SN Computer Science (2020) 1:329
https://doi.org/10.1007/s42979-020-00353-2

SURVEY ARTICLE

Cloud Computing Security Issues: a Stakeholder's Perspective

Garima Verma[1] · **Sandhya Adhikari**[2]

Received: 25 July 2020 / Accepted: 28 September 2020 / Published online: 10 October 2020

Abstract
Cloud computing is a rising technology that has gained significant attention over past decades. It offers various features such as-on-demand access, broad-network access, unlimited resource pool, etc. Despite so many merits, cloud computing has been full several challenges. Security indeed has remained one of the biggest challenges. Researchers, all over world, have been working on designing different types of security mechanism which can work on different levels on cloud environment. However, the literature on cloud security is quite wide and touches several issues pertaining to different stakeholders. The current study addresses the above issue by presenting a detailed review of challenges of security that are faced by different stake holders, such as cloud service provider (CSP), cloud user (CU), etc. This study will help the various researchers to find all security concerns at one place with critical reviews.

Keywords Cloud computing · Security · Cloud service provider · Cloud user

Introduction

The cloud computing has become an inseparable part of day-to-day business life. Around the world, most organizations are using cloud-based services in the form of either platform-as-a-service (PaaS), software-as-a-service (SaaS), or infrastructure-as-a-service (IaaS) [1]. The main benefits gained by these organizations are that they can expand their business with less expenditure in infrastructure, pay as per use payment models and less investment for skills that are generally required for updation of any new technology [2]. But generally in view of benefits and cost-effective solutions, many organizations, small as well as big, do not pay much attention towards the security threats and different challenges of cloud environment. Sometimes, these challenges become so dangerous that these can result in great loss in terms of data hacking, privacy of customers, integrity of information, etc. [3, 4]. Security is always a key component whenever we talk about any technology based on open network, i.e., Internet. Same with cloud computing also, because it is also based on Internet. However, the difference lies in cloud security and other technologies when we talk about the different components responsibility towards managing security. The cloud service provider (CSP) is one of the stake holders who should be responsible for handling security of applications, operating System (OS), network traffic, and infrastructure [1, 4]. Similarity cloud user (CU) is another stakeholder who is responsible for handling security for user access, data, and applications to the some extent. Table 1 shows the usual distribution of responsibilities for different security components for different types of cloud services [5].

Table 1 represents only the ideal scenario for distribution of responsibilities. Sometimes, CSP can define these responsibilities in different manner outlined by the service-level agreement (SLA) [6]. The CU should be well aware about all the concerns before signing on the legal agreement.

The remaining paper is organized as follows: Sect. "Related Work" will present the detailed literature review; Sect. "Conclusion" will cover the security challenges for different stake holder levels also. At the end, Section 4 will draw the conclusion.

This article is part of the topical collection "Computational Statistics" guest edited by Anish Gupta, Mike Hinchey, Vincenzo Puri, Zeev Zalevsky, and Wan Abdul Rahim.

✉ Garima Verma
garima.verma@dituniversity.edu.in

[1] School of Computing (IT), DIT University, Dehradun, India

[2] School of Computing (CSE), DIT University, Dehradun, India

Table 1 Distribution of responsibilities for different security components

Security component	Infrastructure as a service	Platform as a service	Software as a service
User access management	CU	CU	CU
Data access	CU	CU	CU
Applications	CU	CU	CSP
Operating system	CU	CSP	CSP
Network traffic	CU	CSP	CSP
Hypervisor	CSP	CSP	CSP
Infrastructure	CSP	CSP	CSP
Physical	CSP	CSP	CSP

Related Work

Security Challenges

Researchers have covered various aspects of security in cloud in their works, such as cloud security issues and related challenges, attack vectors associated with architectural components [3, 7, 8]. If we talk about the business organization, then biggest challenge for them is that they need to be aware always with different type of risks at different level. Because, as the popularity of the technology increases new challenges comes in the scenario. Table 2 presents a list of some security challenges in cloud and possible solutions for organizations.

Morsy et al. 2010 present the detailed analysis of security aspects in cloud environment. They have taken various perspectives for survey such as architecture of cloud, characteristics of cloud, stake holders and delivery models, etc. All the services in cloud bind with high dependency stack. The PaaS delivery model is built over IaaS; similarly, SaaS is built over PaaS, which means that the security complicacy of one layer makes compilations is another layer as well [14]. Takabi et al. 2010 explored various distinctive issues with cloud computing environment that creates security and privacy challenges. The authors discussed various issues in various levels such as authentication, virtualization, access control, etc. [15]. The article also elaborates some approaches that user can follow when moving towards cloud-based services. Vulnerabilities play the most important role in any open access system. It always shows the risk of attacks. The vulnerabilities possible in cloud environment are discussed by Grobauer et al. 2011, which can be defined in areas such as—it can be due to core technologies such as web, virtualization, etc., possible due to essential characteristics defined in National Institute of Standards and Technology (NIST) model [1, 4]. There are five categories of cloud security defined by Khalil et al. 2014, security standards are defined protocols that should be defined by the company for providing cloud services, network security involves various types of attacks such as DoS, DDoS etc., access control deals with the data privacy issues of the user, cloud infrastructure is a security category which covers all the attacks target in the delivery models, and last category defined by author is data, which covers security issues related with migration of data, confidentiality of data, integrity of data, etc. [3]. Cloud service models' major security issues are discussed by Anjana et al. 2018, the major responsibilities of CSP and CU decided by the cloud service models, as shown in Table 1. Apart from these security issues on delivery models, authors discussed about various threats such as weak API, covert channels by virtual machines (VMs), intruder can modify data, etc. Some counter measures suggest by authors with reference to the defined attacks such as identity management, dynamic credentials, digital signatures, etc. [5]. Table 3 shows the comparative analysis of the different related works [5–10, 14, 16–19], etc.

Security Concerns of Stakeholders

According to NIST reference architecture, there are five major stakeholders to perform task in cloud computing [1]: cloud service provider (CSP), cloud user or consumer (CU), cloud broker, cloud auditor, and cloud carrier.

Cloud User (CU)

The major stakeholders for cloud computing are cloud user or consumer (CU), cloud service providers (CSP), cloud auditor, and cloud broker [20]. The CU is the most affected stakeholder if any kind of breach happens over cloud. According to the recommendation ITU-T X.160, the major threats and challenges for CU are [20]:

- Secure access to the services—the main concern of CU is to access the services in a secure way and will share services only to the trusted entities. Any kind of loop hole can create major loss for CU.
- Data security—the user is always interested in the updation of its own data, but this concern is also subject to the unauthorized access also.
- Confidentiality and privacy—the data confidentiality is also one of the major concerns on cloud. The threat is there, because the data of CU are handled by third party and it has full control on data. If while processing any type of attack for example man in middle attack happens, then the confidentiality will be breach.
- Data control—certain level of control on data in cloud.
- Service availability—the cloud-based services taken by the user should be available all the time and at all places.

Table 2 Common challenges with cloud-based services

Challenge	Description	Possible solutions
Absence of visibility and control over assets	One of the greatest merits of using cloud-environment technologies is, the consumer is not responsible for the maintenance of resources such as hired servers. However, this becomes one of the de-merit as well topic of concern for customers giving the responsibility for day-to-day maintenance of a hired resources such as software services, platform services, or computing (infrastructure) asset may result in having lack of control over that rented assets [1, 9]	Verify the ability of security controls Prepare event response plans beforehand Analyze information about their data, services, and clients for abnormal usage patterns (if any) which can lead to security breach
Some cloud service providers may not fulfill security measures according to the industry protocols	There are various security compliance regulations that organizations have to meet, such as General data protection regulation (GDPR), Payment card industry (PCI) data security regulation, Health insurance portability and accountability act (HIPAA), etc. [10]. If organization fails to meet these standards then it may result in penalties or fines, which can impact negatively on the image of organization. But in actual all CSP do not offer security measures according to the industry protocols. If company takes cloud-based service without verifying industry required standards then it may result in audits and penalties of the business	First, verify with the CSP which regulatory standards they offer [8]
Issues of data privacy	If an organization accepts the cloud-based services, means it gives the complete rights of data to a third party. The organization can face problems of great risk in this situation. There can be possibility of data breach, if there is no provision of data security in the adopted cloud service [11]	Before going for adoption of cloud-base service, define level of privacy required Choose vendors who can provide required service with the required data privacy provisions [11]
Event log management and notification	It is already discussed that the organization does not have control of data and visibility. On cloud if the network gets compromised, then problem is to identify what resources and data are compromised. If the cloud provider does not offer the management of event logs, then it is almost impossible to track the affected resource or data [12]	Before taking services, check what type of event log services CSP provides If data breach situation has occurred, then inform all the possible clients for that [12]
User access control management	If the organization is taking cloud-based services, then it is a major security challenge that what type of user access control it should have. Especially it becomes a critical issue if the service does not offer strong control settings [13]	Check the access control management policy beforehand If possible, then suggest them to add control settings as per your requirements [13]
Security risk due to vendor lock-in	Vendor lock-in is a situation where the customer is dependent on the technology of one cloud service vendor and cannot migrate to the other one due to the issues of interoperability. If critical data are on cloud, the migration creates various security issues [2]	It is always important to have flexibility to change providers whenever required, for that better to keep some critical components in-house instead on cloud [2]

Table 3 Comparative analysis of the related work

Study	Year	Type of Study	Purpose	Basic Cloud features	Virtualization and virtual machine	Issues covered	Security and privacy mechanisms or approaches (Identity, access, encryption n, trust, etc.)	Results
Neumann et al. [6]	2010	Survey	Discussed security with respect to the cloud architecture, characteristics, stakeholders, and delivery models	Yes	No	Security for architecture components	Yes	Suggested some security enablers technology that can be used in cloud computing such as- identity management, key management, security performance trade-off, etc
Almorsy et al. [14]	2010		Illustrates the distinct issues of cloud computing that creates security and privacy challenges in clouds	Yes	Yes	Security and Privacy Challenges and Approaches	Yes	discussed various approaches to address security challenges and explore the future work needed to provide a trustworthy cloud computing environment
Grobauer et al. [4]	2011	Survey	Main discussions is done on cloud vulnerabilities	Yes	No	Vulnerabilities in all aspects such as vulnerabilities in cloud characteristics, vulnerabilities in architecture, etc.	Yes but is short	Suggested and explored various types of vulnerabilities and their possible outcomes
Khalil et al. [3]	2014	Survey	1. Authors detected the cloud vulnerabilities and perform the classification of known security threats and attacks with the present solutions to control, reduce, or prevent them 2. Identification of limitation of current practices to draw future perspectives	No	Yes	Cloud security framework containing various boundaries of defense also identification of the dependency levels being identified among them	Yes	1. As a result 28 cloud security threats being classified into 5 categories, namely: security standards, network, access, cloud infrastructure, and data 2. Identification of 9 attack classes with present countermeasures and a comparison between them on the basis of effectiveness and the shortcomings of the proposed solutions is given

Table 3 (continued)

Study	Year	Type of Study	Purpose	Basic Cloud features	Virtualization and virtual machine	Issues covered	Security and privacy mechanisms or approaches (Identity, access, encryption n, trust, etc.)	Results
Phaphoom et al. [9]	2015	Survey	The main purpose of the paper to define the impact of technical and security-related barriers for the organizational decision if they adopt cloud	No	No	Security, privacy of data, and portability	No	Logistic regression analysis is done, the results shows the significant increase in the level of concern on security, data privacy, and portability for vendor lock-in The decision of cloud adoption in enterprises
Hsu et al. [10]	2015	Survey	The main purpose of the paper was to apply the technology–organization–environment framework for investigating the determinants of cloud computing service adoption behavior	No	No	Different factors like technology, organization, environment, and control variable for cloud adoption behavior	No	Descriptive statistics and model assessment strategy applied and found that, discussed factors were positively related to intention to adopt cloud computing services
Ardagna et al. [7]	2015	Survey	The main purpose of study was to create the focus on the relation between cloud security and assurance	No	Partial	Cloud security, assurance, vulnerabilities, threats, attacks and risk evaluation	Yes	After evaluating total 306 works authors given the recommendations for the development of next-generation cloud security and cloud security assurance solutions
Ramachandra et al. [17]	2017	Survey	The main purpose of the study to understand the various cloud components, security issues, and risks, with emerging solutions for the vulnerabilities in the cloud	No	No	Vulnerabilities, Threats, and Attacks	Yes	Discussion of Vulnerabilities, Threats, Attacks, and Countermeasures & Controls

Table 3 (continued)

Study	Year	Type of Study	Purpose	Basic Cloud features	Virtualization and virtual machine	Issues covered	Security and privacy mechanisms or approaches (Identity, access, encryption n, trust, etc.)	Results
Rizvi et al. [16]	2017		Authors proposed the framework that evaluates the CSP security strengths	No	No	Security evaluation, evaluation rule, security index, interoperability, security auditing factors, etc	No	The security evaluation framework is presented which can quantify information in the form of security index
Subramanian et al. [18]	2018	Survey	The main purpose of the paper was to explore the main security challenges faced by CSP, CU and owner of data	Diagram only	Yes	Crypto-cloud security, SLA, various cyber attacks	Yes	The infrastructure level the virtualizations is the ail concern for security and attacks, the paper addresses the security challenges in virtualization and physical layer
Singh et al. [5]	2018	Survey	The main purpose of paper to present the security issues available in the delivery models	No	Yes	Major responsibilities of CSP and CU, types of vulnerabilities at delivery models, and the types of threats with suggested counter measures	Yes but in short	The qualitative analysis of all vulnerabilities and threats for each service mode id done and countermeasures have been proposed
Kumar et al. [8]	2019	Survey	The main purpose of the study is to present taxonomy of security, threats, different vulnerabilities and its countermeasures	Yes	Yes	Virtualization, Multi-tenant technology, web services	Yes	Identified a unique taxonomy for security, threats, possible vulnerabilities and countermeasures in cloud computing
Tabrizchi et al. [19]	2020	Survey	The main purpose of the survey to identify various security and privacy issues and present the recent security solutions	No	No	Security services, confidentiality, integrity, stakeholders, SLA, security policies etc.	Yes	Shown various security challenges, describes the security concerns of stakeholders, and recent possible solutions

- Interoperability—if the CU has any problem or dissatisfaction with vendor, then there should be a flexibility to migrate from one vendor to another. But generally, they face vendor lock-in problem
- Trust between CU and CSP—the CU should have trust on CSP that he is giving secure services with all security measures. However, it is really difficult to make this kind of trust between CU and CSP and for CSP to provide 100% secure services.

Apart from these challenges, some major challenges according to the delivery model level are listed in Table 1.

Cloud Provider

CSP is responsible to deliver cloud services to the CU. According to the delivery services, these CSP can be IaaS providers, PaaS providers, and SaaS providers [18]. According to the recommendation ITU-T X.160, the major threats and challenges for CSP are [20]:

- Eliminate internal threats—there can be a threat of hacking internal servers, leaking data either by intension, or un-intentional by internal employees.
- Secure administrator access rights—CSP is responsible to define access of administrator rights to the trusted employees only.
- Sharing environment security—many user access same services. There should be proper maintenance of confidentiality, integrity, and authentication (CIA) norms.
- Continuity in services—CSP needs to aware with the different type of attacks such as DoS, DDoS, which can disrupt services of the CSP to CU.
- Independence in software components—CSP has to make sure that if there is any security problem found in one software component, it should not affect to another.

Cloud Auditor

The main function of cloud auditor (CA) to evaluate services provided by the CSP on the basis of performance, privacy and control, etc. CA has three major roles—privacy audit, security audit, and performance audit. The main challenges faced by CA with respect to security are:

- Transparency—because the data and security both are managed by third party, the main challenge is to audit the proper documents prepared by the CSP in the form of SLA with clear CSP policies and security assurance [21].
- New technology certifications—CA is responsible to audit the CSP certifications whenever he applies for scaling and changing technology, so that it should not affect any kind of services and security provided to the CU.
- Encryption Technology—CA has to ensure that the proper encryption technology should be used by the CSP, so that the plain text should not flow around the channels [21].

Cloud Broker

Cloud brokers (CB) are the organizations that behave as an interface between CSP and CU. They generally offer some value-added services to CU such as an interface with various integrated services at one place. Services provided by the brokers are commonly—intermediation, aggregation, and arbitrage [22]. The main benefit of CB to the CU is sometime the CB provides some extra services to the CU on demand. The main security concerns for CB are the CSP needs to verify what kind of role and position he is giving to CB in the chain of data processing and accessing from cloud. CB serves various types of clients on the same platform; assurance is required from data leakage and privacy.

Cloud Carrier

The main role of cloud carrier (CC) is to provide the connectivity and channel between CSP and CU [23]. Generally, the carriers are Internet network, telecommunication, and different devices for providing the services of cloud. The SLA is required to be prepared between CSP and CC before providing services. The channels used by CC are commonly encrypted channels, because the security of the data while transporting is the major responsibility of CC [23]. Because while transporting sensitive data if the data get stolen or leaked, then there can be major loss to the CU which can result in the business and image loss to the CSP, as well.

Suggestions for Cloud Security

There are various public cloud service providers that provide real secure environment for protecting data on cloud such as Amazon, Google, etc. However, the real challenge starts when cloud user access that data and data leaves the cloud environment [1, 24]. The major challenges can be stolen login credentials, unprotected channel, etc. The cloud cyber security can be one of the solutions for secure data transfer from cloud to cloud user. There are various techniques used and suggested by researchers to provide the security of data, such as multi-factor authentication, multi-level authentication, creation of different back solutions, creation of logs, encryption for end to end data transfer, permissions log for access management, etc. [1, 4, 25].

Conclusion

The various types of challenges and security issues are explored in the paper. There are six major challenges which can be faced to the business organizations if they decide to use the cloud-based services. The paper has also explore the possible solutions against the challenges. There are five major stake holders in the cloud computing and the paper discusses the security concern and responsibility of each stake holder whether it is CSP, CU, CB, CA, or CC. A comparison of survey is done in the paper on the basis of issues discussed by the different researchers in Table 3. This paper can help the researchers to start and choose their area of research, and also provides the major security concerns at one place.

Compliance with Ethical Standards

Conflict of Interest We hereby declare that this manuscript is an original work and is not under consideration for publication in any other journal. All authors have approved the submission of the manuscript to the respective journals.

References

1. G. Rastogi, R. Sushil (2015) Cloud computing implementation: Key issues and solutions, in 2015 International Conference on Computing for Sustainable Global Development, INDIACom 2015.
2. Lee J. A view of cloud computing. Int J Networked Distrib Comput. 2013;1(1):2–8. https://doi.org/10.2991/ijndc.2013.1.1.2.
3. Khalil IM, Khreishah A, Azeem M. Cloud computing security: a survey. Computers. 2014;3(1):1–35. https://doi.org/10.3390/computers3010001.
4. Grobauer B, Walloschek T, Stöcker E. Understanding cloud computing vulnerabilities. IEEE Secur Priv. 2011;9(2):50–7. https://doi.org/10.1109/MSP.2010.115.
5. Singh A. Security concerns and vulnerabilities in cloud computing: a qualitative analysis. Int J Inf Technol. 2019;11(4):683–90. https://doi.org/10.1007/s41870-018-0108-1.
6. P. G. Neumann (2004) Security and privacy. In: Computer Science Handbook, Second Ed., CRC Press, pp. 77–1–77–5. https://doi.org/10.4324/9781315115757-7.
7. Ardagna CA, Asal R, Damiani E, Vu QH. From security to assurance in the cloud: a survey. ACM Comput Surv. 2015;48:1. https://doi.org/10.1145/2767005.
8. Kumar R, Goyal R. On cloud security requirements, threats, vulnerabilities and countermeasures: a survey. Comput Sci Rev. 2019;33:1–48. https://doi.org/10.1016/j.cosrev.2019.05.002.
9. Phaphoom N, Wang X, Samuel S, Helmer S, Abrahamsson P. A survey study on major technical barriers affecting the decision to adopt cloud services. J Syst Softw. 2015;103:167–81. https://doi.org/10.1016/j.jss.2015.02.002.
10. Hsu CL, Lin JCC. Factors affecting the adoption of cloud services in enterprises. Inf Syst E-bus Manag. 2016;14(4):791–822. https://doi.org/10.1007/s10257-015-0300-9.
11. Rastogi G, Sushil R. Secured identity management system for preserving data privacy and transmission in cloud computing. Int J Futur Gener Commun Netw. 2018;11(1):23–36. https://doi.org/10.14257/ijfgcn.2018.11.1.03.
12. Journal A, Basic OF. Cloud computing adoption by business organization: a systematic review. Aust J Basic Appl Sci. 2017;11(November):17–28. https://doi.org/10.22587/ajbas.2017.11.13.3.
13. G. Rastogi, R. Sushil, A Review Paper on Cloud Identity Management Systems, Int. Conf. Cloud Comput. Big Data, June 2016, Phuket, Thailand.
14. M. Almorsy, J. Grundy, I. Müller (2016) An analysis of the cloud computing security problem. Available: https://arxiv.org/abs/1609.01107. Accessed July 2020
15. Takabi H, Joshi JBD, Ahn GJ. Security and privacy challenges in cloud computing environments. IEEE Secur Priv. 2010. https://doi.org/10.1109/MSP.2010.186.
16. Rizvi S, Ryoo J, Kissell J, Aiken W, Liu Y. A security evaluation framework for cloud security auditing. J Supercomput. 2018;74(11):5774–966. https://doi.org/10.1007/s11227-017-2055-1.
17. Ramachandra G, Iftikhar M, Khan FA. A 2Survey on security in cloud computing. Procedia Comput Sci. 2017;110(2012):465–72. https://doi.org/10.1016/j.procs.2017.06.124.
18. Subramanian N, Jeyaraj A. Recent security challenges in cloud computing. Comput Electr Eng. 2018;71:28–422. https://doi.org/10.1016/j.compeleceng.2018.06.006.
19. Tabrizchi H, Kuchaki Rafsanjani M. A survey on security challenges in cloud computing: issues, threats, and solutions no. 0123456789. New York: Springer US; 2020.
20. M. Drozdova, S. Rusnak, P. Segec, J. Uramova, M. Moravcik (2017) Contribution to cloud computing security architecture. ICETA 2017—15th IEEE Int. Conf. Emerg. eLearning Technol. Appl. Proc., no. February 2018. doi: https://doi.org/10.1109/ICETA.2017.8102480.
21. Ryoo J, Rizvi S, Aiken W, Kissell J. Cloud security auditing: challenges and emerging approaches. IEEE Secur Priv. 2014;12(6):68–74. https://doi.org/10.1109/MSP.2013.132.
22. Guzek M, Gniewek A, Bouvry P, Musial J, Blazewicz J. Cloud brokering: current practices and upcoming challenges. IEEE Cloud Comput. 2015;2(2):40–7. https://doi.org/10.1109/MCC.2015.32.
23. S. R. Lenkala, S. Shetty, K. Xiong (2013) Security risk assessment of cloud carrier. Proc.—13th IEEE/ACM Int. Symp. Clust. Cloud, Grid Comput. CCGrid 2013, pp. 442–449. doi: https://doi.org/10.1109/CCGrid.2013.28.
24. Rastogi G, Verma H, Sushil R. Determining factors influencing cloud services adotion in India. Serbian J Manag. 2018;13(2):335–52.
25. Verma G, Chakroborty R. A hybrid privacy preserving scheme using finger print detection in cloud environment. Ingenierie des systemes d'information. 2019;24(3):343–51.