A Survey on Data Security Challenges and Their Solutions in Cloud Computing

Ruchi Billore and Manish Pandey

Abstract As technology increases rapidly, the demand for cloud computing is also growing day by day due to its features like on-demand services, cost efficiency, and rapid elasticity. The work which was traditionally done on-premise, now performed remotely across the internet or off-premise. And with increasing popularization of cloud computing the security becomes a major concern. Because user stores their confidential data on the cloud so they require high-security policies from cloud service providers to keep user's data safe and confidential. In this paper, we are going to explain some major threats associated with data in cloud computing at all stages of the data life cycle and also discuss some solutions to emerge from the threats and these solutions are discussed based on structural properties of the cloud storage system.

Keywords Cloud computing · Cloud service provider · Cloud consumer · Data life cycle

1 Introduction

Cloud computing is a computing which provides on-demand, self-managed and efficient use of virtual resources. In recent years, cloud computing and storage have developed into well-liked topics. These two changing our way of living and have increased production efficiency in some areas. To use cloud base services, one requires only a decent internet connection. At present, if we store data locally, we've to accommodate numerous overheads along with the risks. Because of the defined storage resources and need for convenient usage, we select cloud servers to accumulate every kind of information, which is simple to access for companies and organizations too. For everybody, the cloud server gives an open and favorable storage platform, but it also announces risks of data security. Cloud computing is becoming famous for its three distinguishing qualities. Firstly, it can scale up or

R. Billore (✉) · M. Pandey
Computer Science Engineering, Maulana Azad National Institute of Technology, Bhopal, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2021

V. Nath and J. K. Mandal (eds.), *Proceeding of Fifth International Conference on Microelectronics, Computing and Communication Systems*, Lecture Notes in Electrical Engineering 748,
https://doi.org/10.1007/978-981-16-0275-7_25

scale down quickly as per the user requirement. Secondly, users have to pay only for what they use and require no capital expenditure to start using cloud services. And finally, it is self-service for which there is no need for IT experts to install or use any resources. Along with these, cloud computing also provides fast access to resources and applications, it gives you the latest applications for use without wasting your time and expenditure on installations.

As every coin has two sides, which means along with these many pros of clouds, there are some major cons associated with data security, as cloud consumer even stores confidential data on the cloud such as documents, organizations policies, etc. Due to easy and remote access control, i.e., we can use our data from anywhere in the world where the only requirement is a good internet connection, this feature attracts users the most and makes cloud computing popular for storing data and sharing information through it, due to which security becomes major concern among cloud service providers and we are going to explain some of the data security-related concerns of cloud computing and further techniques used to resolve security risks and make cloud computing more secure and most trusted third-party resource to store data.

Data of consumers are stored on a shared cloud system rather than the devices of cloud service providers, so consumers don't have the knowledge about how the data is stored on the cloud or how their data is encrypted and stored on the cloud to maintain integrity and confidentiality of data so that only authorized person can access it and if an attacker somehow manages to get the data, still the information cannot be decrypted easily. The NIST defines cloud computing as: "Cloud computing is a model for enabling ubiquitous, convenient and 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models" [1] explained in Fig. 1.

A. *Deployment models:*

- **Public Cloud:** In a public cloud, the cloud service provider owns the cloud infrastructure and makes it available to every user. By tapping on the public cloud, consumers can get new capabilities on demand just by paying the subscription fee for the resources they wish to use.
- **Private Cloud:** In a private cloud, a single organization owned the cloud infrastructure. It may be handled by the organization itself or by a third-party, where the storage network and hardware assume the top levels of security. Only the clients who owned this private cloud are able to access the data stored in the data centre.
- **Community Cloud:** In community Cloud, cloud infrastructure is shared among different organization (ex. security requirements, policy, etc.). It would be handled by either organization or by a third party and may be located locally or across the internet.

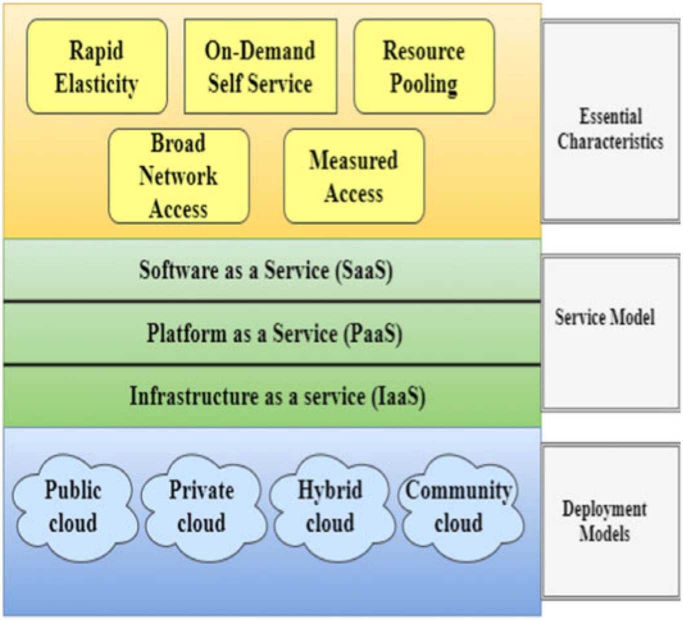

Fig. 1 Cloud model

- **Hybrid Cloud:** In a hybrid cloud, the cloud infrastructure is a combination of public and private cloud in a single environment and by standardized or proprietary technology. Clouds are bound together that permits application and data portability.

B. *Service models:*

- **Software as a Service (SaaS):** This service is totally managed and hosted by the cloud service providers in which a cloud consumer is directly going to use the applications. Consumers can use the services via a web browser or mobile application.
- **Platform as a Service (PaaS):** PaaS is concerned with abstraction and providing integrated development environments or platforms such as databases, application platforms (ex. to run Python, PHP, or other code), file storage and collaboration, or even proprietary application processing. The main inequality lies in the fact that with PaaS, there isn't any load of handling the underlying networks, servers, etc.
- **Infrastructure as a Service (IaaS):** IaaS is responsible for providing the infrastructure where the consumer can deploy and runs arbitrary software such as operating systems and applications. IaaS provides virtual resources to the consumers on a pay per usage basis so that consumers do not require to buy and maintain their own physical servers, they use resources in a convenient and as per their requirement.

C. *Essential characteristics:*

- Resource pooling is known to be the most elementary characteristic where the cloud service provider basically hide resources and the provider itself is responsible for collecting them in a pool which is then partitioned so as to allocate them to different consumers.
- By using on-demand self-service, Consumer's provision for the resources from the pool is fulfilled They themselves are required to manage their resources. The administrator has no role to play in this task.
- Broad network is actually the availability of the resources over a network without the requirement of any physical access. An important point to note here is that the network is not necessarily part of the service
- Rapid elasticity simply allows consumers to expand or contract the resources, i.e., provisioning and de-provisioning of resources they use from the pool of resources. This task, as it sounds is quite delicate but is accomplished automatically. This helps to match the level of resource consumption with the demands.
- The usage of resources is a measured service. Which is used to monitor and report that consumer can only use what they are allotted. And utility computing term comes from here. Since the cloud computing resources can now be consumed like water and electricity, so similarly user have to pay for what they use.

The remaining paper flow: Sect. 2 introduces the different types of data security threats, risks, and challenges present in cloud computing, Sect. 3 contains the solution to those problems discussed in Sect. 2, and then finally, Sect. 4 concludes the whole paper.

2 Related Works

Many researchers have published their paper on cloud computing by taking different aspects like: observed attacks, identified vulnerabilities, and some suggested remedies.

1. "Morsy et al. [18] explained cloud security issues in virtualization and service-oriented technologies along with security dimensions related to isolation and multitenancy. Based on the analysis they recommended for an integrated and adaptive configuration-based security model. However, their study does not have a detailed analysis of the security requirements, related threats, associated vulnerabilities, and corresponding countermeasures, and their mappings."
2. Zhang et al. [19] defined cloud architecture into four layers to provide the services of cloud. And highlighted some security measures as the challenges for the cloud like: Automated security provisioning, virtual machine migration, hardware server consolidation, energy management, software framework, data security, storage technologies.

3. Pearson [20] to address the cloud related trust and privacy issues, the classical techniques are no longer flexible. Also defines the relation between the threats, vulnerabilities and privacy issues.
4. Modi et al. [25] discussed security issues in the cloud architecture deliberated as a layered architecture. However, by taking the data storage and data life cycle management techniques into account they could have given more privacy-related issues and their solutions.
5. Dahbur et al. [24] provide guidance to address the threats, vulnerabilities, risks that cloud environment brings itself. However, they did not provide the insight view of these issues.
6. Cong Wang et al. [21] discuss about data security issues and proposed a scheme provides data manipulation and security.
7. Subashini and Kavitha [23], they give study of security issues on the basis of delivery models of cloud. Explains different threats possible on each model (SaaS, PaaS, and IaaS).
8. Raj Kumar [22] explained about the security threats using transmission of information in cloud computing. Encryption and decryption techniques for providing to the cloud computing.

3 Security Threats in Cloud Computing

3.1 Threats

In cloud computing, trust is a major issue between the cloud service provider and the cloud consumer and also raises the number of security issues. The cloud security alliance (CSA) did a survey aimed to raise awareness of threats, risks, and vulnerabilities in the cloud and find the top 11 threats listed in the below Table 1:

3.2 Security Risks of Data

From the generation of data to the destruction of it, the data goes from many stages called data life cycle [2, 3]. The data life cycle can be divided into 7 stages and these seven stages are categorized into 3 layers [4] illustrated in Fig. 2, Many data security issues in the cloud is involved in all stage of the data life cycle some of them are discussed:

[1] **Data creation:** The data creation phase involves two activities, creating new data sets or manipulating older data. Only authorized users can make changes to the existing data. In cloud computing, cloud consumers and cloud service providers communicate with the help of interfaces and APIs [5]. Cloud computing posses certain data protection risks for cloud entities. Between the

Table 1 List of threats

Threat no.	Name of threat
1.	"Data Breaches"
2.	"Misconfiguration and Inadequate Change Control"
3.	"Lack of Cloud Security Architecture and Strategy"
4.	"Insufficient Identity, Credential, Access and Key Management"
5.	"Account Hijacking"
6.	"Insider Threat"
7.	"Insecure Interfaces and APIs"
8.	"Weak Control Plane"
9.	"Metastructure and Applistructure Failures"
10.	"Limited Cloud Usage Visibility"
11.	"Abuse and Nefarious Use of Cloud Service"

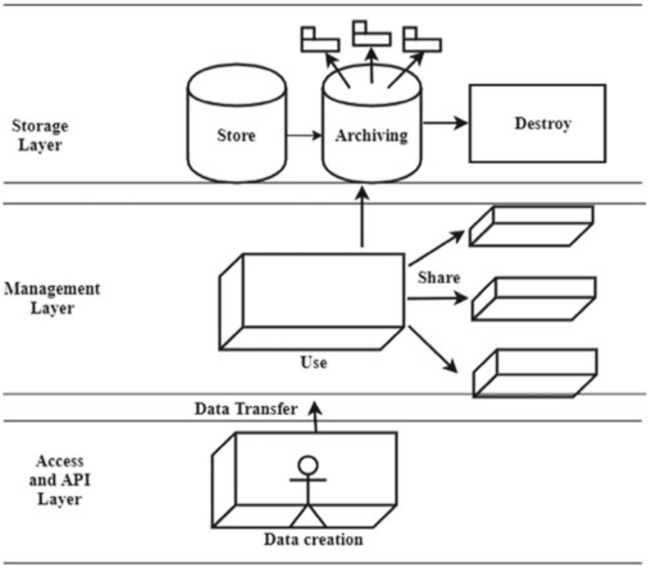

Fig. 2 Data life cycle

cloud entities, different kinds of service-level-agreement (SLA) are involved which lead to certain kinds of data leaks. It often happens, that checking the data handling practices of the provider becomes difficult for the cloud user [5].

[2] **Data transfer:** By default, data transmission is done through transport level security (TLS), which transfers data in a secured channel [6]. But there may be some chances of issues and threats possible. Tracing the path of data, auditing. It is tedious to trace the path because of the non-linear behaviour of the cloud

[7]. While data is transferred an eavesdropper can take confidential data and may inject some malicious information with original data. Therefore, along with the confidentiality, integrity of data is also required in the cloud.

[3] **Data use:** To gain better data access performance, the management layer caries out the task of collaboration between various storage devices through the cluster computing, distributed file system, and grid computing technology [4]. When a user accesses the data present in the cloud, to protect data from unauthorized user access is a major issue. Because once the attacker gets access privileges the privacy of data is broken and the attacker can change the encryption keys to prevent authorized users from the use services. Because of the metered feature of cloud computing many organizations adopting cloud computing without knowing about the threats [5].

[4] **Data share:** Increasing the usage range of data and information is made accessible between users, customers, and partners [8]. When data owner authorizes data access to other partners there may be chances that malicious insiders can take advantage and misuse the information and cannot maintain original security measures and usage restriction.

[5] **Data storage:** In the cloud, the user is not aware where their data is stored in the cloud due to the shared resources property of cloud i.e. data location is unknown, which leads questions of security, legal and requirement of regulatory compliance [6]. To store the massive amount of data, the data erasure technique is used by the service provider to satisfy users demand for storage. Due to this data integrity, transparency and availability issues arise in the cloud [4]. Multitenancy is also the main characteristic provided by cloud. Therefore, multiple consumers can store data on the same platform which makes data more vulnerable to data breach and loss of data [9].

[6] **Archiving:** The process of identifying and moving older inactive data to an independent storage device for long-term possession is called data archival. Archived data is important and can be used in the future so it focuses on the storage system. If storage media is portable then media is out of control and there is a risk of data leakage. If off-site archiving is not provided by the cloud service provider, the availability of the data will be threatened [2].

[7] **Destroy:** When data is no longer in use it is permanently destroyed using physical or digital means [8]. The data deleted may be still present and can be restored and inadvertently disclose sensitive information, due to the physical characteristic of storage medium [2].

4 Solutions for Security Issues

4.1 Access and Application Programing Interface (API) Layer

Protect the system from unauthorized user access. Before the user starts using cloud services, it is necessary to identify them whether the user is authorized or not. Roy I and Ramadan gave a fourth privacy protection system named "Airavat," which can prevent system from privacy leakage. This system uses decentralized information flow control (DIFC) and differential privacy protection protocols [10]. Khalid, develop a protocol for authentication and authorization. This protocol gave information about anonymous users and by using this, we can protect systems from unauthorized user access [6]. Lalitha proposed a work in which if the malicious user tries to access the system then an alert goes to admin with IP address through which admin can scrutinize the activities of the malicious user and can also block that IP address to prevent the system from unauthorized access [16]. Arora, build a secure cloud ecosystem, in which 2-step verification is applied, the first user enters the username and password after this they get one-time-password (OTP) to prove their identity, if the attacker gets password then also, he cannot enter into the system. For data transmission, SSL and TSL 1.2 are used and at the end uses a hybrid cryptographic system for encryption of data [9]. Puthalin proposed a security verification scheme using Dynamic prime numbers. Which reduces communication overhead [6].

4.2 Management Layer

To protect data from illegal user access, the basic requirement is the encryption of data. Which provides confidentiality to the user data. But the problem with encryption is the management of keys. User is not able to manage large amount keys therefore cloud service provider needs to maintain encryption keys. The Organization for the Advancement of Structured Information Standards (OASIS) Key Management Interoperability Protocol (KMIP) working to overcome key management problems [12]. With personal privacy information protection sharing of data is a challenge. Randike Gajanayake proposed a framework for privacy protection depends on Information Accountability (IA) components. IA agents monitor the activity of users. When the user tries to de illegal activity, IA agents detect it and apply some methods that force the user to accept his mistake [17]. Dong, defines a security policy for effective, scalable and privacy-preserving data sharing. The policy is made with the combination of two techniques i.e. CP-ABE and IBE [6].

4.3 Storage Layer

In cloud computing, it is necessary to use a secure storage system. R. Nivedhaa and J. Jean Justus, explain a secure erasure coding technique in which users data is divided and then encrypted using advanced encryption standard algorithm and proxy re-encryption [14]. Mowbray proposed a client-based security management tool. In which the user can configure it according to their requirement and can store and use their confidential information in the cloud in a secured manner [13]. Wei proposed a first protocol that makes storage and computation secure [15].

5 Conclusion

Over time, the use of cloud computing and inventing new features and techniques in it are increasing rapidly due to its prominent characteristics. At the same time, data security risks, threats, and challenges are also increasing and need to be solved as soon as possible. Because cloud computing is now used in health care, banks, private and public organizations, and many other fields. Where the user stores their confidential data, which cannot be compromised at any cost and for that it requires the highest security measures for data. In this paper, analysis of some data security threats and their solutions over the stages of the data life cycle and structural properties of the storage system are covered.

References

1. Mell P, Grance T. The NIST Definition of Cloud Computing, Version15, 10-7-09, http://www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def-v15.pdf
2. Chen D, Zhao H (2012) Data security and privacy protection issues in cloud computing. In: 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, pp 647–651
3. The-Egregious-11-Cloud-Computing-Top-Threats-in-2019-Feb 2020: https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/
4. Zhe D, Qinghong W, Naizheng S, Yuhan Z (2017) Study on data security policy based on cloud storage. In: 2017 IEEE 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), Beijing, 2017, pp 145–149
5. Hendre A, Joshi KP (2015) A semantic approach to cloud security and compliance. In: 2015 IEEE 8th International Conference on Cloud Computing, New York, NY, pp 1081–1084
6. Subramanian N, Jeyaraj A (2018) Recent security challenges in cloud computing. Comput Electr Eng **7**(2018), 28–42. http://dx.doi.org/10.1016/j.compeleceng.2018.06.006
7. Bhadauria R, Sanyal S (June 2012) Survey on security issues in cloud computing and associated mitigation techniques. Int J Comput Appl (0975-888) June 2012
8. https://assets.cloudsecurityalliance.org/legacy/wp-uploads/2011/09/Domain-5.docx

9. Arora A, Khanna A, Rastogi A, Agarwal A (2017) Cloud security ecosystem for data security and privacy. In: 2017 7th international conference on cloud computing, data science & engineering - confluence, Noida, pp 288–292
10. Cloud computing security. http://en.wikipedia.org/wiki/Cloud_ computing_security
11. Aich A, Sen A, Ranjan Dash S. A Survey on Cloud Environment Security Risk and Remedy. Computer Science and Engineering, KIIT University Bhubaneswar, India{acrana.dgp09,alosen10}
12. OASIS Key Management Interoperability Protocol (KMIP) TC. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip
13. Bowers KD, Juels A, Oprea A (2009) Proofs of retrievability: Theory and implementation. In: Sion R, ed. Proc. of the 2009 ACM Workshop on Cloud Computing Security, CCSW 2009, Co-Located with the 16th ACM Computer and Communications Security Conf., CCS 2009. Association for Computing Machinery, New York, pp 43–54 https://doi.org/10.1145/1655008.1655015
14. Nivedhaa R, Justus J.J (2018) A secure erasure cloud storage system using advanced encryption standard algorithm and proxy re-encryption. In: 2018 international conference on communication and signal processing (ICCSP), Chennai
15. Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, Vasilakos AV. Security and privacy for storage and computation in cloud computing. Inf Sci 2014 **258**:371–86. www.elsevier.com/locate/ins
16. Lalitha VP, Sagar MY, Sharanappa S, Hanji S, Swarup R (2017) Data security in cloud. In: 2017 international conference on energy, communication, data analytics and soft computing (ICECDS), Chennai, 2017, pp 3604–3608
17. Gajanayake R, Iannella R, Sahama T (2011) Sharing with care an information accountability perspective. IEEE Internet Comput **15**:31–38
18. Morsy MA, Grundy J, Müller I (2010) An analysis of the cloud computing security problem. In: Proceedings of APSEC 2010 cloud workshop, pp 1–6
19. Zhang Q, Cheng L, Boutaba R (2010) Cloud computing: state-of-the-art and research challenges. J Internet Serv Appl **1**(1), 7–18. http://dx.doi.org/10.1007/s13174-010-0007-6
20. Pearson S (2013) Privacy, security and trust in cloud computing. In: Pearson S, Yee G (eds) Privacy and Security for Cloud Computing, Springer, London, UK, pp 3–42. ISBN: 978-1-4471-4189-1, http://dx.doi.org/10.1007/978-1-4471-4189-1_1
21. Wang C, Wang Q, Ren K (2015) Ensuring data storage security in cloud computing. US National Science Foundation, pp 1–4
22. Kumar Raj (2015) Research on cloud computing security threats using data transmission. Int. J. Adv. Res. Comput. Sci. Softw. Eng. India 5(1):
23. Subashini S, Kavitha V.: A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl **34**(1):1–11. ISSN: 1084-8045. http://dx.doi.org/10.1016/j.jnca.2010.07.006
24. Dahbur K, Mohammad B, Tarakji AB (2011) A survey of risks, threats and vulnerabilities in cloud computing. In: Proceedings of the 2011 international conference on intelligent semantic web-services and applications, ISWSA 2011. ACM, New York, pp. 1–6, ISBN: 978-1-4503-0474-0. http://dx.doi.org/10.1145/1980822.1980834
25. Modi C, Patel D, Borisaniya B, Patel A, Rajarajan M (2013) A survey on security issues and solutions at different layers of cloud computing. J Supercomput **63**(2), 561–592, ISSN: 1573-0484. https://doi.org/10.1007/s11227-012-0831-5