Journal of Physical Sciences, Vol. 24, 2019, 133-141
ISSN: 2350-0352 (print), www.vidyasagar.ac.in/publication/journal
Published on 6 June 2019

A Survey on Security Challenges in Cloud Computing

D. I. George Amalarethinam[1] and S. Edel Josephine Rajakumari[2]

[1]Department of Computer Science
Jamal Mohamed College (Autonomous), Tiruchirappalli – 620020
Tamil Nadu, India. Email: di_george@ymail.com
[2]Department of Computer Science, Holy Cross College (Autonomous)
Tiruchirappalli – 620002, Tamil Nadu, India.
Email: edeltheprincess@gmail.com

ABSTRACT

Cloud Computing is an innovative paradigm that offers computing resources such as network, storage, servers, applications and services when there is a demand, based on pay-as-you go principle. In Cloud computing, the resources are shared by Cloud consumers. Cloud provides computing infrastructure with a development platform on which users can develop their own applications. It diminishes the capital expenditures to be spent on applications development. The cloud consumers can avail the resources from anywhere at any time with an internet service. Though Cloud has several advantages, it has certain security challenges to be resolved. In this paper, the Security Challenges of Cloud Computing in various aspects are discussed.

Keywords: Cloud, resources, services, applications, authentication, security, denial of service, distributed denial of service.

1. Introduction

Cloud computing is a boon to the fast growing Information Technology world. It introduces the concept of virtualization of resources as services which includes network, storage, servers, applications and services. Where there is an internet connection, the cloud service is accessible. The computing resources are pooled over a cloud that can be provisioned to the users when they need them. The users will be charged only for what they consumed from the cloud. This facilitates the small and medium scale businesses by reducing the capital expenditures of deployment of the resources at sites.

The NIST describes Cloud Computing as "A model for enabling ubiquitous, 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" [1]. The Cloud model has five vital characteristics: a) on-demand self-service, b) broad network access, c) resource pooling, d) rapid elasticity and e) measured/metered service.

A. Cloud Service Models

There are three types of Cloud services popularly used: a) SaaS – Software as a Service (applications), b) Paas-Platform as a Service (Operating Systems, Database,

development tools) and c) IaaS – Infrastructure as a Service (Servers, Storage, network, virtual machines).

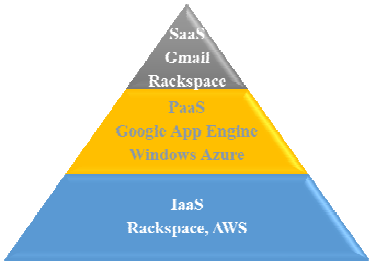

Figure 1.1: Cloud service models

B. Cloud deployment models

A Cloud deployment models is a specific type of Cloud environment, distinguished by its ownership, size and access. The four common deployment models are

a) Private Cloud – It is solely for an organization.

b) Public Cloud – General people can access the Cloud.

c) Community Cloud – Organizations having similar kind of requirements can share the cloud Infrastructure.

d) Hybrid Cloud – any combination of Private, Public and community clouds.

C. Benefits of cloud computing

a) **Low Costs** – There will be no capital expenditures for installing hardware and software. With an internet connection, resources can be obtained from a Cloud Service Provider (CSP).

b) **24×7 Availability** – The cloud services are accessible from anywhere at any time without service provider interaction.

c) **Elasticity** – Sometimes the demand for resources may be high; sometimes may be low. According to the resources' demand, the services will be available to the consumers without delay.

d) **Automated Updates** – It is the responsibility of CSPs, to updating and maintaining the Software in the Cloud environment.

e) **Pay as you go** – the consumers will be charged only for the resources they consumed from the cloud.

2. Security challenges in cloud computing

Cloud virtually offers resources as services to its consumers based on their subscription. Though, it has several advantages over traditional computing, there are certain challenges need to be encountered. Some of the major challenges are discussed in this section:

a) Reliability

The consumers' data are stored in third party's server. They do not know where or which machine their data are stored. They are not aware of what security mechanisms provided to safeguard their data [2].

b) Privacy
Cloud consumers store their personal data into cloud that is stored in some physical machines scattered around the world. All the data transferred only through internet. It is not guaranteed that the data cannot be hacked by malicious users.

c) Bandwidth
When the demands for resources are high or large volume of data to be stored in the cloud, high bandwidth will be required.

d) Availability
At times, when huge amounts of resources are to be served at a time, the cloud becomes unable to meet all the consumers' demands.

e) Integrity
It is to be ensured that the correctness and trustworthy of the consumers' data. The data should not be illegally tampered, improperly modified, deliberately deleted or maliciously fabricated.

f) DoS
Denial of Service attack launched by malicious users by selecting a victim machine and sending bulk requests to the machine at the same time, the services will be made unavailable to the authentic users.

g) DDoS
A Distributed Denial of Service (DDoS) is a type of attack launched by distributed attackers to exhaust the available resources which results in server unresponsiveness and service unavailability so that the legitimate users cannot gain access to the resource.

h) Authentication
Every cloud user should be authenticated before accessing the resources.

i) Access control
The cloud users must be categorized and given permissions according to the type of the users. Malicious users might try to hack other user's account.

3. Review of literature

Asma et. al. [2] enlisted the information security issues in Cloud Service models. The Security issues in SaaS are Availability, Confidentiality, Privacy and Integrity. In PaaS, information theft, distrust hypervisor and distrusted virtual machines are considered as major security issues. Malicious Virtual machines, Denial of Service (DoS) are issues in IaaS.

B. Hari Krishna et. al. [3] highlighted some major security threats of cloud computing:

a) Attacks by other customers

b) Shared Technology Vulnerabilities

c) Failures in Provider Security

d) Availability and reliability issues

e) Legal and regulatory issues

f) Insecure APIs

g) Data loss/leakage

h) Malicious insiders

i) Unknown risk profile

j) Account, Traffic Hijacking & Service

Ramachandra et. al. [4] discussed the major threats and open security issues: Data breach, IP spoofing, ARP spoofing, DNS poisoning, SQL injection, OS injection, LDAP injection, cloud orchestration and zombie or DDoS.

Iyenger and Ahamed [5] have made a detailed review on DDoS attack and mitigation techniques in Cloud computing environment. DDoS is an extensive effect of Denial of Service (DoS), the difference is the volume and vulnerability of the attack launched and the number of attackers attempt to attack the server resource. There are three types of DDoS attacks viz., volumetric attacks, protocol attacks and application layer attacks. Some variants of DDoS attacks are UDP flood, SYN flood, ICMP flood, HTTP flood, NTP flood, ping of death and slowloris. The effects of DDoS are business loss, loss of fame and revenue loss for product owners.

Jain and Jaiswal [6] focused the parameters that affect cloud security: cloud network, database, operating system, virtualization, resource allocation, transaction management, load balancing, and concurrency control and memory management. They categorize the cloud security issues as follows: Data issues, privacy issues, and infected application and confidentiality issues. Also they proposed a layered framework for cloud security which comprises virtual network monitor layer, cloud data layer, cloud storage layer and virtual machine layer.

Vurukonda and Rao [7] have classified cloud security challenges into data storage issues, identity management & access control, contractual and legal issues. The issues are further classified into Data storage issues: Data privacy & integrity, data recovery & vulnerability, improper media sanitization and data backup. Identity management and access control: malicious insider and outside intruder. Contractual and Legal issues: Service Level Agreements (SLAs) and legal issues.

Nadeem [8] has made a survey on Cloud Security issues and Challenges. The survey articulates the following: Browser based vulnerabilities such as SSL certificates spoofing, phishing and attacks on browser cache. Integrity of data is affected by weak encryption, lack of control over audit, authorization and authentication. Also it leads to data theft and data loss. Weak passwords, key loggers and other fraudulent mechanisms lead to identity theft.

Ughade and Chopde [9] discussed about top five threats in Cloud computing in their survey paper. The threats are Data breach, Data loss, insecure interfaces and APIs, Denial of Service and Account or service traffic hijacking. Also social engineering attack,

malware injection attack and phishing attack are conferred. Blowfish and MD5 security algorithms also described in the paper.

Sun et. al. [10] focused on data security and privacy issues. They define security as the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information and availability and the prevention of unauthorized withholding of information. The major issues in cloud computing are resource security, resource management and resource monitoring. Cloud security can be divided into four subcategories: safety mechanisms, cloud server monitoring or tracing, data confidentiality and avoiding malicious insiders' illegal operations and service hijacking.

An et. al. [11] enlisted the following to be considered as security issues in cloud computing: Data at rest, Data theft, Data loss, natural disaster and physical data location. Also privacy and application issues are examined.

Subashini and Kavitha [12] have surveyed on security issues in service delivery models. Data Security issues in SaaS model are Cross-site scripting (XSS), Access control weaknesses, OS and SQL injection flaws, Cross – site request forgery (CSRF), cookie manipulation, insecure storage and insecure configuration. Network security issues such as network penetration and packet analysis, session management weaknesses and insecure SSL trust configuration are validated in SaaS model.

Varsha et. al. [13] surveyed security issues in Cloud computing and determined top seven security issues discovered by Cloud Security Alliance (CSA). Multi-tenancy is observed as the major security issue in the paper.

Wei et. al. [14] introduced the two major classes of cloud security: Cloud Storage Security (CSS) and Cloud Computation Security (CCS). CSS means the integrity of stored data at unreliable cloud servers. CCS indicates the correctness of the computation performed by unreliable cloud servers. A novel basic SecCloud protocol was proposed and its operations were elaborately discussed in the paper. Three types of attacks were summarized in the paper viz. Storage cheating attack model, Computation cheating attack model and Privacy cheating attack model. Also, Security and Performance analysis were made to prove the efficiency of the proposed protocol. The SecCloud protocol eradicates both the storage and computation issues of cloud computing.

Gupta et. al. [15] presented taxonomy of security issues, taxonomy of DDoS attacks in cloud, and taxonomy of DDoS defense mechanisms in cloud environment. The paper evidently described the mechanism of DDoS attack and the defense measures of it. Also, several security issues of Cloud were discussed in the paper. The possible security issues in Cloud service delivery models are DoS attack, DNS Server attack, IP-based attacks, Impersonation, Cross-VM attack, Data breaches, privacy breaches, Session hijacking, Access control violation, physical damage of infrastructure, etc.. Furthermore, strengths and weaknesses of DDoS defense methods were enlisted in the paper.

Khan et. al. [16] discussed the cloud security issues such as multi-tenancy, elasticity, insider attacks, outsider attacks, Loss of control, data leakage, etc., and suggested some techniques to secure data in cloud. The security techniques are authentication and

identity, Data encryption, Information integrity and privacy, secure information management, malware-injection attack solution and flooding attack solution. The security standards such as Security Assertion Markup Language (SAML), Open Authentication, OpenID and SSL/TLS are recommended to keep up a secure cloud environment.

Authors	**Security Issues enlisted**	**Countermeasures/ solutions recommended**
Anjum Asma et. al. [2]	Availability Confidentiality Privacy Integrity	Redundancy Data Encryption OTP, digital certificate & biometric verification Rain-6 & digital signature
B. Hari Krishna et. al. [3]	Regulatory Compliance Data Segregation Data Location Insecure APIs Data loss/leakage	Discovery key cloud provider Clear Contract Recovery facilities Enhanced Enterprise infrastructure Data Encryption
Gururaj Ramachandra et. al. [4]	Data breach IP spoofing ARP spoofing, DNS poisoning SQL injection LDAP injection cloud orchestration Zombie or DDoS.	End-end encryption Scanning for malicious activities Validation for cloud consumer Secure interfaces and APIs Secure leveraged resources
N Ch Sriman Narayana Iyenger et. al. [5]	DDoS	DDoS Defence Mechanisms: Multilevel Trust Filtration Trilateral Trust Fuzzy Logic based mechanism Layered Load Balancing Chaotic theory based mechanism
Gaurav Jain et. al. [6]	Data issues privacy issues infected application confidentiality	Verify the access controls Control the consumer access devices Monitor the data access Share demanded records & verify the data deletion A layered framework for security
Muhammad Aamir Nadeem [8]	SSL certificates spoofing Phishing	Intrusion Prevention System (IPS) Intrusion Detection System

	weak encryption lack of control over audit authorization authentication data theft data loss Weak passwords key loggers identity theft	(IDS) Firewalls business continuity plan disaster recovery plan
Kapil A. Ughade et. al. [9]	Data breach Data loss insecure interfaces and APIs Denial of Service Account or service traffic hijacking social engineering attack malware injection attack phishing attack	Blowfish Algorithm MD5 Algorithm
Y Z An et. al. [11]	Data at rest Data theft Data loss natural disaster physical data location	Vulnerability shielding (IDS) Trusted Cloud Service Provider Security check events Data storage regulations Facilities for recovery Identification management and authentication
Lifei Wei et. al. [14]	Storage cheating attack Computation cheating attack Privacy cheating attack	Basic SecCloud Protocol Advanced SecCloud Protocol
Gupta, B.B. et. al. [15]	DoS attack DNS Server attack IP-based attacks, Impersonation Cross-VM attack Data breaches privacy breaches Session hijacking Access control	DDoS defense mechanisms

	violation physical damage of infrastructure	
Shaireen Khan et. al. [16]	Multi-Tenancy Elasticity Insider attacks Outsider attacks Loss of control Data Leakage Abuse of Cloud services Malware injection DoS	Authentication and Identity Data Encryption Information Integrity and Privacy SLA Secure Information Management Malware injection attack solution Flooding attack solution SAML OAuth OpenID SSL/TLS

Table 1: Security issues and recommended solutions

4. Conclusion

Cloud computing has been completely transformed the traditional computing practices to innovative, optimized and cost-effective computing methods. It offers incredible benefits to the computing world and it leads the IT to an advanced level of modernization. With an internet connection and a Cloud, everything becomes possible in the IT realm. Yet, there are some challenges regarding secure information sharing in the cloud need to be resolved. There are several researches going on providing numerous security mechanisms to Cloud computing. In this paper, the security issues of cloud and some security mechanisms to eradicate them are concentrated and emphasized. Although existing security measures are need to be enhanced for providing more security in the cloud environment.

REFERENCES

1. Peter Mell and Timothy Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication, 14 (2011) 800 – 145.
2. Anjum Asma, Mousmi Ajay Chaurasia and Hala Mokhtar, Cloud Computing Security Issues, International Journal of Application or Innovation in Engineering & Management, 1(2) (2012) 141 - 147.
3. B. Hari Krishna, S.Kiran, G. Murali and R. Pradeep Kumar Reddy, Security Issues in Service Model of Cloud Computing Environment, International Conference on Computational Science, Elsevier publications, (2016) 246 – 251.
4. Gururaj Ramachandra, Mohsin Iftikhar and Farrukh Aslam Khan, A Comprehensive Survey on Security in Cloud Computing, Elsevier publications, (2017) 465 – 472.

5. N Ch Sriman Narayana Iyenger and Junath Naseer Ahamed, A Review on Distributed Denial of Service (DDoS) Mitigation Techniques in Cloud Computing Environment, International Journal of Security and its Applications, (2016).
6. Gaurav Jain and Arti Jaiswal, Security Issues and their Solution in Cloud Computing, Concepts Journal of Applied Research, 2(3) (2018) 1 - 6.
7. Naresh vurukonda and Thirumala Rao, A study on Data Storage Security Issues in Cloud Computing, Elsevier publications, (2016) 128-135.
8. Muhammad Aamir Nadeem, Cloud Computing: Security Issues and Challenges, Journal of Wireless Communications, 1 (2016) 10 – 15.
9. Kapil A. Ughade and Nitin R. Chopde, Survey on Security Threats and Security Algorithms in Cloud Computing, International Journal of Science and Research, 4 (4) (2015) 2196-2200.
10. Yunchuan Sun, Junsheng Zhang, Yongping Xiong and Guangyu Zhu, Data security and privacy in cloud computing, International Journal of Distributed Sensor Networks, 10 (7) (2014) 1 - 9.
11. Y.Z.An, Z.F.Zaaba and N.F.Samsudin, Reviews on Security Issues and Challenges in Cloud Computing, IOP Conference Series: Materials Science and Engineering, 160 (1) (2016).
12. S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, 34 (2011) 1-11.
13. Varsha, Amit Wadhwa and Swati Gupta, Study of security issues in cloud computing, International Journal of Computer Science and Mobile Computing, 4 (6) (2015) 230 - 234.
14. Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen and Athanasios V. Vasilakos, Security and privacy for storage and computation in cloud computing, Information Sciences, 258 (2014) 371–386.
15. K.Bhushan and B.B.Gupta, Security challenges in cloud computing: state-of-art, Int. J. Big Data Intelligence, 4 (2) (2017) 81-107.
16. Shaireen Khan, Shadab Hasan, Shashank Singh, Sumera Zafar and Shobhit Joshi, Cloud computing: security issues and security standards, International Journal of Engineering and Management Research, Special Issue (ACEIT - 2018) 31-36.