Vulnerabilities and Potential Threats of Cloud computing

Subjects: Computer Science, Artificial Intelligence | Agricultural Engineering

Contributor: Abdul Razaque

Cloud computing has become a prominent technology due to its important utility service; this service concentrates on outsourcing data to organizations and individual consumers. Cloud computing has considerably changed the manner in which individuals or organizations store, retrieve, and organize their personal information. Despite the manifest development in cloud computing, there are still some concerns regarding the level of security and issues related to adopting cloud computing that prevent users from fully trusting this useful technology.

Keywords: cloud computing ; security

1. Introduction

Cloud computing is considered as a utility-driven paradigm derived from a “pay as you use” concept responsible for enabling consumers to remotely share technology-based resources instead of possessing these resources locally [1][2].

Cloud computing transports a reliable, custom-made information technology (IT) perimeter for cloud users with an ensured quality of service. In cloud computing, services are afforded from the cloud clients’ points of view and are presented as IT-related skills, reachable with no in-depth familiarity of the used technologies and with a titular coordinating effort [3][4].

The cloud as a concept can be defined as the “storing of data anywhere and accessing it anytime”. Cloud clients who have appropriate permissions can access the stored data. For more information about the cloud characteristics, readers can refer to [5]. Four diverse types of delivery models are supported in cloud computing: private cloud, public cloud, hybrid cloud, and community cloud [6][7].

- The private cloud is usually utilized by a limited number of users capable of accessing highly confidential data.
- The public cloud is commonly employed for hosting sensitive data, in which data integrity is repeatedly mutable.
- The hybrid cloud combines two or more delivery models. This model can be applicable to cloud users who would like to retain their most crucial data on-premises while storing their fundamental data on the cloud. The combined delivery models can be private-, public-, or community-based models; however, a standardized technology can be utilized to bound the data. The hybrid cloud improves security and lowers the price. However, the high management complexity is the major drawback.
- The community cloud can be considered as a type of public cloud in which various cloud clients share a specific infrastructure with a community that engages with one another on an identical interest.

Cloud computing merges various technologies and procedures to preserve cloud client’s data. Thus, there are competitions between cloud service providers to provide the latest security mechanisms. Notwithstanding, several security-wise ambiguities still exist which make many organizations reluctant to fully utilize cloud computing [8].

In cloud computing, data security, privacy, and safety are fundamental measures which establish the trust level between the cloud clients and cloud providers. Cloud computing is broadly employed in diverse fields such as economy, social, finance, educational institutions, and government offices. Therefore, users store confidential information on the cloud and retrieve it at their convenience. Prior to developing and designing cloud computing, privacy and security requirements have to be exhaustively explored. Individuals and organizations are still distrustful due to the existing security vulnerabilities that threaten cloud computing. In fact, cloud computing lacks explicit security and privacy protection regulations.

2. Vulnerabilities, and Potential Threats

2.1. TPA-Based Cloud Vulnerabilities

Encrypting data on the cloud is necessary while avoiding considerable processing overhead. Many organizations are leaning towards cloud-based IT solutions because of the multiple benefits that cloud computing affords. Nevertheless, before making use of cloud computing, cloud clients should be aware of potential vulnerabilities (**Figure 1**) that might mutate cloud clients' hopes of increasing scalability and decreasing coordination cost into a misery of misuse and data breaches [9]. Therefore, the security issues associated with cloud adoption should be considered. The most common vulnerabilities effecting TPAs are given as follows:

- Loss of control;
- Lack of trust (mechanisms).

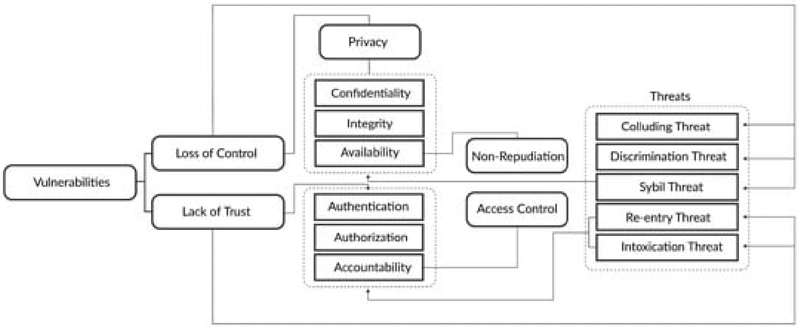

Figure 1. Security requirements, vulnerabilities, and threats.

2.1.1. Loss of Control

When clients/users lose their authority over their resources stored on the servers of the cloud service provider (CSP), a loss of control occurs [10]. A deficiency in authentication and authorization placed by the service providers contributes to bigger security risks and concerns. Most of the cloud services providers do not provide data encryption for the data at rest. As a result, the data cannot be safeguarded if a data breach occurs at the cloud service provider side [11].

Let us consider the server S_c in the CSP and clients $C = \{C_1, C_2, \ldots, C_k\}$ that use the services $S = \{S_1, S_2, \ldots, S_k\}$. We take the security requirements $R_{se} = \{R_{se1}, R_{se2}, \ldots, R_{se-n}\}$ to impose on the server. Thus, the risk $R_{p,q}$ can be referred to as $R_{p,q}$ for $1 \leq p \leq k$ and $1 \leq q \leq n$ that has a security requirements S_p for the clients. We let PS_q , for $1 \leq q \leq n$ be the probability that the server loses the control to meet the security requirements. The loss of control $\forall\gamma$ be determined as:

$$\forall\gamma = \sum_{1 \leq q \leq n} R_{p,q} \times PS_q$$

2.1.2. Lack of Trust (Mechanisms)

Trust is one of the important aspects for maintaining quality. Trust is faith or confidence in the cloud services delivered by the CSP [12]. Trust permits the clients to use the service in the cloud without any panic.

To reinforce the confidence of the clients, it is necessary to build trust among clients, TPA, and CSP. The problem is a lack of trust for data storage on the servers of the clouds for clients. Furthermore, most organizations store their private and sensitive information on cloud servers. If a CSP reliably provides the services, then there is the possibility that a TPA might play a role as a malicious adversary when auditing the services. There is the possibility that the TPA might share the private and sensitive data to other unknown parties to harm the legitimate owners of the data. Thus, there is a need to build a trust model to deal with the lack of trust of the clients. The trust model based on time factor is considered as feedback. If the feedback is older, it is considered to be of a lower weight, whereas newer feedback is counted as having a higher weight. Thus, the feedback of the client can be determined as:

$$C_{fe} = \frac{1}{1 + \omega(t - T_{\delta})} 0 < \sigma$$

TPA takes the responsibility to evaluate and authenticate the client while maintaining privacy preservation depicted in **Figure 2**. This is carried out because the actions taken by the TPA could be malicious for the client and CSP.

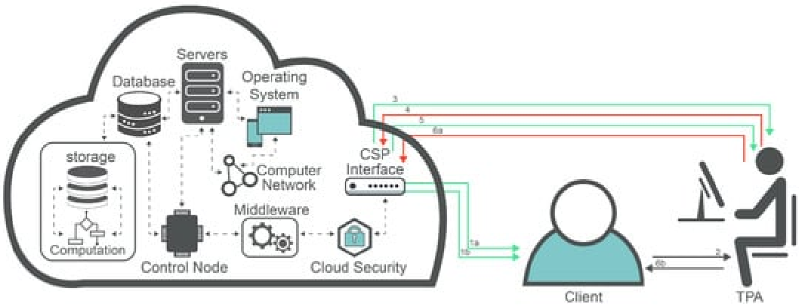

Figure 2. Evaluation and authentication of the client through CPS.

Cloud clients should be aware of the following seven issues.

- Privileged user access;
- Regulatory compliance;
- Data location;
- Data segregation;
- Recovery;
- Investigative support;
- Long-term viability.

2.2. TPA-Based Cloud Threats

Several security requirements are violated because of the diverse attacks that target cloud computing as depicted in **Figure 3**.

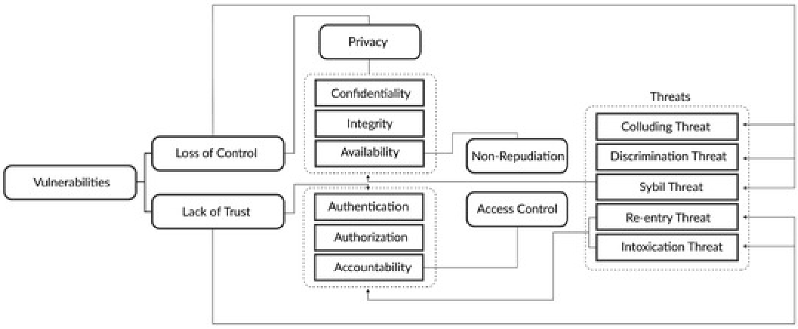

Figure 3. Security requirements, vulnerabilities, and threats.

2.2.1. Collusion Threats

This type of threat consist of a form of attack known as collusive malicious feedback that is created by malicious cloud clients who misuse feedbacks to tamper with trust model outcomes. Collusion attacks exist in three forms:

- Self-promoting: malicious cloud clients falsely promote a specific cloud service provider by recording remarkable positive feedback;
- Slandering: malicious cloud clients defame a specific cloud service provider by sending remarkable negative feedback;
- Occasional collusion feedback attack: this kind of attack occurs when a remarkable negative or positive feedback is occasionally entered by malicious cloud clients.

2.2.2. Sybil Threats

This type of attack is launched by malicious cloud clients utilizing several identities to tamper with test outcomes. Various counterfeit ratings are generated by malicious cloud clients utilizing low product value in which products are purchased in short time. This type of attack can be categorized as:

- Self-promoting: this is also known as a ballot-stuffing attack. In this attack, significant positive feedback is added by malicious cloud clients to promote a specific cloud service provider;

- Slandering: another name of this attack is bad-mouthing. This attack is launched by malicious cloud clients to defame a specific cloud service provider using significant negative ratings.

- Occasional Sybil feedback attack: in this attack, significant amounts of negative or positive feedback are entered occasionally by malicious cloud client to either promote or defame a specific cloud service provider.

2.2.3. ON OFF Threat or Intoxication Threat

Malicious cloud clients adjust their behaviors either to act as harmful or harmless users. More specifically, the cloud client initially performs ordinarily until gaining trust, then the client begins to misbehave. Regrettably, this type of misbehavior is hard to detect. This deficiency is derived from peer-to-peer network and is known as the dynamic personality of peers. This attack can be resolved using a forgetting factor approach.

2.2.4. Discrimination Threat

Discrimination attacks occur when distinct qualities of services are afforded from cloud service providers to cloud clients. This attack jeopardizes cloud service providers’ trust because various ratings are provided by clients as a result of this attack. Mitigating or preventing this attack is a difficult task to accomplish.

2.2.5. Newcomer or Reentry Threat

This attack is carried out by a previous client who has been terminated due to unethical behavior and who reenters the domain with a new identification. Reentry or newcomer attack can be mitigated/prevented by contrasting credential records utilizing the client location and then using the location as a unique ID.

References

1. Razaque, A.; Jararweh, Y.; Alotaibi, B.; Alotaibi, M.; Hariri, S.; Almiani, M. Energy-efficient and secure mobile fog-based cloud for the Internet of Things. Future Gener. Comput. Syst. 2021, 127, 1–13.
2. Huang, H.; Sun, X.; Xiao, F.; Zhu, P.; Wang, W. Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments. J. Parallel Distrib. Comput. 2021, 148, 46–57.
3. Ibrahim, F.A.; Hemayed, E.E. Trusted cloud computing architectures for infrastructure as a service: Survey and systematic literature review. Comput. Secur. 2019, 82, 196–226.
4. Razaque, A.; Vennapusa, N.R.; Soni, N.; Janapati, G.S. Task scheduling in cloud computing. In Proceedings of the Systems, Applications and Technology Conference (LISAT) 2016 IEEE Long Island, Farmingdale, NY, USA, 29 April 2016; pp. 1–5.
5. Arwa, M.; Hamdan, M.; Khan, S.; Abdelaziz, A.; Babiker, S.F.; Imran, M.; Marsono, M.N. Software-defined networks for resource allocation in cloud computing: A survey. Comput. Netw. 2021, 195, 108151.
6. Yeh, T.; Chen, Y. Improving the hybrid cloud performance through disk activity-aware data access. Simul. Model. Pract. Theory 2021, 109, 102296.
7. Razaque, A.; Li, Y.; Liu, Q.; Khan, M.J.; Doulat, A.; Almiani, M.; Alflahat, A. Enhanced Risk Minimization Framework for Cloud Computing Environment. In Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, 28 October–1 November 2018; pp. 1–7.
8. Kalluri, R.K.; Guru, C.V. An effective analytics of third party auditing and Trust architectures for integrity in cloud environment. Mater. Today Proc. 2021, 79, 69–76.
9. Perez-Botero, D.; Szefer, J.; Lee, R.B. Characterizing hypervisor vulnerabilities in cloud computing servers. In Proceedings of the ACM 2013 International Workshop on Security in Cloud Computing, Dresden, Germany, 9–12 December 2013; pp. 3–10.
10. Razaque, A.; Amsaad, F.; Hariri, S.; Almasri, M.; Rizvi, S.S.; Frej, M.B.H. Enhanced grey risk assessment model for support of cloud service provider. IEEE Access 2020, 8, 80812–80826.
11. Razaque, A.; Nadimpalli, S.S.V.; Vommina, S.; Atukuri, D.K.; Reddy, D.N.; Anne, P.; Vegi, D.; Malllapu, V.S. Secure data sharing in multi-clouds. In Proceedings of the IEEE 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 3–5 March 2016; pp. 1909–1913.

12. Dunne, N.J.; Brennan, N.M.; Kirwan, C.E. Impression management and Big Four auditors: Scrutiny at a public inquiry. Account. Organ. Soc. 2021, 88, 101170.