IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⵗ Impact Factor 7.918 ⵗ Vol. 11, Issue 11, November 2022

DOI: 10.17148/IJARCCE.2022.111128

Identification of data integrity attacks in cloud computing

Samarth Kamble[1], Radhey Saykar [2], Gaurav Somani[3]

Student, Computer Engineering, Pune Institute of Computer Technology, Pune, India[1]

Student, Computer Engineering, Pune Institute of Computer Technology, Pune, India[2]

Student, Computer Engineering, Pune Institute of Computer Technology, Pune, India[3]

Abstract: Cloud computing has grown dramatically in recent years. Because of the low cost and pay-as-you-go nature of the cloud, many organizations are shifting away from traditional computing models. Despite the fact that the Cloud Service Provider (CSP) guarantees that the data stored in their remote cloud server will be intact and secure. However, there are numerous data integrity issues that must be addressed. Data integrity is a major concern in the cloud environment. In this paper, we reviewed several previous studies that identified issues with cloud data storage security, such as data theft, unavailability, and data breach of cloud server data. We also provided a detailed analysis of the various types of data integrity attacks such as SQL injection attacks, Unauthorized access attack, Authentication attack.

Keywords: Data integrity, Cloud security, Cloud services, Data privacy, Attacks on cloud.

I. INTRODUCTION

A variety of services are provided through the internet or a network as" loud computing." Technology advancements over the past few years have resulted in cloud computing, which has caused an organization's workflows to move off-site. Delivery of IT services and resources, such as bandwidth, databases, servers, storage, software, networks, and more, is flexible and affordable thanks to the Internet [2,3]. Today's new technology is so well-liked that academic scholars and businesses are interested in it [4]. Running a private data centre or having a lot of secondary storage is out of reach for many enterprises. Although cloud computing has numerous advantages, there are significant technical challenges and security concerns, such as data integrity, confidentiality, and privacy. Users and organisations lose their confidential data when they put data or information in cloud storage [7]. A variety of measures are required by cloud service providers (CSPs) to guard against alteration and corruption of customer data [8]. Service level agreements (SLAs) place restrictions on and hold cloud service providers (CSPs) accountable for information security, although they do not guarantee complete data integrity. Security is the top concern in cloud computing, according toa survey conducted by the International Data Organization (ID) [9]. It is critical to address privacy concerns and data integrity in the cloud [10,11,6]. We will first address the prior research paper on data integrity challenges in cloud computing in this overview paper. We will go into more detail about the potential data integrity attacks in opensource computing as well as the methods used to identify and avoid them later.

II. CHALLENGES AND ISSUES

The fact that users have no control over the data when it is stored in cloud storage is the primary drawback of cloud computing. Instead, Cloud Service Providers (CSP) control all the data stored in cloud data centres. The data may be altered, destroyed, or corrupted without the user's knowledge. The most significant obstacle to data integrity is the lack of consensus among stored sensitive data. Loud production is less expensive and requires less resource management, but there are significant security, privacy, and integrity risks associated with it. The multiuser architecture makes it possible for resources assigned to one user to eventually be assigned to another user. An attacker could use malicious code to take sensitive data from a previous user by taking advantage of the resource pooling vulnerability. In multi-tenant clouds, data storage risks can arise from improper disk cleaning. Data becomes unusable because of accidental or deliberate malfunctions in the substrate. Data falsification as well as unauthorized access to secure environments can be prevented through the use of security mechanisms [12].

To stay ahead of the competition, some organizations are now offering competitive rates as well as speedy and secure IT solutions. There are significant costs associated with security, upkeep, space, employment, and other factors when businesses store data on their own servers.IT companies discovered a solution that could store company data at a lower cost, could be accessible to anyone on the network, and could be accessed by anyone using cloud computing [13,8]

A. Advantages

1. Compatibility: The documents can be made compatible to other operating systems thanks to cloud computing.
2. Cost effectiveness: The documents can be made compatible to other operating systems thanks to cloud computing.
3. Flexibility and time: One may effortlessly access their data from anywhere at any time thanks to cloud storage. This might compel individuals from all around the world to work on the same project concurrently. There is no need to waste time managing and maintaining

B. Disadvantages

1. Data integrity: Information accessed or altered by unauthorized users can be considered integrity.The application platform is shared by multiple institutions on a multitenancy basis, allowing users to share information with any other unauthorized user in the cloud and causing an integrity breach. Data is an important part of cloud services like SaaS and PaaS that provide services. As a result, data integrity is a rudimentary task.
2. Data location: The location of the data is very important for the Storage as a Service (SaaS) model. Due to the unknown location of their data, some cloud users are reluctant to store sensitive data there. This is one of the most common worries that most businesses have, which causes security problems, legal problems, and requirements for regulatory compliance. Unreliable cloud service providers have made this one of the most pressing issues.
3. Data privacy: Data privacy is crucial in the world of cloud computing. Many businesses find it more convenient to store important data on-site rather than on the cloud. Many questions are generated because users of the cloud are unaware of how their data is kept, moved, operated in the cloud, and other things of the sort. Some of the many questions which cloud users have concern whether or how data is exchanged with third parties, the creation and deletion of files, the location of information, information backup, and who has access to the information.
4. Multiple people and organisations can access the cloud environment from any location because their data is saved in one location. If there is a break or cloud issue, sensitive data of the clients may be exposed. Due to its multi-tenancy, customers using various apps on the virtual machines may share the same database, and any compromising incidence may have an impact on other users sharing the exact same database. The common causes of data breaches were found to be hacking and malware, according to Kumar and Arri’s (2013) 2011 Data Breach Investigations Report.
5. Internet connectivity: The requirement of an active internet connection could be problematic. Even if the Cloud Service Providers (CSPs) ensure high quality service, a fault on client side can cause poor service experience.
6. Malicious insiders: Authorized personnel who are tasked by cloud service providers with managing and maintaining the cloud are referred to as malicious insiders. These clients frequently send sensitive data to file-sharing services after stealing or manipulating it from cloud providers. This unethical work can be paid for by these insiders. Service providers may not always be able to act against these employees.

III.DATA INTEGRITY ATTACKS ON CLOUD STORAGES

A. Unauthorized access: Users cannot access files or data during this assault, and data is changed without their knowledge. This is a possibility both inside and outside the cloud security organisation. The most serious assault was this one. When this occurs, it leads to a data breach employing reusing drivers and old hardware[9,10].

B. SQL injection attack: This is the most typical and popular data attack. This requires a web application that makes a SQL query, transmits it to the database, and returns the relevant data when the query has been processed by the database[11]. This is what typically occurs. This attack happens when a malicious text or piece of data is sent in a request and subsequently causes the system to take a step that it should not normally do.

C. Security against internal and external attacks: A user increases their risk of being attacked if they log out before leaving the system. Someone else can access the system and carry out destructive actions that could reveal both internal and external attacks [9,12]. Data about users is not secure on the S-side. Additionally, always on data encryption safeguards data privacy.

D. Authentication Attacks:

1. Phishing Attack - Here the attacker finds every combination of code and tries it.
2. Replay Attack - It happens when an unidentified person views the data stream and sends the communication data to this location under their own identity. To stop this attack, timestamps and sequence numbers must be used.
3. Brute force OR Dictionary attack - Here the attacker attempts any combination of passwords to gain access to user’s data. Lengthier the password, harder it is for the attacker to crack it.

DOI: 10.17148/IJARCCE.2022.111128

IV. IMPLICATIONS

A. Proof of retrievability technique: Proof of retrievability technique is used to verify the date of from cloud service provider remotely. In this method the user stores files in CSP along with authentication key. Using this key user can authenticate the data from server without storing it locally.

B. Protecting Data Integrity Using Encryption: Data encryption considers the better solution for storing data in cloud storage. Encrypting the data before storing it to cloud server makes it useless. Additionally hash value technique can also be used to ensure that encrypted data is not modified. The hash value of data is calculated and stored with encrypted data. Encryption on its own only provides confidentiality and does not provide authenticity or integrity.

C. Hash function and summary representation: Since cryptographic operations are computationally expensive, it's more convenient to run them over a short summary that represents the (potentially much larger) amount of data. A cryptographic hash function takes an arbitrary length input and produces a fixed length digest or "hash" which will serve as a summary of the data. Since the function maps arbitrarily large inputs to a fixed output range, collisions are guaranteed to occur. However, by making the size of the hash output sufficiently large, the collision probability can be made negligible. Another important property of a hash function is that even very small changes in the input data, say a single bit flip, will result in substantial changes in the output hash.

V. CONCLUSION

In this article we have covered several attacks which CSP's can identify. Cloud Service Providers like AWS, Microsoft Azure, Digital Ocean, etcetera oversees protecting the user's data. Even though they claim that the data will be safe, security breaches might cause data integrity to be lost. Several writers have suggested various mitigation techniques to lessen the likelihood of these attacks. It is critical to remember that cloud computing must be carefully built to maintain data security. The area of data integrity in cloud computing presents a lot of unresolved research questions. The current methodologies and upcoming techniques considerably aid the growing giant as Cloud Computing.

ACKNOWLEDGMENT

The authors would like to thank **Prof. Nikita Y. Kapadnis**, Assistant Professor, Pict, Pune for her guidance in writing this paper.

REFERENCES

[1]. Durga Venkata Sowmya Kaja, Yasmin Fatima and Akalanka B. Mailewa "Data Integrity Attacks in Cloud Computing: A Review of Identifying and Protecting Techniques" Feb 2022 IJRPR ISS N 2582-7421.

[2]. Data breach investigation report by Kumar and Arri, India, 2013.

[3]. "Survey on various data integrity attacks in cloud environment and the solutions - IEEE Conference Publication.". Feb. 05, 2021.

[4]. Lai, Cheng-I., Alberto Abad, Korin Richmond,Junichi Yamagishi, NajimDehak, and Simon King. " Attentive filtering networks for audio replay attack detection." In ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), pp. 6316-6320. IEEE, 2019.

[5]. A. Jyoti, M. Shrimali, S. Tiwari, and H. P. Singh, "Cloud computing using load balancing and service broker policy for IT service: a taxonomy and survey," J. Ambient Intell. Humaniz. Comput., vol. 11, no. 11, pp. 4785–4814, , Nov. 2020.

[6]. R. V. Rao and K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing," Procedia Comput. Sci., vol. 48, pp. 204–209, Jan. 2015.

[7]. V. Chang and M. Ramachandran," Towards Achieving Data Security with the Cloud Computing Adoption Framework," in IEEE Transactions on Services Computing. Feb. 1, 2016.

[8]. M. Henze, J. Hiller, O. Hohlfeld and K. Wehrle," Moving Privacy Sensitive Services from Public Clouds to Decentralized Private Clouds," 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW), Berlin, 2016.

[9]. Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. " Vulnerability prioritization, root cause analysis, and mitigation of secure data analytic framework implemented with mongodb on singularity linux containers." , In Proceedings of the 2020 the 4th International Conference on Compute and Data Analysis, pp. 58-66. 2020.

[10]. S. Sudalai and S. S., "A Survey on Cloud Security Issues and Challenges with Possible MeasuresA Survey on Cloud Security Issues and Chall enges with Possible Measures,", Apr. 2016.

DOI: 10.17148/IJARCCE.2022.111128

[11]. Lai, Cheng-I., Alberto Abad, Korin Richmond,Junichi Yamagishi, NajimDehak, and Simon King. ” Attentive filtering networks for audio replay attack detection.”, ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 6316-6320. IEEE, 2019.

[12]. Review on Cloud Computing Security Challenges, European Scientific Journal, April 2020

[13]. T. V. Sathyanarayana and L. M. I. Sheela,” Data security in cloud computing,” International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), Chennai, 2013.

[14]. “Cloud computing features, Issues and Challenges: A big picture”, Deepak puthal, B.P.S Sahoo, Sambit Mishra, Satyabrata swain, International Conference on Computational Intelligence Networks, 2015.

[15]. Bojken SH, Shqiponja A, Marin A, Aleksander XH,” Protection of Personal Data in Information Systems”, International Journal of Computer Science, 2013

[16]. Cloud Computing Data Security and Risk Assessment Jing J Li and Qinyuan W.Li, State Grid Zhejiang Electric Power Research Institute, Hangzhou, China

[17]. Data Integrity Attacks in Cloud Computing: An Overview of Identifying and Protecting Techniques, International Journal of Innovations in Engineering and Science, 2022

[18]. Data Integrity Attacks in Cloud Computing: A Review of Identifying and Protecting Techniques, International Journal of Research Publication and Reviews, 2022

[19]. Survey on Various Data Integrity Attacks in Cloud Environment and the Solutions, International Conference on Circuits, Power and Computing Technologies by Meena S Esther Daniel Dr. N.A. Vasanthi, 2013

[20]. Data Integrity and Security in Distributed Cloud Computing by NOMULA MADHAVI and MUNIYANAIK KETHAVATH, 2019.