International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 4

ISSN: 2454-4248
563 – 567

Cloud Service Models Threats and Vulnerabilities: A Review

P. S. Suryateja
Dept. of CSE
Vishnu Institute of Technology
Bhimavaram, India
e-mail: suryateja.pericherla@gmail.com

***Abstract*—**Cloud computing is emerging as the dominant technology for provisioning resources based on demand and for moving a major part of in-house IT systems and processes away thereby reducing the management overhead and capital expenditure. Cloud computing is a conglomerate of elements from autonomic computing, grid computing, and utility computing. Majority of the services in cloud are delivered as Software-As-A-Service (SAAS), Platform-As-A-Service (PAAS), and Infrastructure-As-A-Service (IAAS). As cloud reaps the benefits from various technologies, it is also affected by the issues which beset those technologies and also create new issues. One major issue which hinder with the widespread adoption of cloud computing is security. This paper provides a classification of threats and vulnerabilities based on the service models of cloud computing. Classification of threats and vulnerabilities is an effective way for cloud administrators, cloud consumers, and other stakeholders for identifying, understanding, and addressing security risks.

Keywords*-Cloud computing, Cloud threats, Cloud vulnerabilities, Cloud threats classification, Cloud service models security issues*

*****

I. INTRODUCTION

In the recent years cloud computing is gaining traction among the researchers and industry. According to recent reports, more than 90% of the medium to large scale organizations have some kind of workload running on the cloud. The three commonly available cloud service or delivery models are SAAS, PAAS, and IAAS [10]. Let's discuss about them in detail.

Software-As-A-Service (SAAS): In SAAS, the user or consumer subscribes to a service provided by the cloud provider. The service can be email, storage, database, etc. The management overhead on consumer is very less as it is handled by the cloud provider. Examples of SAAS are Gmail, Dropbox, Facebook, Twitter etc.

Platform-As-A-Service (PAAS): In PAAS, the user or consumer subscribes for a platform or programming environment (a stack) for developing and deploying their own applications. The management overhead is shared between the consumer and provider. Consumers of PAAS have more flexibility in configuring the operating systems and other components when compared to SAAS. Examples of PAAS are Google AppEngine, Windows Azure, AWS Elastic Beanstalk, Heroku, etc.

Infrastructure-As-A-Service (IAAS): In IAAS, cloud providers virtualize the physical hardware and provide them as compute, storage, and network services to consumers. In IAAS, consumers have great flexibility in modifying the virtualized cloud infrastructure. Examples of IAAS are Amazon EC2, Amazon S3, Rackspace, Microsoft Azure, etc.

The major issue regarding the adoption of cloud computing as a complete solution for companies' IT requirements is security. According to Cloud Security Alliance, the cloud security incidents are increasing at a blazing pace. Even the large enterprises like Google, Amazon, Microsoft are not an exception for security incidents. There are several threats and vulnerabilities [10] that cause great risk to the cloud. Classifying these threats and vulnerabilities will help the cloud stakeholders in accessing the security of various components in the cloud. The rest of the paper is organized as follows. Section II presents the related work. Section III discusses about the classification of threats and vulnerabilities based on service models and finally Section IV concludes the paper.

II. RELATED WORK

As a part of the study, a total of 63 papers (shown in Figure 1) from well reputed journals and conferences are selected based on the keyword, cloud security. 10 papers were downloaded from ACM Digital Library, 19 papers were downloaded from IEEE Xplore, and 34 papers were downloaded from ScienceDirect. From this corpus of 63 papers, 35 papers were discarded which didn't contain threats and vulnerabilities of cloud computing. After processing the initial corpus, 28 papers were selected. A summary of the processing of papers is presented in Table I. Finally 9 papers were considered which were most relevant to the topic of discussion i.e., classification of threats and vulnerabilities of cloud computing.

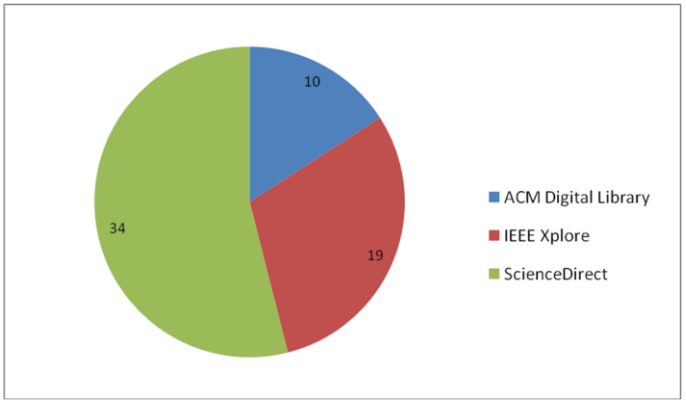

Figure 1. Illustration of papers collected from different sources

Saadi et al. [1] discusses about various security issues in cloud computing like data breach, account or service traffic hijacking, insecure interfaces and APIs, DoS (Denial of

 ISSN: 2454-4248
563 – 567

Service), shared technology vulnerabilities, insider attacks, and malware injection. They also proposed a solution for mitigating various threats that includes a decentralized cloud firewall and a HIDS (Host-based Intrusion Detection System). However, there is no classification of threats based on service models.

TABLE I. SUMMARY OF PAPERS COLLECTED FROM DIFFERENT SOURCES

Source	No. of Papers Before Processing	No. of Papers After Processing	Criteria for Discarding Papers
ACM Digital Library	10	6	Relevance to the topic of interest (threats and vulnerabilities in cloud computing)
IEEE Xplore	19	8	
ScienceDirect	34	14	
Total	63	28	

El Moctar et al. [2] lists out various issues related to cloud computing like data security, and accessibility in SAAS, relations with third parties, development life cycle, and security of the underlying infrastructure in PAAS, and issues in IAAS. They also discuss various solutions for controlling the security threats. They classified threats and vulnerabilities into five categories namely: security standards, network, access control, cloud infrastructure, and data. The classification of threats and vulnerabilities is not based on cloud service models.

N. Ahmad [3] mentions several security issues in cloud computing and classifies them into five domains: system virtualization, application programming, data, network and communication, and business and legal issues. Again the five domains are divided into several sub domains. However, classification based on service models is absent. D. Zissis et al. [4] classifies cloud security threats into three categories namely: application level (SAAS), virtual level (PAAS and IAAS), and physical level. There is no clear separation between PAAS and IAAS in the classification. Also vulnerabilities are not present in the classification.

S. Iqbal et al. [5] presents a taxonomy for cloud based attacks and vulnerabilities, and also for potential mitigation strategies with the aim of providing an in-depth understanding of security requirements in the cloud environment. Although the attacks are classified based on cloud service model, there is no clear separation between threats and vulnerabilities. M. A. Khan [6] provides a classification of attacks and countermeasures in cloud computing environment. Security issues are categorized into several types but are not based on cloud service models.

G. Ramachandra et al. [7] discusses about different cloud components, security issues, and risks, along with possible solutions that may mitigate the vulnerabilities in the cloud. They provided a list of various threats in cloud computing like: shared technology vulnerabilities, data breach, account or service traffic hijacking, DoS, malicious insider, Internet protocol, injection vulnerabilities, API and browser vulnerabilities, changes to business model, abusive use, and availability. There is no classification of these threats and vulnerabilities.

S. A. Hussain et al. [8] provides a multi-level classification of security threats across different cloud services at each layer. They also provide risk levels associated with various services at these layers. Finally they provide a way to issue dynamic contracts based on this multi-level classification for each cloud layer that decides security requirements dynamically for cloud consumer and provider. Although there is a classification of threats, there are no vulnerabilities.

A. Singh et. al. [9] describes various topics related to cloud computing like: cloud computing architecture, deployment models, different technologies associated with cloud, cloud security issues, threats, and attacks. The cloud security threats mentioned are: different service delivery/receiving model, abusive use of cloud computing, insecure interfaces and APIs, malicious insiders, shared technology issues, data loss and leakage, services/account hijacking, risk profiling, and identity theft. Although the threats are classified based on cloud service models, there are no vulnerabilities present in that. The summary of analysis conducted on existing literature is presented in Table II.

III. CLASSIFICATION OF THREATS AND VULNERABILITIES

A general list of threats in cloud computing [10] consists of data breaches, data loss, malicious insiders, DoS, vulnerable systems and APIs, weak authentication and identity management, account hijacking, shared technology vulnerabilities, lacking due diligence, APT (Advanced Persistent Threats), abuse of cloud services, a lack of responsibility, insufficient security tools, human error, ransomware, Spectre and Meltdown, and unprotected IoT devices.

The vulnerabilities associated with data breaches are targeted attacks, simple human errors, application vulnerabilities, and poor security policies. The service models that might be affected by these vulnerabilities are SAAS, PAAS, and IAAS. The vulnerabilities associated with data loss are natural disasters, simple human errors, hard drive failures, power failures, and malware infection. These vulnerabilities might affect IAAS. The vulnerabilities associated with malicious insiders are former employees, system administrators, third party contractors, business partners. These vulnerabilities might affect SAAS, PAAS, and IAAS.

DoS threats are associated with weak network architecture, insecure network protocols, and application vulnerabilities. These vulnerabilities might affect SAAS, PAAS, and IAAS. Vulnerable systems and APIs are associated with weak API credentials, key management, operating system bugs, hypervisor bugs, and unpatched software vulnerabilities. These vulnerabilities might affect SAAS, PAAS, and IAAS. Weak authentication and identity management is associated with social engineering attacks, MITM (Man-In-The-Middle) attacks, and malware infection vulnerabilities. These vulnerabilities might affect SAAS, PAAS, and IAAS.

The vulnerabilities associated with account hijacking are social engineering attacks, MITM attacks, and malware infection. These vulnerabilities might affect SAAS, PAAS, and IAAS. The vulnerabilities associated with shared technologies are VM (Virtual Machine) vulnerabilities,

 ISSN: 2454-4248
563 – 567

hypervisor vulnerabilities, and third party software vulnerabilities. These might affect PAAS and IAAS. The vulnerabilities associated with lacking due diligence are no auditing and SLA (Service Level Agreement). These vulnerabilities might affect SAAS model.

APTs (Advanced Persistent Threats) are associated with spear phishing or whaling, direct hacking, USB malware, network penetration, and third-party API vulnerabilities. These vulnerabilities might affect SAAS, PAAS, and IAAS. The vulnerabilities associated with abuse of cloud services are no cloud service monitoring and SLAs. These might affect PAAS, IAAS models. Insufficient security tools threat might affect SAAS and IAAS models. The vulnerabilities associated with human error are human negligence and insufficient security training. These might affect SAAS and IAAS.

The vulnerabilities associated with ransomware threat are infrastructure vulnerabilities, platform vulnerabilities, and application vulnerabilities. These vulnerabilities might affect SAAS and IAAS. Spectre and Meltdown threat is associated with hardware design vulnerabilities. These might affect IAAS. Finally, unprotect IoT devices are associated with vulnerabilities like weak device management, network vulnerabilities, and hardware vulnerabilities. These vulnerabilities might affect SAAS and IAAS. The summary of threats and vulnerabilities classification based on cloud service models is presented in Table III.

IV. CONCLUSION

More and more organizations are moving to the cloud day-by-day and there is a need to focus on the security of data and other resources to decrease the risks. This paper gives a general overview of threats and the associated vulnerabilities in cloud computing and also classifies them based on cloud service models: SAAS, PAAS, and IAAS. This provides cloud stakeholders with a reference for addressing the security gaps. The widely referenced solution in literature for protecting data is encryption [12]. Future work is to survey various solutions available to mitigate the cloud security threats and simulate some of them using a cloud simulator [11] or in a live testbed using OpenStack.

REFERENCES

[1] C. Saadi and H. Chaoui, “A new approach to mitigate security threats in cloud environment,” in Proceedings of the Second International Conference on Internet of things and Cloud Computing - ICC ’17, 2017, pp. 1–7.

[2] C. B. O. M. El Moctar and K. Konate, “A survey of security challenges in cloud computing,” 2017 Int. Conf. Wirel. Commun. Signal Process. Netw., no. 1, pp. 843–849, 2017.

[3] N. Ahmad, “Cloud Computing : Technology , Security Issues and Solutions,” 2017.

[4] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Futur. Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, 2012.

[5] S. Iqbal, M. L. Mat Kiah, B. Dhaghighi, M. Hussain, S. Khan, M. K. Khan, and K. K. Raymond Choo, “On cloud security attacks: A taxonomy and intrusion detection and prevention as a service,” J. Netw. Comput. Appl., vol. 74, pp. 98–120, 2016.

[6] M. A. Khan, “A survey of security issues for cloud computing,” J. Netw. Comput. Appl., vol. 71, pp. 11–29, 2016.

[7] G. Ramachandra, M. Iftikhar, and F. A. Khan, “A Comprehensive Survey on Security in Cloud Computing,” in Procedia Computer Science, 2017, vol. 110, no. 2012, pp. 465–472.

[8] S. A. Hussain, M. Fatima, A. Saeed, I. Raza, and R. K. Shahzad, “Multilevel classification of security concerns in cloud computing,” Appl. Comput. Informatics, vol. 13, no. 1, pp. 57–65, 2017.

[9] A. Singh and K. Chatterjee, “Cloud security issues and challenges: A survey,” J. Netw. Comput. Appl., vol. 79, pp. 88–115, 2017.

[10] P. S. Suryateja, “Threats and Vulnerabilities of Cloud Computing: A Review”, International Journal of Computer Sciences and Engineering, Vol.6, Issue.3, pp.297-302, 2018.

[11] P. S. Suryateja, "A Comparative Analysis of Cloud Simulators," Int. J. Mod. Educ. Comput. Sci., vol. 8, no. 4, pp. 64–71, 2016.

[12] B.SriVarsha, P.S.Suryateja, "Using Advanced Encryption Standard for Secure and Scalable Sharing of personal Health Records in Cloud," International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5(6), 7745-7747, 2014.

 ISSN: 2454-4248
563 – 567

TABLE II. SUMMARY OF ANALYSIS CONDUCTED ON EXISTING LITERATURE

Reference	Author(s)	Title of Paper	Gap Identified
[1]	Saadi et al.	A new approach to mitigate security threats in cloud environment	Mentioned only security issues. There is no classification based on service models.
[2]	El Moctar et al.	A survey of security challenges in cloud computing	Security issues are classified into different categories. Not based on service models.
[3]	N. Ahmad	Cloud Computing : Technology , Security Issues and Solutions	Security issues are classified into different categories. Not based on service models.
[4]	D. Zissis et al.	Addressing cloud computing security issues	Threats are classified based on service models. Vulnerabilities are absent.
[5]	S. Iqbal et al.	On cloud security attacks: A taxonomy and intrusion detection and prevention as a service	Threats are classified based on service models. Vulnerabilities are absent.
[6]	M. A. Khan	A survey of security issues for cloud computing	Security issues are classified into different categories. Not based on service models.
[7]	G. Ramachandra et al.	A Comprehensive Survey on Security in Cloud Computing	Mentioned only security issues. There is no classification based on service models.
[8]	S. A. Hussain et al.	Multilevel classification of security concerns in cloud computing	Threats are classified based on service models. Vulnerabilities are absent.
[9]	A. Singh et. al.	Cloud security issues and challenges: A survey	Threats are classified based on service models. Vulnerabilities are absent.

TABLE III. CLASSIFICATION OF THREATS AND VULNERABILITIES BASED ON CLOUD SERVICE MODELS

Threat No.	Threat Name	Possible Vulnerabilities	Service Model(s) Susceptible to Vulnerabilities
T01	Data Breaches	Targeted Attack	SAAS, PAAS, IAAS
		Simple Human Errors	
		Application Vulnerabilities	
		Poor Security Policies	
T02	Data Loss	Natural Disasters	IAAS
		Simple Human Errors	
		Hard Drive Failures	
		Power Failures	
		Malware Infection	
T03	Malicious Insiders	Former Employee	SAAS, PAAS, IAAS
		System Administrator	

 ISSN: 2454-4248
563 – 567

		Third Party Contractor	
		Business Partner	
T04	Denial of Service (DoS)	Weak Network Architecture	SAAS, PAAS, IAAS
		Insecure Network Protocol	
		Vulnerable Application	
T05	Vulnerable Systems and APIs	Weak API Credentials	SAAS, PAAS, IAAS
		Key Management	
		Operating System Bugs	
		Hypervisor Bugs	
		Unpatched Software	
T06	Weak Authentication and Identity Management	Social Engineering Attacks	SAAS, PAAS, IAAS
		Man-In-The-Middle (MITM) Attack	
		Malware Infection	
T07	Account Hijacking	Social Engineering Attacks	SAAS, PAAS, IAAS
		Man-In-The-Middle (MITM) Attack	
		Malware Infection	
T08	Shared Technology Vulnerabilities	VM Vulnerabilities	PAAS, IAAS
		Hypervisor Vulnerabilities	
		Third-Party S/W Vulnerabilities	
T09	Lacking Due Diligence	No Auditing	SAAS
		Service Level Agreement	
T10	Advanced Persistent Threats (APT)	Spear Phishing or Whaling	SAAS, PAAS, IAAS
		Direct Hacking	
		USB Malware	
		Network Penetration	
		Third-Party APIs	
T11	Abuse of Cloud Services	No Cloud Service Monitoring	PAAS, IAAS
		Service Level Agreement	
T12	A Lack of Responsibility	Human Negligence	SAAS, IAAS
		Service Level Agreement	
T13	Insufficient Security Tools	--	SAAS, IAAS
T14	Human Error	Human Negligence	SAAS, IAAS
		No or Insufficient Security Training	
T15	Ransomware	Infrastructure Vulnerabilities	SAAS, IAAS
		Platform Vulnerabilities	
		Application Vulnerabilities	
T16	Spectre and Meltdown	Hardware Design Vulnerabilities	IAAS
T17	Unprotected IoT Devices	Weak Device Management	SAAS, IAAS
		Network Vulnerabilities	
		Hardware Vulnerabilities	