the server or services are overloaded by the attackers which are mostly fake. Here, attacker uses some bots or software to send bulk requests. Sometimes, many attackers send such bulk & fake requests from different part of the world; this can be termed as Distributed Denial of Service (DDoS).
- **Elevation of privilege:** This is a dangerous type of attack. In this type of attack, attacker becomes a privileged user to gain access of the system/ service. Since he has the access to the system / service, he can destroy or compromise the system / service according to his/her wish. The attacker may also run some malicious code of his/her choice to make situation more worsen[18, 19].

7. Analysis

7.1 STRIDE vs. Three Orthogonal Dimensional Model Analysis

The detailed analysis table proves that most of the threats are human initiated with deliberate intentions. The attacker may be an insider or an outsider. This model shows that the human are more vulnerable to create any kind of attacks towards various resources. This is also indicates that the proper training and the rigorous norms could be the essential security measure for any organization. The security measures are supposed to be implemented at the server as well as gateway level, which can filter the messages from both the sides.

7.2 STRIDE vs. Hybrid Model Analysis

The detailed analysis under Hybrid model proves that most of the security threats are occasional and focuses on the complete operational aspects of the system. The operational area can lead to the complete functional deficiency of the system resources by which the complete control can be accessed by the intruder. Even though the human agent stimulates the vulnerability into threats, the sources for carrying attacks are mostly through technology. These kinds of threats can be well handled by the same technology in an optimistic way.

7.3 STRIDE vs. Classification Pyramid Model Analysis

The detailed analysis of Pyramid model indicates that, most of the threats could be possible through the continuous and thorough knowledge of an intruder about the source. With the extensive knowledge about the system vulnerability, the attacker can cause a severe damage to the targeted system. This can lead to different levels of hazards like data loss to complete control loss. This emphasis on the complete encapsulation of the system details with high level of access monitoring and frequent auditing of logs.

8. Findings

After analyzing all the three models with STRIDE, We could conclude that each model helps in attacks mitigation process in a different way. The Orthogonal

Table 1. STRIDE vs. three orthogonal dimensional model

	Three Orthogonal Dimensional Model		
STRIDE threats	**Agent**	**Motivation**	**Localization**
Spoofing Identity	Human	Deliberate	External
Tampering with data	Human	Deliberate	External/Internal
Repudiation	Human	Deliberate	Internal
Information Disclosure	Human/Technology/Force	Deliberate/Accidental	External
Denial of Services	Human/Technology	Deliberate	External
Elevation of Privileges	Human	Deliberate	Internal

Table 2. STRIDE vs. hybrid model

	Three Orthogonal Dimensional Model		
STRIDE threats	**Security Threat Frequency**	**Area of Security Threat Activity**	**Security Threat Source**
Spoofing Identity	Less Frequency	Personnel Security	People-Intentional
Tampering with data	Moderate	Communication & Data Security	Technical/People(Intentional)
Repudiation	Moderate	Operational	People-Intentional
Information Disclosure	Moderate	Operational	Intentional/Unintentional
Denial of Services	Less Frequency	Operational	Intentional
Elevation of Privileges	Less Frequency	Complete Control	Technical & Intentional

Table 3. STRIDE vs. classification pyramid model

	Classification Pyramidal Model		
STRIDE threats	**Attacker's Knowledge**	**Criticality of the Area**	**Loss**
Spoofing Identity	High	Moderate	Confidential Data Loss, Misuse of Data
Tampering with data	High	Severe	Confidential Data May loss
Repudiation	Low	Low	Reputation is Lost
Information Disclosure	Low	Severe	Information Leakage may lead to any attacks
Denial of Services	High	Severe	Resources under-utilized
Elevation of Privilages	High	Severe	Control lost on the complete system and can generate any kind of attacks

model analyses the motivation and the agents of the threat which can be considered during the prevention phase of mitigation process. Once the agents and the reason could be identified and generalized then the corresponding security measures can be implemented in place before the vulnerability can turn into an attack.

The Hybrid model tabulates the area of damage with the frequency of attack occurrence. This can be considered as a Detection Phase of Attack mitigation process. Once the vulnerable area and the damage levels are understood, then the implementation of the security measures can be customized and much targeted to face the security breaches.

The Classification Pyramid model can be considered as a Recovery Phase of any Attack mitigation process. It helps the user the estimate the level of damage caused and the criticality of the system after the damage. Based on this analysis, the user can decide the recovery procedure like repairing or discarding the affected resources. It can also be used as a base for the contingency planning of an organization to handle the threats in an efficient way.

9. Conclusion

Security is the most delicate and important aspect when organizations are moving on cloud. Data and resources are vital assets for any organization which needs to be secured. For better security, analyzing available threats and vulnerabilities are important which can be done from above threat classification models. From analysis we can state that different models can focus on different aspects of risk/attack mitigation process. When an organization creates the security policy, they can take help of these models to understand the problem areas and create a concrete plan for different phases. This way, organizations can secure their assets and plan the security better way.

10. References

1. Gartner Highlights Five Attributes of Cloud Computing. 2015. Available from: http://www.gartner.com/newsroom/id/1035013
2. Kirubakaramoorthi R, Arivazhagan D, Helen D. Analysis of cloud computing technology. Indian Journal of Science and Technology. 2015 Sep; 8(21). doi no:10.17485/ijst/2015/v8i21/79144

3. Vulnerability (computing). 2015. Available from: https://en.wikipedia.org/wiki/Vulnerability_%28computing%29
4. Vulnerabilities, Threats and Attacks. 2015. Available from: http://ptgmedia.pearsoncmg.com/images/1587131625/samplechapter/1587131625content.pdf
5. Bertino E, et al. Web Services Threats, Vulnerabilities and Counter Measures. Security for Web Services and Service-Oriented Architectures. Berlin Heidelberg: Springer-Verlag; 2010. Doi no: 10.1007/978-3-540-87742-43
6. Threat (computer). 2015. Available from: https://en.m.wikipedia.org/wiki/Threat_agent
7. Network security types of attacks. 2015. Available from: http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html
8. Jouini M, Ben Arfa Rabai L, Ben Aissa A. Classification of security threats in information systems. 5th International Conference on Ambient Systems, Networks and Technologies (ANT2014); 2014.
9. Gordon LA, Loeb MP, Lucyshyn W, Richardson R. CSI/FBI Computer Crime and Security Survey – 2006. 11th Annual CSI/FBI Computer Crime and Security Survey; 2006.
10. McCue A. Beware the insider security threat. CIO Jury; 2008. Available from: http://www.silicon.com/management/cio-insights/2008/04/17/bewaretheinsider-security-threat-39188671/
11. Rehausser P, Zimmer W, Gliesche O-S. Threat modeling for re-architecting security in cloud computing. 2015.
12. Microsoft MSDN. 2015. Threat modeling, Chapter 3. Available from: https://msdn.microsoft.com/en-us/library/ff648644.aspx
13. Ruf L, Thorn A, Christen T. Gruber B, Suisse AG, Portmann R, Luzer H. Threat modeling in security architecture - The nature of threats. ISSS Working Group on Security Architectures.
14. Sandrogeric, Zeljkohutinski. Information system security threats classifications. Journal of Information and Organizational Sciences. 2007; 31(1).
15. Alhabeeb M, Almuhaideb A, Le P, Srinivasan B. Information security threats classification pyramid. 24th IEEE International Conference on Advanced Information Networking and Applications Workshops; 2010. p. 208-13.
16. Kamongi P, Gomathisankaran M, Kavi K. Nemesis: Automated architecture for threat modeling and risk assessment for cloud computing. 2014.
17. Jouinia M, Ben Arfa Rabaia L, Ben Aissa A. Classification of security threats info system. 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014); 2014.
18. Reisman B, Ruebush M. MCSE: Windows server 2003 network security design study guide: Exam 70-298; Chapter 2. Identifying and designing potential threats.
19. The STRIDE Threat Model. 2015. Available from: https://msdn.microsoft.com/en-us/library/ee823878%28v=cs.20%29.aspx