Conference paper

by Maniah Maniah

Submission date: 19-Jun-2019 08:47AM (UTC+0700)

Submission ID: 1145086370

File name: ISICO_2019_paper_66.docx (1.96M)

Word count: 3700

Character count: 19711

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2019) 000–000

Procedia
Computer Science

www.elsevier.com/locate/procedia

The Fifth Information Systems International Conference 2019

Survey on Threats and Risks in the Cloud Computing Environment

Maniah[ab]*, Edi Abdurachman[c], Ford Lumban Gaol[d], Benfano Soewito[e]

[a]*Bina Nusantara University, Jl. Kebon Jeruk Raya No. 27, Jakarta 11480, Indonesia*
[b]*Politeknik Pos Indonesia, Jl. Sariasih No. 54, Bandung 40151, Indonesia*
[c]*Bina Nusantara University, Jl. Kebon Jeruk Raya No. 27, Jakarta 11480, Indonesia*
[d]*Bina Nusantara University, Jl. Kebon Jeruk Raya No. 27, Jakarta 11480, Indonesia*
[e]*Bina Nusantara University, Jl. Kebon Jeruk Raya No. 27, Jakarta 11480, Indonesia*

Abstract

A very important job in handling Cloud Computing services is handling threats as early as possible, both threats to users or threats to cloud service providers. Threats in the cloud context are all things that will bring loss to company assets that will cause IT risks to be stored in cloud computing. The purpose of this study is to survey threats in the scope of: Data, Applications, Infrastructure, and services in general in the cloud computing environment. The types of threats or attacks in the context of the cloud have been defined through surveys of relevant articles. The research methodology used is conducting a survey on some of the results of previous studies relating to threats or obstacles in cloud computing carried out in 5 steps, namely: writing the formulation, conducting a search, conducting selection and evaluation, analysis, and summarizing the results. From the survey results, there are many types of threats / obstacles in the cloud computing environment, which are divided into 4 (four) groups, namely: Threats to applications, Threats to data, Threats to infrastructure, Threats to cloud services in general. The results of this study are to provide a more detailed understanding of the types of threats for each service in the cloud.

Keywords: Cloud Computing, Threats, Survey ;

* Corresponding author. Tel.: 082-120-008-472
E-mail address: maniah@poltekpos.ac.id

1. Introduction

Threats to information technology assets (both applications and data) will have an impact on the organization's operations and assets. This form of threat is the main factor in determining the value of risk. In an organization the risks that arise are an integral part of all business activities. Definition of risk is the possibility of unwanted incidents and their consequences for certain assets, while the level of risk is the possibility of the level or value of the risk raised [1]. Whereas technology risk is a process that includes the process of identifying hazards according to their nature, possibilities, potential impacts, then can be assessed and controlled [2]. Another opinion says that the risks associated with information technology are business risks, especially business risks related to the use, ownership, operation, involvement, influence, and adoption of IT in the company [2]. The threat to IT risk in the context of cloud is very important to be considered for the sustainability of information technology and to guarantee trust for partners.

The development of Cloud Computing is very fast, so there is a possibility that many companies will soon switch from intranet (On-Premise) applications to Cloud Computing, although the risk is likely to be very large due to shared data usage. In [3] mentions there are 5 negative things from Cloud Computing, namely: (i) lack of legal protection, (ii) ownership of hardware, (iii) policy, (iv) unreliable machine technology, and (v) assumptions individual.

The purpose of this study was to survey the results of previous research papers related to writing about threats or attacks or obstacles that often arise in cloud computing environments that can be aimed at either cloud service providers or service recipients. The hope is that with a deep understanding of the types of threats to cloud computing, efforts can be made to reduce risk in the cloud environment.

The writing system in this paper consists of: the first part presents the importance of this research. The second part, provides a basic explanation of threats or obstacles in the context of the cloud. The third section, reviews several papers related to this study. In the next section explain the results of surveys and discussion of discussions about the types of threats that often appear in the cloud environment. And finally is the conclusion.

2. Related Work

Threats in the cloud context will certainly be very closely related to hazards that will threaten the sustainability of company assets stored in the cloud. So we claim here that the threat is a very critical foresight to be handled as early as possible, so that the impact of threats to cloud services will be reduced as little as possible by the risk of IT. In the next section we will discuss in detail the results of some previous research literature related to understanding and types of threats in the context of the cloud. Many previous studies discussed risk management. The following will discuss the threat to information technology risk in the context of cloud computing related to our research.

3.1. Threats / Obstacles on the Cloud Services

Assets that have been migrated in the cloud are important to identify what hazards might arise and efforts to overcome them, to maintain the security of these assets[4]. In his research[2] said that the most important problem or obstacle in the cloud computing environment is a security problem for dating threats, which will endanger both users and service providers in Cloud Computing. The main task that is not less important for cloud service providers is to ensure that the services available for data readiness are available properly and can be easily accessed by users for the continuity of their business[5]. Such as the existence of data security issues in the cloud (multi-tenancy, loss of control, and trust) is the main focus for cloud service providers to ensure that these issues can be controlled and provide the best solution in the event of problems[6].

Furthermore, [7]defines the security threat to cloud computing services based on 3 approaches, namely: resource use deviations in the context of cloud computing, data misuse, and crimes against data on the cloud. In his research[8], set the level of threats to current assets, which consist of: low (0-0.33), average (0.34-0.66), and height (0.67-1, 00). Different research is done by[9], namely looking at threats from the point of view of fog computing, even though this is no different from cloud computing, there are possible threats that will emerge, for example weak policies related to handling existing threats.

There is also a threat to the cloud in the form of service availability problems, namely the Distributed Denial of Service (DDoS) attack, which threatens the availability of unauthorized bandwidth services due to an increase in service costs [10]. In the paper [11] the possibility of a threat can occur in the vulnerability to the right of access to the system that is not directly, so he suggested creating a standard for a vulnerability. Every time we discuss a cloud computing environment, threat problems that might emerge are always a topic that is not forgotten, as written by [12] in his paper explaining cloud computing is one of them related to the source of threats in the cloud environment, namely: the existence of internal attacks in the form of crime by personnel behavior, some from external, such as a virus attack.

The earlier research [13] has been very detailed in reviewing several approaches that discuss threats to cloud computing. the issues he raised were related to threats to users and threats to cloud service providers. Next, [13], concluded that the standards for cloud security are as follows:

1. Threats to the model and framework
2. Threats to technology
3. Threats to indications of disaster
4. Threats to data backup systems
5. Threats to data confidentiality management
6. Threats to system accounts
7. Threats to connection security systems
8. Threats to VMs. VMs (Virtual Machine) is a computer file that is virtual but works like the original computer.

Until now the problem of data storage security is also something that is still very important to note in a cloud environment, this is because there are still many very dangerous attacks on data storage systems in the cloud and there are still many data leaks by irresponsible parties. This problem is described by [14] related to data storage security systems in cloud computing. As stated by [15] in his paper explaining related to Critical Success Factors (CSFs) in e-learning that are applied to cloud environments, one of the important factors of concern is the security, convenience, and reliability of services to users so as not to be threatened distrust of cloud service users.

3.2. IT Risk in the Context of Cloud

When migrating to the cloud there are many assets that switch functions related to risks that might arise due to adjustments to cloud services, it is necessary to identify risks in advance of those assets. Information technology risks that might appear in the cloud such as: data sharing, external data storage, problems during communication in accessing data[4]. IT risk will have an understanding that is slightly different from other risks that exist within the company's business scope[16].

Companies will get many benefits when IT risk is implemented, including companies can see in more detail the possibilities of current and future IT risks and the impact that will arise[17]. The risk of IT on the cloud is due to a security attack related to cloud-based services. As also in research[18] that security attacks on the cloud are identical to the threat term can be handled well if the symptoms of the threat have been recognized before. If the symptoms of a security attack on data in the cloud can be identified, then we can reduce the risk of IT in the context of cloud computing. Although the actual way of handling IT risk (applications and data) that has been migrated to the cloud can no longer be handled in a classic way, meaning that the company must have reliable resources in order to handle the company's information technology security management.

3. Research Methodology

This paper will discuss the types of threats in the context of services in the cloud, which means something that will harm all components in the cloud environment, both for users and cloud service providers. Cloud service providers provide this type of service: (i) IaaS (Infrastructure as a Service); (ii) PaaS (Platform as a Service); and (iii) SaaS (Software as a Service), [2] states that if a company wants to migrate to the cloud, one of the challenges is the problem of threats from cloud services. To survey several types of threats or attacks and risks that are relevant in the context of cloud computing, do the following 5 steps:

Step 1: Write down the formulation: Threats or risks to the cloud computing environment.

Step 2: Search: Search by Keyword and Boolean "+" Operator, on IEEE Xplore Digital Library, Springer, science direct. "threate" + "Risks" + "Information" + "Technology" + "on Environment" + "Cloud Computing"

Step 3: Conduct selection and evaluation: Selection and evaluation is done by selecting paper titles related to Threats and Risks in the Cloud Computing environment, the last 22 articles obtained.

Step 4: Analysis: Of the 22 articles there are 7 articles that explain in detail related to the types of threats or attacks that result in risks in the cloud context, then collected based on each article, found that from one paper there are several types of threats

Step 5: Summarize the results: The types of threats obtained in step 4 are related to the types of service resources in the cloud that can be risky due to threats or attacks. The results are grouped into data, applications, infrastructure and services in general (which are not included in the data, application or infrastructure group).

4. Result and Discussion

A threat is something that will happen, which is part of determining the appearance of risk. The types of threats discussed here are threats in the context of the cloud which can cause disruption of services from cloud service providers to users. The following are some discussions about IT risk-related threats in cloud computing based on survey results.

Researches related to security vulnerabilities and those that cause threats are very useful for companies that will migrate to the cloud [19]. The survey results are related to the types of threats or obstacles that often arise in the cloud computing environment, as shown in table 1. The type of threat is collected based on the reference paper and the year of publication.

Table 1. Type of threats on cloud computing

No.	Type of threat on cloud computing	Cloud service resources	Reference
1	Availability of Services,	Service in general	[10]
	Data/Vendor Lock-In,	Data	
	Data Confidentiality & Auditability,	Data	
	Data Transfer Bottlenecks,	Data	
	Performance Unpredictability,	-	
	Scalable storage,	Infrastructure	
	Bugs in large distributed systems,	Application	
	Scaling Quickly,	-	
	Reputation Fate Sharing,	-	
	Software Licencing	Application	
2	Abuse use of cloud computational resources,	-	[7]
	Data breaches,	Data	
	Cloud security attacks	-	
3	Multi-tenancy,	Infrastructure	[6]
	Loss of Control,	-	
	Trust Chain in Clouds	-	
4	Violation of SLAs,	-	[19]
	Improper virtual machine management,	Data	
	Using suspicious software	Application	
5	Account or service hijacking,	Application	[18]
	Data scavenging,	Data	
	Data leakage,	Data	
	Denial of service,	-	
	Costumer data manipulation,	Application	
	VM (Virtual Machine) escape,	Infrastructure	
	VM Hopping and Malicious VM creation,	Infrastructure	
	Insecure VM migration,	Infrastructure	
	Sniffing/spoofing virtual networks,	Infrastructure	
	Eaves dropping,	Application	
	Hypervisor viruses,	Application	
	Legal interception point,	Data	

No.	Type of threat on cloud computing	Cloud service resources	Reference
	Trusted transaction,	Application	
	Smartphone data slinging,	Data	
	Insecure APIs,	Application	
	Shared technology vulnerabilities	Infrastructure	
6	Elevation of Privilege,	-	[20]
	Repudiation,	-	
	Denial of Service,	-	
	Injection and XSS Attack,	Application	
	Wrapping attack,	-	
	Weak Service Level Agreements (SLAs),	-	
	TCP/ Session Hijacking,	Infrastructure	
	Roll back attack,	Data	
	Data loss or Leakage,	Data	
	Data manipulation,	Data	
	Violation of SLAs	-	
7	The feat of unauthorized access,	Application	[21]
	Data corruption,	Data	
	Infrastructure failure,	Infrastructure	
	Service availability,	-	
	Difficulty in detecting problems,	-	
	Security,	-	
	Data/Vendor Lock-In,	Data	
	Attacks against virtualization,	Application	
	API-level attacks against cloud services,	Application	
	Old attacks with new implications	-	

It appears that each paper reveals more than one type of threat, even one type of threat can appear in another paper. To better understand the relationship between types of threats with cloud service resources in the cloud computing environment, in table 2 the authors show groupings. This grouping is based on the definition and understanding of the scope of this type of threat. So that there are 4 groups of service resources that might be threatened by attacks in the context of cloud computing, namely: (i) Threats to applications; (ii) Threats to data; (iii) Threats to infrastructure; and (iv) Threats to cloud services in general.

First (i) Threats to applications; Attempts at attacks on software, including invalid features and attacks on virtualization. Usually this attack is more threatening on the application programming interface aimed at server applications. There are also tapping on videos and virus attacks. Second (ii) the threat to the data is due to the authority to analyze the data, the existence of disturbances during data transfer, incorrect data handling, data manipulation, and can also be caused by corrupt data. Some are caused due to the use of smartphones to access confidential data. Third (iii) Threats to infrastructure usually occur due to failure / damage to the infrastructure. The most enabling threat to infrastructure is due to Multi-tenancy. The next threat is (iv) Related to cloud services in general. Some forms of threats include: service availability, poor performance, misused cloud resources.

Table 2. Group based threats of ‘‘Cloud Computing”.

No.	Group	Type of threat	Reference
1	Threats to applications	Bugs in large distributed systems	[10]
		Software Licensing	[10]
		The feat of unauthorized access	[20]
		Attacks against virtualization	[20]
		API-level attacks against cloud services	[20]
		Account or service hijacking	[19]
		Costumer data manipulation	[19]
		Eaves dropping	[19]
		Hypervisor viruses	[19]
		Using suspicious software	[21]
		Trusted transaction	[19]
		Insecure APIs	[19]
		Injection and XSS Attack	[22]
2	Threats to data	Data/Vendor Lock-In	[10], [20]

		Data Confidentiality & Auditability	[10]
		Data Transfer Bottlenecks	[10]
		Data corruption	[20]
		Data breaches	[7]
		Data scavenging	[19]
		Data leakage	[19]
		Insecure VM migration	[19]
		Improper virtual machine management	[21]
		Legal interception point	[19]
		Smartphone data slinging	[19]
		Roll back attack	[22]
		Data manipulation	[22]
		Data loss or Leakage	[22]
3	Threats to infrastructure	Scalable storage	[10]
		Infrastructure failure	[20]
		Multi-tenancy	[6]
		VM escape	[19]
		VM Hopping and Malicious VM creation	[19]
		Insecure VM migration	[19]
		Sniffing/spoofing virtual networks	[19]
		Shared technology vulnerabilities	[19]
		TCP/ Session Hijacking	[22]
4	Threats to cloud services in general	Availability of Services	[10], [20]
		Performance Unpredictability	[10]
		Scaling Quickly	[10]
		Reputation Fate Sharing	[10]
		Difficulty in detecting problems	[20]
		Old attacks with new implications	[20]
		Loss of Control	[6]
		Trust Chain in Clouds	[6]
		Abuse use of cloud computational resources	[7]
		Denial of service	[19]
		Elevation of Privilege	[22]
		Repudiation	[22]
		Wrapping attack	[22]
		Violation of SLAs	[22]
		Cloud security attacks	[7]
		Weak Service Level Agreements (SLAs)	[22]

Based on the survey results, the data obtained in this study turned out that the types of threats to cloud computing that were identified emerging from year to year were threats to service availability, data corruption, unsafe APIs (APIs (Application Programming Interface) is an application that is intended as an intermediary application between two interconnected applications, for example when we use Facebook, then we access an application called APIs [20]), and weak service-level agreements (SLA). SLA is an agreement between the service provider and the service user in the context of cloud computing [22].

But along with the development of various studies on service threats in cloud Computing,[8] is more focused on the results of his research that reviews the function to calculate how likely the threat in the context of Cloud computing can affect the occurrence of IT risks.

5. Conclusion

This article focuses more on how we can understand several types of threats that often appear in cloud computing environments. In this paper, the author gives an idea that is the author's contribution to classifying types of threats based on service resources in the context of the cloud. This grouping is determined based on the definition and scope of the types of threats.

By classifying the types of threats that exist, it is expected that companies that will or have migrated to cloud computing can reduce the possibility of this threat as early as possible. The threat to cloud computing is the responsibility of all interested parties, including users and cloud computing service providers.

With the rapid development of information technology, especially cloud computing technology, it is possible that once a type of threat or attack in the cloud computing environment will continue to grow, so this must be anticipated as soon as possible. But in this article the author still has limitations to explain how techniques to anticipate the development of threats or attacks in cloud computing today.

The author hopes to all parties, this paper can help in understanding the handling of security services in cloud computing, especially against threats that may arise in every form of cloud services, so that we can reduce as little as possible the impact of existing threats, namely IT risks in the context of cloud

Acknowledgements

Our sincere gratitude to Politeknik Pos Indonesia and Doctor of Computer Science Programs with the support to complete this research.

References

[1] K. Djemame, "A Risk Assessment Framework for Cloud Computing," 2016.

[2] M. Nada, B. Youssef, B. Brahim, and R. Boubker, "Survey: Risk assessment models for cloud computing: evaluation criteria," vol. 1, pp. 3–7, 2017.

[3] A. Rot, "Selected Issues of IT Risk Management in the Cloud Computing Model . Theory and Practice," no. Imcic, pp. 89–94, 2017.

[4] I. Shareeful, S. Fenz, E. Weippl, and H. Mouratidis, "A Risk Management Framework for Cloud Migration Decision Support," 2017.

[5] R. Wang, "Research on data security technology based on cloud storage," *Procedia Eng.*, vol. 174, pp. 1340–1355, 2017.

[6] A. Gholami and E. Laure, "Security and Privacy of Sensitive Data in Cloud Computing : A Survey of Recent Developments," pp. 131–150, 2015.

[7] T. Chou, "Security Threats on Cloud Computing," vol. 5, no. 3, pp. 79–88, 2013.

[8] A. D. Kozlov and N. L. Noga, "Risk Management for Information Security of Corporate Information Systems Using Cloud Technology," *Elev. Int. Conf. "Management large-scale Syst. Dev. (MLSD*, pp. 1–5, 2018.

[9] C. Esposito and A. Castiglione, "Challenges of Connecting Edge and Cloud Computing : A Security and Forensic Perspective," pp. 13–17, 2017.

[10] M. Armbrust, A. D. Joseph, R. H. Katz, and D. A. Patterson, "Above the Clouds : A Berkeley View of Cloud Computing," 2009.

[11] E. Mostajeran, M. Nizam, M. Mydin, M. F. Khalid, B. I. Ismail, and R. Kandan, "Quantitative Risk Assessment of Container Based Cloud Platform," 2017.

[12] C. Belbergui, "Cloud Computing : Overview and Risk Identification Based on Classification by Type," 2017.

[13] K. Lee, "Security Threats in Cloud Computing Environments 1," vol. 6, no. 4, pp. 25–32, 2012.

[14] D. Zhe, W. Qinghong, S. U. Naizheng, and Z. Yuhan, "Study on Data Security Policy Based On Cloud Storage," pp. 145–149, 2017.

[15] Q. N. Naveed and N. Ahmad, "Critical Success Factors (CSFs) for Cloud-Based," pp. 140–149, 2019.

[16] G. Wahlgren and S. Kowalski, "IT Security Risk Management Model for Cloud Computing : A Need for a New," 2013.

[17] ISACA, "COBIT 5 for Risk," 2013.

[18] Mahesh, "Data Security and Security Controls in Cloud Computing," pp. 11–13, 2016.

[19] N. Khan and A. Al-yasiri, "Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework," *Procedia - Procedia Comput. Sci.*, vol. 94, pp. 485–490, 2016.

[20] N. F. Efozia, E. Ariwa, D. C. Asogwa, O. Awonusi, and S. O. Anigbogu, "A Review of Threats and Vulnerabilities to Cloud Computing Existence," 2017.

[21] W. R. Claycomb and A. Nicoll, "Insider Threats to Cloud Computing : Directions for New Research Challenges," 2012.

[22] S. Singh, Y. Jeong, and J. Hyuk, "A Survey on Cloud Computing Security : Issues , Threats , and Solutions," *J. Netw. Comput. Appl.*, 2016.

Conference paper

ORIGINALITY REPORT

16%	10%	9%	14%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

6%

★ Submitted to Binus University International

Student Paper

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

Conference paper

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7