Secure Cloud Infrastructure Review

Subjects: Computer Science, Cybernetics

Contributor: Murad Rassam

Cloud computing is currently becoming a well-known buzzword in which business titans, such as Microsoft, Amazon, and Google, among others, are at the forefront in developing and providing sophisticated cloud computing systems to their users in a cost-effective manner. Security is the biggest concern for cloud computing and is a major obstacle to users adopting cloud computing systems. Maintaining the security of cloud computing is important, especially for the infrastructure.

Keywords: cloud computing ; secure cloud infrastructure ; application security ; network security ; host security ; data security

1. Introduction

The idea behind cloud computing is to provide all possible facilities such as software, IT infrastructure, and services to its customers for use over the internet. Cloud computing systems are large-scale, heterogeneous collections of autonomous systems and flexible computational architecture. This technology is emerging, as it is considered the first choice for businesses that do not want to deal with the in-house maintenance of systems and a development team [1]. Many businesses, such as Amazon AWS, Google, IBM, Sun, Microsoft, and many others, are developing efficient cloud products and technology [2]. In cloud technology, data are shared via virtual data centers from the customers and the organization [2].

Cloud computing has evolved as a popular and universal paradigm for service-oriented computing where computing infrastructure and solutions are delivered as a service. The cloud has revolutionized the abstraction and use of computing infrastructure through its features (e.g., self-service on-demand, broad network access, resource pooling, etc.), making cloud computing desirable [3]. However, security is the biggest challenge, and concerns regarding cloud computing continue to arise as we witness an increasing number of new developments in cloud computing platforms [4]. In the post-COVID-19 world, it is clear that more people and businesses are adopting cloud services, software, and infrastructure, as they can be accessed anytime, and from anywhere. To handle security risks, several research works and developments, such as in [5][6][7][8], have been proposed. Nonetheless, there are still more opportunities for new techniques to make the cloud more secure. Most of the existing techniques for securing the cloud do not focus on the new types of security risks that might face the cloud computing infrastructure. Hence, they cannot detect attacks or vulnerabilities that might come from the cloud service provider's side or the consumer's side. Furthermore, very few existing works have examined the different levels of cloud infrastructure altogether. Due to the high importance of investigating such issues, this paper conducted an extensive survey on the issues that the cloud computing infrastructure faces at different levels (application, host, network, and data level). It also presents the existing solutions used to mitigate these issues. Additionally, this paper highlights some open challenges that still need to be solved and suggest directions for future work. To the best of our knowledge, this study is the first effort to provide a systematic review of associated security issues and solutions based on cloud levels (application, host, network, and data level). The following are the main contributions of this study: Conducting a systematic evaluation of 103 articles on cloud infrastructure in connection with attacks and defenses. Providing a new taxonomy for a systematic review of cloud infrastructure levels. Investigating four levels that aim to cover all vulnerabilities that might come from the cloud service provider's side or the consumer's side. Identifying the limitations of the examined studies and highlighting the open research challenges and proposed directions for future work.

2. Cloud Computing Background and Terminologies

The idea behind cloud computing is not new. In the 1960s, John McCarthy envisioned that computing services will be offered to the general public as a utility [3]. The term "cloud" has also been used in various aspects, such as the concept of widespread ATM networks in the 1990s and the e-commerce outlets currently used by hundreds of millions of people around the world. However, the term only started to gain momentum after Google's CEO Eric Schmidt defined a "cloud" as the business model of offering services across the Internet in 2006 [9]. In 2011, the National Institute of Standards and Technology (NIST) defined cloud computing as a paradigm for allowing convenient, ubiquitous, and on-demand network access to a shared pool of configurable computing resources such as servers, storage, services, applications, and networks that can be quickly provisioned and released with minimal interaction or management effort from service providers. This cloud paradigm consists of five essential attributes, three service delivery models, and four deployment models [3], as shown in **Figure 1** (which is adapted from the study in [10]).

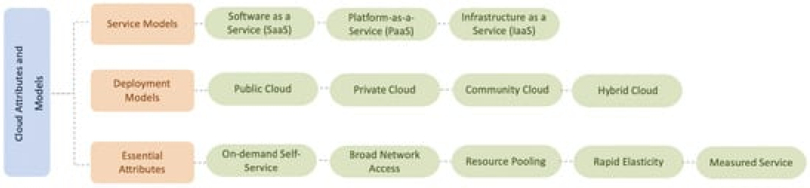

Figure 1. Cloud attributes and models.

Many actors play a major role in cloud computing, as shown in **Table 1** .

Table 1. Cloud Stakeholders.

Stakeholders in Cloud	Definition
Service Providers	**The cloud computing systems are owned and operated by service providers and deliver service to third parties. The providers will be responsible for maintaining and upgrading systems, such as Google, Microsoft, IBM, Oracle, Amazon, and Sun [11].**
Consumers	**The effective subscribers purchase the services and use the system based on their operational expenses from service providers [11].**
Enablers	**Organizations that facilitate adoption, utilization and delivery to selling services in cloud computing [11].**
Regulators	**International entities that penetrate the other stakeholders [11].**

The study in [12] conducted a systematic literature review of the integration as a service between trusted computing and cloud computing for infrastructure as a service (IaaS). Cloud computing integration and trusted computing can create a new infrastructure architecture as a service that encourages more cloud service tenants to trust cloud service providers.

In [13], the authors investigated the key contemporary security problem in cloud computing and provided the best practices for service providers and organizations hoping to manage cloud services. **Table 2** presents a summary of the existing related surveys in terms of their contributions and the levels of infrastructure they covered. It summarizes existing survey papers in cloud infrastructure over the period from 2016 to 2020. As noticed, most of these surveys were conducted at only one level of cloud infrastructure. For instance, the surveys in [14][15][16][17], focused on only the data level, while the survey in [18] focused on only the application level. Moreover, a survey [19] was conducted on the network level and another paper [13] on the host level.

Table 2. Summary of existing surveys.

Reference	Contribution	Data	Application	Host	Network
[20]	**The study reviewed the security issues regarding user data sensitivity on cloud architecture.**	√			
[14]	**The study focused on identified cloud computing security issues during data migration to the cloud and presented solutions for resolving potential threats.**	√			
[15]	**The survey performed a taxonomy to compare key services that are regularly used by cloud applications.**	√	√	√	√
[21]	**This study focused on the crypto cloud with various Communication, Storage, and Service Level Agreements.**		√		√
[22]	**The survey focused on data privacy.**	√			
[16]	**The study highlighted the security requirements for cloud computing.**		√		
[18]	**The study was classifying types of threats based on service resources in the context of the cloud.**	√	√		

Reference	Contribution	Data	Application	Host	Network
[23]	**The study reviewed DDoS techniques used in cloud computing.**				√
[19]	**The study evaluated major attacks targeting the security of Cloud Computing.**	√	√	√	√
[24]	**The study reviewed technologies that allow for privacy-aware outsourcing of storage and processing of sensitive data to public clouds.**	√			
[25]	**The study provided security issues and requirements for the cloud, identified threats, and known vulnerabilities.**	√	√		√
[13]	**The study is more about the security from providers perspectives.**	√	√	√	√
This survey	**Provides an extensive survey on issues that cloud computing infrastructure faced at its levels (Application, Host, and Network and data level).** **Presents some existing solutions used to mitigate these issues.** **Highlights some open challenges that still need to be solved.**	√	√	√	√

3. Security Issues in Cloud Computing Infrastructure

Four main levels should be considered when planning for and applying security in cloud infrastructure, which are data level, application level, network level, and the host level [26]. These levels are shown in **Figure 2** .

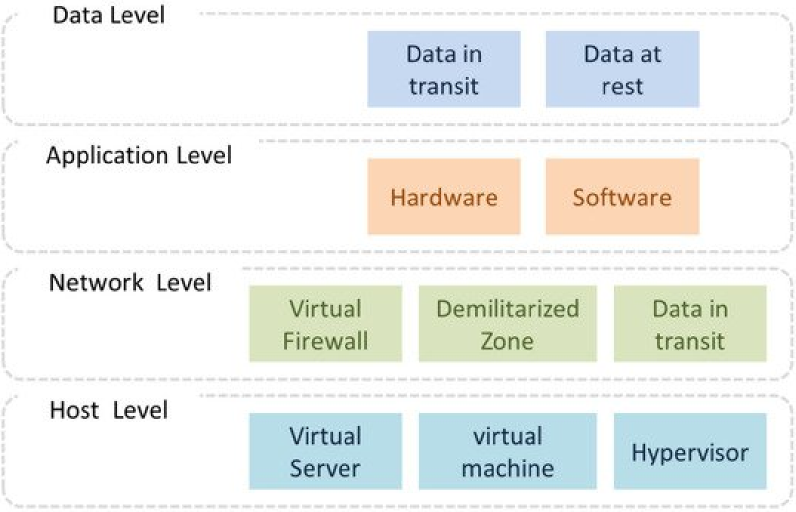

Figure 2. Cloud infrastructure levels.

There are many attacks on cloud users, such as phishing and fraud, that can affect the infrastructure of cloud services. Phishing and fraud are ways to steal a legitimate user's identity, such as credentials and credit card information. Usually, phishing is performed by sending the user an email containing a connection to a fraudulent website that looks like a legitimate one. When the user visits the fraudulent website, the username and password are sent to the attacker, who can use them to attack the cloud. Another type of phishing and fraud is to send the user an email claiming to be from the provider of cloud services and to ask the user to provide his/her credentials for maintenance purposes [27]. Although attacks targeting the end user on the cloud look similar to those on conventional systems, they are not identical, as cloud users can gain access from different platforms, which gives the attacker more options to break into the system.

Issues regarding confidentiality are rising due to the growing number of cloud users working in a multi-tenant environment, where compromising one system could lead to a chain of subsequent compromises in other systems. Sniffing attack is the most prominent issue. This occurs in a cloud environment when unencrypted packets of data are transferred between two entities in the cloud. These packets can, therefore, be captured, leading to the exploitation of confidential information. In a cloud environment, the existence of an entity with a promiscuous mode in the network node highly suggests that data in the node are being monitored by an attacker [28]. In addition, the reused IP addresses lead to the compromising of confidentiality, if not handled properly when reassigned to another user [28].

Since user data are stored in the server set of the cloud service provider (CSP) that operates concurrently and in a distributed way, the integrity and the confidentiality of the data stored at the CSP must be maintained. This can be achieved by ensuring that CSP employees have restricted access to user data and strict security procedures to ensure that only authorized employees gain control and access to CSP servers. In addition, well-defined data backups and redundant data storage can be used by the CSP to make data recovery possible [27]. However, the transparency between the user and the service provider may play a decisive role in this matter [29], as the customer is aware of the storage sites, the policies followed, as well as the protection methods followed.

4. Related Existing Solutions in Cloud Levels

The work in [30] defined the data security modeling design in cloud computing. Data security in all cloud storage layers was discussed. Based on this study, the standard cloud storage uses a three-level cloud data security model that can be expanded to a fourth level responsible for data integrity checks. The paper introduced the design of a four-level data security model in cloud computing that describes each part of cloud data security using Petri nets.

The authors in [31] suggested a hybrid algorithm to improve cloud data security using an encryption algorithm. To improve cloud security, this study combined homographic and blowfish encryption algorithms. The blowfish algorithm was used to generate a security key. A symmetric key block was used for both decryption and encryption. Homographic encryption, on the other hand, provides confidentiality of data and prevents storing the information in plain text at any stage.

Another important point is that more attention is given to the availability of the network by solving DNS issues using firewalls; however, there are several forms of DNS attacks such as a man-in-the-middle attack, modified data attack, DNS ID spoofing attack, corrupted data attack, and DDOS attack that cannot be solved by using the traditional firewalls and can be overcome by other techniques.

According to [32], a parameterized scheduling policy focused on minimizing the makespan, combined with an energy-efficiency policy based on the hibernation of every virtual machine whenever possible, could reduce the energy consumption of large-scale data centers without affecting the overall performance of cloud computing systems. In the same work, the authors described a model for reducing energy consumption in cloud computing environments that can reduce the energy consumption of a cloud computing system by up to 45%. The proposed model is divided into two parts: an energy-aware independent batch scheduler and a set of energy-efficiency policies for idle VM hibernation. The experimental results show the good performance of the proposed model.

References

1. Elsherbiny, S.; Eldaydamony, E.; Alrahmawy, M.; Reyad, A.E. An extended Intelligent Water Drops algorithm for workflow scheduling in cloud computing environment. Egypt. Inf. J. 2018, 19, 33–55.
2. Hanen, J.; Kechaou, Z.; Ben Ayed, M. An enhanced healthcare system in mobile cloud computing environment. Vietnam J. Comput. Sci. 2016, 3, 267–277.
3. Mell, P.; Grance, T. The NIST Definition of Cloud Computing; Nation-al Institute of Standards and Technology: Gaithersburg, MD, USA, 2011.
4. Hatwar, S.V.; Chavan, R. Cloud Computing Security Aspects, Vulnerabilities and Countermeasures. Int. J. Comput. Appl. 2015, 119, 46–53.
5. Dinh, P.T.; Park, M. Dynamic Economic-Denial-of-Sustainability (EDoS) Detection in SDN-based Cloud. In Proceedings of the 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), Paris, France, 20–23 April 2020.
6. Karajeh, H.; Maqableh, M.; Masa’deh, R. Privacy and security issues of cloud computing environment. In Proceedings of the 23rd IBIMA Conference Vision, Valencia, Spain, 13–14 May 2020.
7. Han, J.; Zang, W.; Chen, S.; Yu, M. Reducing Security Risks of Clouds Through Virtual Machine Placement. In Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy, Philadelphia, PA, USA, 19–21 July 2017.
8. Saravanan, N.; Umamakeswari, A. Lattice based access control for protecting user data in cloud environments with hybrid security. Comput. Secur. 2021, 100, 102074.
9. Vaquero, L.M.; Rodero-Merino, L.; Caceres, J.; Lindner, M. A Break in the Clouds: Towards a Cloud Definition; ACM: New York, NY, USA, 2008.
10. Siddiqui, S.; Darbari, M.; Yagyasen, D. A Comprehensive Study of Challenges and Issues in Cloud Computing. In Soft Computing and Signal Processing; Springer: Singapore, 2019; pp. 325–344.

11. Marston, S.; Li, Z.; Bandyopadhyay, S.; Ghalsasi, A. Cloud Computing—The Business Perspective. Decis. Support Syst. 2011, 51, 176–189.

12. Ibrahim, F.A.M.; Hemayed, E.E. Trusted Cloud Computing Architectures for infrastructure as a service: Survey and systematic literature review. Comput. Secur. 2019, 82, 196–226.

13. Qureshi, A.; Dashti, W.; Jahangeer, A.; Zafar, A. Security Challenges over Cloud Environment from Service Provider Prospective. Cloud Comput. Data Sci. 2020, 1, 1–48.

14. Faheem, M.; Akram, U.; Khan, I.; Naqeeb, S.; Shahzad, A.; Ullah, A.; Mushtaq, M.F. Cloud Computing Environment and Security Challenges: A Review. Int. J. Adv. Comput. Sci. Appl. 2017, 8, 183–195.

15. Sikeridis, D.; Papapanagiotou, I.; Rimal, B.P.; Devetsikiotis, M. A Comparative taxonomy and survey of public cloud infrastructure vendors. arXiv 2017, arXiv:1710.01476.

16. Bokhari, M.U.; Makki, Q.; Tamandani, Y.K. A Survey on Cloud Computing. In Big Data Analytics; Advances in Intelligent Systems and Computing; Springer: Singapore, 2018; Volume 654, pp. 149–164.

17. Kumar, R.; Goyal, R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Comput. Sci. Rev. 2019, 33, 1–48.

18. Abdurachman, E.; Gaol, F.L.; Soewito, B. Survey on Threats and Risks in the Cloud Computing Environment. Procedia Comput. Sci. 2019, 161, 1325–1332.

19. Alhenaki, L.; Alwatban, A.; Alamri, B.; Alarifi, N. A Survey on the Security of Cloud Computing. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019.

20. An, Y.Z.; Zaaba, Z.F.; Samsudin, N.F. Reviews on Security Issues and Challenges in Cloud Computing. IOP Conf. Ser. Mater. Sci. Eng. 2016, 160, 012106.

21. Subramanian, N.; Jeyaraj, A. Recent security challenges in cloud computing. Comput. Electr. Eng. 2018, 71, 28–42.

22. Kumar, P.R.; Raj, P.H.; Jelciana, P. Exploring Data Security Issues and Solutions in Cloud Computing. Procedia Comput. Sci. 2018, 125, 691–697.

23. Dong, S.; Abbas, K.; Jain, R. A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments. IEEE Access 2019, 7, 80813–80828.

24. Domingo-Ferrer, J.; Farràs, O.; Ribes-González, J.; Sánchez, D. Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. Comput. Commun. 2019, 140, 38–60.

25. Tabrizchi, H.; Rafsanjani, M.K. A survey on security challenges in cloud computing: Issues, threats, and solutions. J. Supercomput. 2020, 76, 9493–9532.

26. Saini, H.; Saini, A. Security Mechanisms at different Levels in Cloud Infrastructure. Int. J. Comput. Appl. 2014, 108, 1–6.

27. Turab, N.M.; Abu Taleb, A.; Masadeh, S.R. Cloud Computing Challenges and Solutions. Int. J. Comput. Netw. Commun. 2013, 5, 209–216.

28. Mohiuddin, I.; Almogren, A.; Alrubaian, M.; Al-Qurishi, M. Analysis of network issues and their impact on Cloud Storage. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019.

29. Aich, A.; Sen, A. Study on Cloud Security Risk and Remedy. Int. J. Grid Distrib. Comput. 2015, 8, 155–166.

30. Balogh, Z.; Turčáni, M. Modeling of data security in cloud computing. In Proceedings of the 2016 Annual IEEE Systems Conference (SysCon), Orlando, FL, USA, 18–21 April 2016.

31. Sajay, K.R.; Babu, S.S.; Vijayalakshmi, Y. Enhancing the security of cloud data using hybrid encryption algorithm. J. Ambient. Intell. Hum. Comput. 2019, 1–10.

32. Fernández-Cerero, D.; Jakóbik, A.K.; Grzonka, D.; Kołodziej, J.; Fernández-Montes, A. Security supportive energy-aware scheduling and energy policies for cloud environments. J. Parallel Distrib. Comput. 2018, 119, 191–202.

Retrieved from https://encyclopedia.pub/entry/history/show/35558