Review

Improve the Security of Cloud Computing to Enhance Network Security

Shirmohammad Tavangari * , Somayeh Taghavi Kulfati , Aref Yelghi

Posted Date: 18 July 2023

doi: 10.20944/preprints202307.1222.v1

Keywords: cloud computing; security challenges; security techniques

Review

Improve the Security of Cloud Computing to Enhance Network Security

Shirmohammad Tavangari [1,*], Somayeh Taghavi Kulfati [2] and Aref Yelghi [3]

[1] University of British Columbia, ElectricalandComputerEngineering Faculty, 2332 Main Mall, Vancouver, BC Canada V6T 1Z4
[2] Mehrastan Education Institute, Faculty of Technical Engineering, Computer Science Department, P9CQ,Mehrastan, Iran, fanavari_17shahrivar@gums.ac.ir
[3] Istanbul Topkapi University, Faculty of Engineering, Computer Engineering, Istanbul, Zeytinburnu, Zeytinburnu, 32721, Istanbul, Turkey, arefyelghi@topkapi.edu.tr
* Correspondence: s.tavangari@alumni.ubc.ca

Abstract: In recent years, significant progress has been observed in cloud computing. As the number of companies using the cloud increases, so does the need to protect user data. Today, the major challenges facing cloud computing include the security, protection, and processing of data belonging to users. This study aims to investigate security issues and identify appropriate security techniques in the world of cloud computing.Also, the identification of security challenges that may arise in the field of cloud computing in the future has been evaluated. In this research, we used two different research methods: systematic literature review (SLR), and survey and interview with different security experts who work in the field of cloud computing.All the security challenges, most compromised attributes and identified mitigation techniques from both SLR and survey were presented and discussed.

Keywords: cloud computing; security challenges; security techniques

Introduction:

Cloud computing (CC) includes servers and computers that provide services to users using the Internet.[1,2]In this model, users can connect to cloud servers and use processing capacity, memory, storage and other required resources to do their work. In fact, CC is considered as a new approach to manage and use of computing resources and information technology using Internet. In CC, instead of buying and maintaining the required hardware and software, there is access to these resources, and capability to run applications and provide services through the Internet.[3]CC is growing rapidly in the IT space and cloud infrastructures are visible every where.The major current Cloud providers include Amazon, Microsoft, Google, IBM, Oracle, Eucalyptus, VMware, Eucalyptus, Citrix, Salesforce, Rackspace, and many vendors offer different Cloud services.[4]

The most advantages of CC are the very wide services, increasing the availability and reducing costs, as well as increasing the flexibility and scalability of systems.[5,6] While virtualization and CC offer a wide range of dynamic resources, but due to providing services and transferring information through the Internet, security issues are considered as one of the challenges, which causes users to resist accepting computing technology.[7-10]Since in these systems, users' information is kept and stored in a space far from the user's control, the issue of user security and privacy is also raised.[11]Cloud service providers are required to take special privacy measures in order to gain the satisfaction and trust of their customers. Because without adopting strategic policies to protect privacy and security of people in using cloud services, service delivery may face challenges. According to the results of studies conducted in 2021 by Alouffi, security has been introduced as the most challenging issue of CC.[12]Also, we can point out performance and availability as the other important challenges. Security in CC can improve communication between users and service

 doi:10.20944/preprints202307.1222.v1

providers. On the other hand, different security techniques improve system and software performance and resistance to attacks.

This study aims to investigate the current status of security in CC, identifying security weaknesses in cloud service providers as well as its users, evaluating legal issues related to CC security, and providing applicable solutions to improve CC security. Considering the growing use of CC in various organizations and industries, this research present the security and stability of CC systems and increasing the trust of users and service providers by identifying security challenges and introducing techniques to reduce them.

Methods and Materials:

We performed the electronic search in the international databases: ISI web of knowledge, Google-Scholar search engine, IEEE, Science direct,Springer and Scopus. The following key words were searched ({Cloud Computing} OR {Cloud security techniques} OR {security challenges} AND {systematic review} OR {systematic literature review} OR {research review}). Moreover, the reference list of the potentially appropriate studies were screened to identify additional relevant studies.

In addition to the systematic review, a questionnaire was designed according to the specifications and requirements of the research and then sent electronically to professors and experts related to the field of CC. In this questionnaire, experts were asked to present the future challenges in CC and methods of identifying threats and techniques used to reduce them based on their attitudes. The questionnaire is mentioned in the attachment.

Results:

A. Identified challenges and mitigation techniques from SRL

The literature review analysis reveals 43 security challenges. These challenges threaten the characteristics of CC including confidentiality, integrity, availability, security, responsiveness, usability, reliability, and auditability. A detailed description of these challenges and compromised features is provided in Appendix A.Figure 1 shows the threat records of these challenges. Confidentiality 31% and integrity 24% are the most threatened. While the contribution of usability, reliability, responsiveness, and audit ability is less than 10%.We recognized 34 security techniques from SLR.A detailed description of these techniques is provided in Appendix B. These mitigation techniques have a great impact on the performance, security, efficiency, QoS, privacy, and access control of CC Figure 2.

B) Future challenges and mitigation techniques from Survey

CC is a new paradigm that has become popular in the last decade and it is difficult to find security experts in this field. In the survey section, based on expert opinions we have identified a total of 18 security challenges that may be faced in the future of CC. These challenges include Hypervisor viruses, Legal interception points, Virtual machine security, Reliable transaction, Risk of multiple tenants, Cloud Smartphone data, Abuse and misuse of CC insecure programming interfaces, Malicious insiders, Common technology vulnerability, Vulnerability and Vulnerability of Common Traffic Hijacking Technology, Privacy, espionage, Business Intelligence, Trade secrets, Data ownership, Availability, transparency. Compromised features resulting from these challenges include confidentiality, security, availability, and integrity.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1222.v1

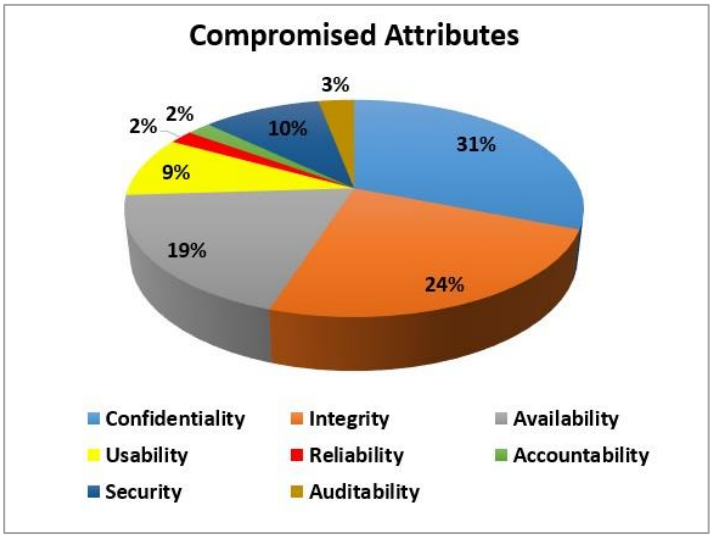

Figure 1. List of features at risk and their contribution.

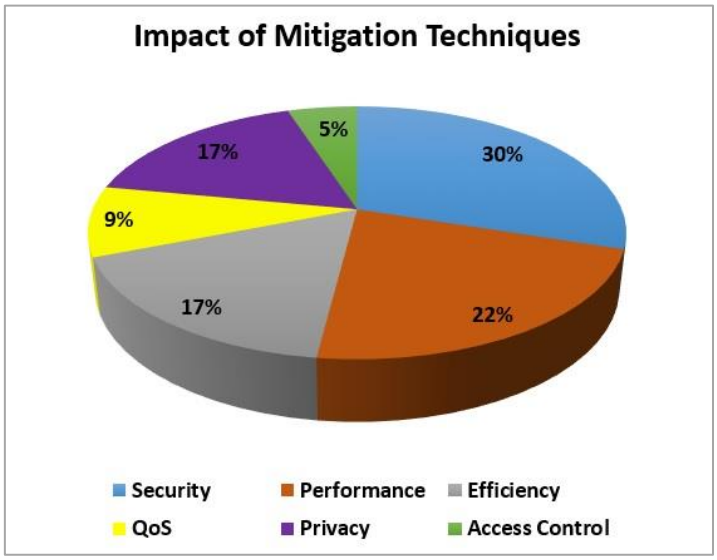

Figure 2. The impact of mitigation techniques on the features of cloud computing.

We identified a total of 9 security techniques from the analysis of the results of the questionnaires. The main security techniques are: Use of optical fiber, Encryption, VPN (virtual private network), IPSec(Internet Protocol Security), Intrusion detection system, Third party auditor, Kerberos, SSH and 5MD message digest for authentication, API monitoring agent, Service Management (SMAPI).

Discussion:

In this study, security challenges and appropriate security techniques in CC were evaluated through a SLR. Also, the identification of future security challenges in the CC was evaluated through the survey of experts in this field.

Based on various studies, 43 challenges in CC have been identified (Appendix A), the most important of which are security challenges. Different challenges affect different features of CC. Confidentiality with 31% has the largest contribution of the threatened features caused by these challenges in the cloud system. Confidentiality ensures that data is not disclosed to unauthorized persons. Loss of physical privacy occurs through social engineering, and loss of electronic privacy occurs when clients and servers do not encrypt their communications.

 doi:10.20944/preprints202307.1222.v1

CC experts suggest main ways to reduce future security challenges.SSL (Secure Socket Layer) or TLS (Transport Layer Security) encryption is used to encrypt the communication between the browser and the web server and is considered as one of the main ways to increase security in websites. Using SSL, information is transferred between the user's browser and the web server in encrypted form, which protects the user's information from unauthorized access. Considering the information stored in the cloud is sensitive for many users and organizations, it is highly recommended to use proper encryption in the communication between the browser and the web server in this space. In fact, many cloud services also use information encryption in communication with users by default. Additionally, proper use of encryption can provide good protection against "MiddleMan" attacks. In order to protect against these attacks, it is necessary to observe in case there are delayed response times to determine whether a "MiddleMan" exists.

The use of optical fiber is also considered as a security tool because this technology creates a protective layer between the two parties in communication. As well as, due to the difficulty in manipulating and changing information in this technique, the possibility of spying attacks and unauthorized access to user data decreases. However, it should be noted that optical fiber is only one method of communication in the cloud, and the use of encryption is still essential consideration to increase the security of communication.

In this study, using the experiences of CC experts, the following are suggested to increase the security of cloud systems in the future: increased efforts in risk management, standard security solutions, defining security strategy, separating security architecture from technical infrastructure, third-party compliance, and lightweight but effective encryption techniques.

Conclusion:

In conclusion, improving security in CC is very important and many companies and organizations are currently developing and improving security solutions for their cloud services. In this context, information security engineers can improve security by investigating security threats, designing and implementing appropriate security systems, and providing the necessary guidelines to increase security in CC. Also, efforts to implement security and privacy regulations in the cloud space can be useful to increase users' trust in CC services.

Appendix A: List of identified challenges in CC and compromised attribute extracted from SLR

No.	Challenges	Compromised attribute	No.	Challenges	Compromised attribute
1	WS- Security	Integrity, Confidentiality	23	Perceived Lack of Reliability	Availability
2	Phishing attack	Confidentiality	24	Auditing	Security, Confidentiality
3	Wrapping attack	Integrity	25	Back-Door	Usability
4	Injection attack	Availability	26	TCP Hijacking	Confidentiality, Integrity
5	IP Spoofing	Confidentiality	27	Social Engineering	Confidentiality
6	Tampering	Integrity	28	Dumpster Diving	Availability
7	Repudiation	Auditability	29	Password Guessing	Confidentiality
8	Information Disclosure	Confidentiality	30	Trojan Horses and Malware	Usability
9	Denial of service	Availability	31	Completeness	Availability
10	Elevation of privilege	Confidentiality	32	Roll back attack	Availability, Usability
11	Physical security	Security, Availability	33	Fairness	Confidentiality

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1222.v1

12	WLAN's security	Usability, Accountability	34	Data Loss or Leakage	Availability
13	Direct attacking method	Confidentiality	35	Computer network attack	Confidentiality, Integrity
14	Replay attack	Integrity	36	Denial of service attack	Availability
15	Man-in-the-middle attack	Availability, Integrity	37	Data security	Integrity, Security
16	Reflection attack	Confidentiality	38	Network security	Integrity, Security
17	Interleaving attack	Integrity, Confidentiality	39	Data locality	Reliability
18	Timelines attack	Usability, Availability	40	Data integrity	Integrity
19	Self-adaptive storage resource management	Integrity, Confidentiality	41	Data segregation	Security, Confidentiality
20	Client monitoring and security	Security	42	Backup	Availability
21	Lack of trust	Confidentiality	43	Data manipulation	Availability, Integrity
22	Weak Service Level Agreements (SLAs)	Availability, Confidentiality			

Appendix B: List of security techniques and their impact extracted from SLR

No.	Security technique	Impact
1	Identity-Based Authentication(IBA)	Privacy, Security
2	RSA algorithm	Security, Efficiency
3	Dynamic intrusion detection system	Performance
4	Multi-tenancy based access control model (MTACM)	Security, access control
5	TLS Handshake	Security
6	Public key based Homomorphic authenticator with random masking	Privacy, Performance
7	Third party auditor(TPA)	Efficiency, QoS
8	Probabilistic sampling technique	Security, Privacy
9	Diffie-Hellman key exchange	Security, Access control
10	Private face recognition	Privacy, Performance
11	Message Authentication Codes (MAC's)	Efficiency
12	Data coloring and software water marking techniques	Performance, Security
13	A Novel Cloud dependability model	QoS, Security
14	Key Policy Attribute-Based Encryption(KP-ABE)	Privacy, Efficiency
15	Proxy Re-Encryption (PRE)	Performance, Security
16	RBAC (Role-Based Access Control) technique	Privacy, Efficiency
17	Application-oriented Remote Verification Trust Model (ARVTM)	QoS, Security
18	Security assertion Markup Language (SAML)	Performance, Privacy
19	Trusted Platform Module (TPM)	QoS, Security
20	Proof Of Retrievability (POR)	Efficiency, Performance
21	Fair MPNR protocol	Security, Performance
22	Sobol Sequence	Security, Performance, Efficiency
23	Redundant Array of Independent Net-storages (RAIN)	Privacy, Efficiency
24	Hadoop Distributed File System	performance

25	Self-Cleansing Intrusion Tolerance (C-SCIT)	Security, Privacy
26	Searchable symmetric encryption (SSE)	Security, Privacy, Performance
27	Provable data possession(PDP)	Security, performance, Efficiency
28	Time bound ticket based mutual authentication scheme	Efficiency, Security, Performance
29	Security Access Control Service (SACS)	Access control Security
30	The Service Level Agreement	QoS, Performance
31	Intrusion detection	Efficiency, Security
32	Hypervisor	Access Control
33	Identity Management	Privacy and Security

References

1. Alam T. Cloud Computing and its role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI). 2020 Feb 3;1(2):108-15.
2. Shukur H, Zeebaree S, Zebari R, Zeebaree D, Ahmed O, Salih A. Cloud computing virtualization of resources allocation for distributed systems. Journal of Applied Science and Technology Trends. 2020 Jun 27;1(3):98-105.
3. Voorsluys W, Broberg J, Buyya R. Introduction to cloud computing. Cloud computing: Principles and paradigms. 2011 Feb 28:1-41.
4. Prodan R, Ostermann S. A survey and taxonomy of infrastructure as a service and web hosting cloud providers. In2009 10th IEEE/ACM International Conference on Grid Computing 2009 Oct 13 (pp. 17-25). IEEE.
5. Apostu A, Puican F, Ularu G, Suciu G, Todoran G. Study on advantages and disadvantages of Cloud Computing–the advantages of Telemetry Applications in the Cloud. Recent advances in applied computer science and digital services. 2013;2103.
6. Gajbhiye A, Shrivastva KM. Cloud computing: Need, enabling technology, architecture, advantages and challenges. In2014 5th International Conference-Confluence The Next Generation Information Technology Summit (Confluence) 2014 Sep 25 (pp. 1-7). IEEE.
7. Basu S, Bardhan A, Gupta K, Saha P, Pal M, Bose M, Basu K, Chaudhury S, Sarkar P. Cloud computing security challenges & solutions-A survey. In2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) 2018 Jan 8 (pp. 347-356). IEEE.
8. Jangjou M, Sohrabi MK. A comprehensive survey on security challenges in different network layers in cloud computing. Archives of Computational Methods in Engineering. 2022 Oct;29(6):3587-608.
9. Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation computer systems. 2012 Mar 1;28(3):583-92.
10. Butt UA, Amin R, Mehmood M, Aldabbas H, Alharbi MT, Albaqami N. Cloud security threats and solutions: A survey. Wireless Personal Communications. 2023 Jan;128(1):387-413.
11. S.Tavangari. A Novel Approach to Accessing the Scheduled Network. TechRxiv, https://doi.org/10.36227/techrxiv.21579456.v1, Nov 2022
12. Sahmim S, Gharsellaoui H. Privacy and security in internet-based computing: cloud computing, internet of things, cloud of things: a review. Procedia computer science. 2017 Jan 1;112:1516-22.
13. Alouffi B, Hasnain M, Alharbi A, Alosaimi W, Alyami H, Ayaz M. A systematic literature review on cloud computing security: threats and mitigation strategies. IEEE Access. 2021 Apr 14;9:57792-807.
14. S.Tavangari. A New Method in the Cryptography. International Journal of Advanced and Management Research, Vol.2, Issue 4, PP.894-900, Aug 2017