https://doi.org/10.46335/IJIES.2022.7.9.11 **e-ISSN: 2456-3463**
Vol. 7, No. 9, 2022, PP. 52-56
International Journal of Innovations in Engineering and Science, www.ijies.net

Data Integrity Attacks in Cloud Computing: An Overview of Identifying and Protecting Techniques

Srushti Pravin Watekar[1], Prof. Neha Mittal [2]

[1]Student, Department of Master of Computer Application, [2]Assistant Professor,
G H Raisoni Institute of Engineering & Technology, Nagpur, India, 440016

srushti.watekar.mca@ghrietn.raisoni.net

***Received on**: 11 June ,2022* ***Revised on**: 07 August ,2022,* ***Published on**: 09 August s,2022*

Abstract- *Cloud Computing is a range of services delivered over the internet or 'the cloud'. In recent years, Cloud Computing has become fastest emerging technology. Because of its low cost and pay-as-you-go manner many organisations are shifting their traditional computing model to a cloud-based model. Even though CSP (Cloud Service Provider) ensures that the data that is stored and secure in their cloud server, there are various data integrity issues which are essential to be addressed. Lack of data integrity in cloud environment is a serious concern. In this paper, I have surveyed previous studies which identifies the issues related to cloud data storagesecurity like unavailability, data breach of cloud server data and data theft.*

Keywords-- Data Integrity, Vulnerabilities, Cloud Computing, IDS/IPS, Security, Attack

I- INTRODUCTION

Cloud computing is a rangeofservices delivered over the internet or the cloud. With advances in technology over the past few years, cloud computing has led to the fact that an organization's workflows are shifted off-site. The Internet enables flexible and cost-effective delivery of IT services and resources, including bandwidth, databases, servers, storage, software, networks, and more[2,3].This newtechnologytoday, is so popular that academicresearchers and industries take interest in it [4]. For many organizations, running a private data center orhavinglarge secondarystorage is over budget. Cloud storage is the best option for these organizations due to its flexibleservice model [5]. Asshown in Figure 1, there arethree cloud storagemodels:

Fig 1- Cloud Service Models

- Iaas (Infrastructure as a Service)
- Paas (Platform as a Service)
- Saas (Software as a Service)

Though there are many benefits of cloud computing [6], there are some technical hurdles and security issues, such as data integrity, confidentiality, and privacy. When a user or organizationstores data or information in the cloud storage, they lose their confidential data [7].Cloud service providers (CSPs) must use a variety of mechanisms to protect their customers' data from modification and corruption [8].Cloud Service Providers (CSPs) are responsible for ensuring information security and are limited by service level agreements (SLAs), but do not provide 100% data integrity.There are many data integrity issues that can confuse cloud providers and become a nightmarefor users. Forexample,

https://doi.org/10.46335/IJIES.2022.7.9.11 e-ISSN: 2456-3463
Vol. 7, No. 9, 2022, PP. 52-56
International Journal of Innovations in Engineering and Science, www.ijies.net

informationcanbe manipulatedintentionally or accidentallythrough malicious actions,vulnerabilities that exist in common multi-user models can be exploited, other user's data can be damaged, data backup failures, data breaches, etc. [3].According to an International Data Corporation (IDC) survey, security is the number one concern in cloud computing [9]. Addressing privacy issues and data integrity in the cloud is urgent [10,11,6]. In this overview paper,we will first discuss the previousresearch paper on data integrity issues in cloud computing. Later, we will discuss the possible data integrity attacks in Cloud Computing and the mechanisms used to detect and prevent them in detail.

II-CLOUD DATA STORAGE CHALLENGES AND ISSUES

The main disadvantage of cloud computing is that once the data is stored in cloud storage, users can haveno control over the data. Instead, cloud serviceproviders (CSPs) have full control over information stored in cloud data centers. CSP maymodify, destroy, or copy data without the user's knowledge.Lack of control over stored sensitive data is the biggest challenge to data integrity. Cloud computing is cheaper and requires less resourcemanagement,but comes with significant data security, privacy, and integrity risks. Due to the multi-user architecture, resources allocated to one user may sooner or later be allocated to another user.An attacker could exploit resource pooling vulnerability and use malicious code to recover sensitive data from a previous user. Incorrect disk clean-up can lead to data storage risk in multi-tenant clouds. Data becomesunusable due to accidental or intentional data backup failures.Securitymechanismscould be used to forestall data falsification and unauthorized access to cloud environments [12].

SomeOrganizationstoday,are offering competitive rates, fast and secure IT solutions to stay ahead of the competition. When the companies store data on their own servers, it cost a lot in terms of security, maintenance, space, employment, etc. Afteryears of research, IT companies found asolution that could store company data atlower cost, can beavailable and accessed by anyone over a network using cloud computing [13,8]. Some benefits of cloud computing are discussedbelow:

1. **Compatibility:**
   The Cloud allows your documents to be compatible with other operating systems as well.
2. **Flexibility and Time:**
   Cloud storage allows you to easily access your data anytime, anywhere over theInternet. This could force people around the world to work on the same project at the same time. No need0 to waste time onmanagement and maintenance.
3. **Cost Effective:**Cloud model reduces the maintenance cost, security cost, softwarelicense cost, personaltraining cost and operational cost by using Pay-as-you-go method.
4. **Back-up and Restore Data:**Once information is stored in the cloud, it can be easilyrestored and backed upfrom the cloud.

In addition, to the benefits mentioned above, the cloud computing alsohassome drawbacks, which are discussedbelow:

1. **Internet Connectivity:** Even if the cloud serviceproviderprovides the highest quality cloud service to their customers, if the internet connection is lost, and they won't be able to access the data until they restore it.
2. **Data Location**: In cloud computing, the physical location of the cloud server where the data is stored is notknown and these details are not transparent to client. Servers may be located in different countries[8].
3. **Data Integrity:**Customer's greatest concerns are that their data will not be intentionally or accidentally corrupted, altered or deleted.
4. **Data Confidentiality and Privacy:** It is important to keep the confidentiality and personal data of clientssafe. However, when data is stored on an external server, the main concern of client is who can access that data.

III-TYPES OF DATA INTEGRITY ATTACKS

The following are some data integrity attacks related to cloud computing:

1. **Unauthorized Access:**In this attack, users have no access to files or data, and data is altered without control. This can happen inside and outside the security organisation in the cloud [14]. This is the most serious attack. When this happens, it results in a data breach using outdated hardware and driver reuse [3]**.**
2. **SQL Injection Attack:** This is the most common and widely used data attacks. This requires a web application that generates a SQL query and it sends it to the database, and when the query is executedon thedatabase,thecorresponding data is returned to the

https://doi.org/10.46335/IJIES.2022.7.9.11 e-ISSN: 2456-3463
Vol. 7, No. 9, 2022, PP. 52-56
International Journal of Innovations in Engineering and Science, www.ijies.net

application.This is whatusually happens. This attack occurs when a malicious string or data is passed in a request and then performs an action on the system that ideally it shouldnotdo [15].

3. **Data Lock-in:** There are no rules or conditions for data storage that depends on CSPs in the cloud [14]. Typically, pieces of data are spread across servers and systems.Corporation shouldnotswitchfromoneprovider to another as this person can lead to loss of user data and cause problemson the front end. If there is no data loss, the CSP server should be stable [3].
4. **Security Against Internal and External Attacks**: If a user leaves the system withoutloggingout, the risk of an attack increases. Someone else can open the system and perform malicious actions thatcan expose internal and external attacks [14]. User data is not secure on the CSPside. In addition, to this always-on data encryptionprotects data privacy [3].
5. **Authentication Attacks:** Following are few authentication attacks:
    - **Phishing Attack-** It is about how anattacker finds everycombination of code and more the complexcode, the longer it takes an attacker to learn it [18].
    - **Replay Attack-** It occurs when unknown person views the data stream and thensends thecommunicationdata tohis location as the original sender. Timestampsandsequencenumbers must be implemented to prevent this attack [16].
    - **Brute Force Attack or Dictionary Attack-** It is a basic attack in which attacker attemptsany combination of passwords to again access to user data.Lengthy passwords take longerfor user to crack to guess the correct password [17].

IV-MECHANISMS USED FOR DETECTING & PREVENTING DATA INTEGRITY ATTACKS ON CLOUD ENVIRONMENT

Attackers can be anythingfromowners to malicious users or untrusted third parties in the CSP. Severalmechanisms and schemashave been proposed to protect data ownership and data integrity in cloud computing environments. Following are some mechanisms reviewed in past studies [19]:

1. **Protecting Data Integrity Using Encryption:** Data encryption is said to be the best solutionforprotecting data in the cloud. Data must be encrypted before being stored on servers, which renders the data unusable. The hashvalue of data must also be computed before being stored on servers. This ensures that the data hasnot been modified [20].
2. **Mitigation of Tag Forgery and Data Leakage Attack:** When CSPs attempt to scam users using deceptive data tags, users can find out and become victims. To prevent such attacks, there are transparent data validation and reliable protection methods. The client generates a call tag before sending CSP information and passes it later to the cloud service provider. They challenge cloud serviceproviders by verifying data integrity via trusted third party (TTP) [19].
3. **Mitigation of Malicious Data Attack:**High Availability and Integrity Layer (HAIL) protocol ensures that user data can be safely retrieved from the server without being compromised. Files are distributed using Erasure's fix code to provide redundancy and to make data available in the event of a server malfunction and this prevents malicious attacks [19].
4. **POR (Proofs of Retrievability) Technique:** This is a technique that uses an authentication key to remotely validate data stored by CSP, eliminating the need to retrieve data from the CSP and store it neither. The original copy of file is stored locally in CSP file along with authentication key. Users can use this authentication key to verify the integrity of their data without extracting files from the CSP[7,21].

V-RESULTS

This section is an overview of the most common data integrity attacks in cloud computing, and this article presents some of the mitigation techniques proposed by someother authors in variousresearcharticles and meetings as solutions to these attacks as described in previoussections.To sum up the summary some problem typeshave anavailable solution to solve like: Data Leakage can be solved by UserRank method, XML attack can be solved by Filter based Approach, Data IsolationFailure can be solved by multi-tenant data isolation or SharingMiddlewareScheme, Spoofing can be solved by Strong Authentication, SQL Injection Attacks can be solved by Parameterized Statements, Sniffer Attacks can be solved by SSH or IPsee and so on.

VI-CONCLUSION

In this article, we havediscussedsome of the attacksthat cloud serviceproviders (CSPs) can detect.IA shortnoteon Cloud Computing and Data Integrity has been discussed. This article is discussed inrelation to relatedwork byother authors. A lot of organisations like AWS are starting to implement cloud computing technologies. CSPs are responsible for securing data of companies that may store data in various formats.Confidentiality and Data Integrity are major concerns for Cloud Computing. Severalmitigationtechniqueshave been discussed to prevent data loss. In conclusion, it is important to note that Cloud computing must be designed carefully to ensure data security and should be considered along with all the aspects of security. Data Integrity is a great opportunity for research work and is a wide-open issue in cloud computing.

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" in Feb 2022 IJRPR ISS N 2582-7421*

[2] *S. Nepal, S. Chen, J. Yao, and D. Thilakanathan, "DIaaS: Data Integrity as a Service in the Cloud," in 2011 IEEE 4th International Conference on Cloud Computing, Jul. 2011, pp. 308–315, doi: 10.1109/CLOUD.2011.35.*

[3] *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*

[4] *Mailewa, Akalanka, and Jayantha Herath. "Operating systems learning environment with VMware." In The Midwest Instruction and Computing Symposium. Retrieved from http://www. micsymposium. org/mics2014/ProceedingsMICS_2014/mics2014_submission_14. pdf. 2014*

[5] *M. F. Al-Jaberi and A. Zainal, "Data integrity and privacy model in cloud computing," in 2014 International Symposium on Biometrics and Security Technologies (ISBAST), Aug. 2014, pp. 280–284, doi: 10.1109/ISBAST.2014.7013135.*

[6] *Y. Chen, L. Li, and Z. Chen, "An Approach to Verifying Data Integrity for Cloud Storage," in 2017 13th International Conference on Computational Intelligence and Security (CIS), Dec. 2017, pp. 582–585, doi: 10.1109/CIS.2017.00135.*

[7] *K. N. Sevis and E. Seker, "Survey on Data Integrity in Cloud," in 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), Jun. 2016, pp. 167–171, doi: 10.1109/CSCloud.2016.35.*

[8] *C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 42–57, Jan. 2013, doi: 10.1016/j.jnca.2012.05.003.*

[9] *Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Dynamic & portable vulnerability assessment testbed with Linux containers to ensure the security of MongoDB in Singularity LXCs." In Companion Conference of the Supercomputing-2018 (SC18). 2018.*

[10] *Akintaro, Mojolaoluwa, Teddy Pare, and Akalanka Mailewa Dissanayaka. "Darknet and black-market activities against the cybersecurity: a survey." In The Midwest Instruction and Computing Symposium. (MICS), North Dakota State University, Fargo, ND. 2019.*

[11] *N. vurukonda and B. T. Rao, "A Study on Data Storage Security Issues in Cloud Computing," Procedia Comput. Sci., vol. 92, pp. 128–135, Jan. 2016, doi: 10.1016/j.procs.2016.07.335*

[12] *Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Security assurance of MongoDB in singularity LXCs: an elastic and convenient testbed using Linux containers to explore vulnerabilities." Cluster Computing 23, no. 3 (2020): 1955-1971*

[13] *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, doi: 10.1007/s12652-020-01747z.*

[14] *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.*

[15]*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*

[16]*Shetty, Roshan Ramprasad, Akalanka Mailewa Dissanayaka, Susan Mengel, Lisa Gittner, Ravi Vadapalli, and Hafiz Khan. "Secure NoSQL based medical data processing and retrieval: the exposome project." In Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 99-105. 2017.*

[17]*Mailewa Dissanayaka, Akalanka, Roshan Ramprasad Shetty, Samip Kothari, Susan Mengel, Lisa Gittner, and Ravi Vadapalli. "A review of MongoDB and singularity container security in regards to hipaa regulations." In Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 91-97. 2017.*

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

[19]*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, doi: 10.1016/j.procs.2015.04.171.*

[20] *M. S. Giri, B. Gaur, and D. Tomar, A Survey on Data Integrity Techniques in Cloud Computing.*

[21]*Mailewa, Akalanka, Jayantha Herath, and SusanthaHerath. "A survey of effective and efficient software testing." In The Midwest Instruction and Computing Symposium. (MICS), Grand Forks, ND. 2015*