IJMRSET

e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 8, August 2023

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.54

6381 907 438 6381 907 438 ijmrset@gmail.com www.ijmrset.com

Analyzing Data Integrity Issues on Cloud

Banazir Imtiyaz, Dr. Saurabh and Mr. Vivek Kumar

PG Student, Department of Computer Science and Engineering, Swami Vivekanand Institute of Engineering and Technology, I.K Gujral Punjab Technical University, Kapurthala Jalandhar, India

Dean, Department of Computer Science and Engineering, Swami Vivekanand Institute of Engineering and Technology, I.K Gujral Punjab Technical University, Kapurthala Jalandhar, India

Department of Computer Science and Engineering, Swami Vivekanand Institute of Engineering and Technology, I.K Gujral Punjab Technical University, Kapurthala Jalandhar, India

ABSTRACT: “Cloud Computing”- The current buzz of the world. Everything is being managed on internet. Organizations shifting all the sensitive and critical information to cloud for the storage and maintenance purposes makes everything available at finger tips or click away. There is no need to spend a hefty amount on storage, maintenance, security, protection, man power for the data. Protecting data loss from mishandling or mismanagement all are some of the very basic advantages or benefits that Cloud ensures thereby drawing attention towards cloud.

However, as they say “All that Glitters is not Gold”. Even though the cost-effective maintenance and flexibility in terms of storage and availability ensured by the Cloud, it exposes Data, the most vital asset of the organization to various threats.

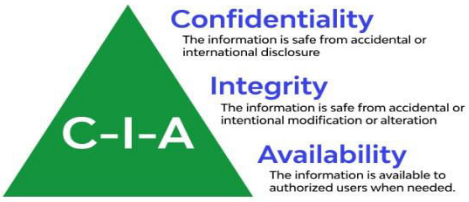
Moreover, till date there is nothing absolute in terms of security. Attack on data can completely expose organization to serious damages which are hard to track and then protected. Cloud does lack in design in terms of infrastructure, access control and security. Once the Data is shifted to cloud, the very basic step user loses control over information.

Even though there are some basic schemes, techniques or proposals that might prevent of track certain attacks, there is still a lot that needs to be done in this field. Thus, it encompasses various opportunities for the researchers to develop a proper security mechanism protecting data integrity, authenticity and confidentiality.

I. INTRODUCTION

In current times everything we see is available on Cloud. Gone are the days of carrying and storing long ledgers, storage devices. It seems to be a concept of early man’s time. Nowadays, everything is available on a single click. Data, resources are the assets to the firm or an organization and threat to this could prove to be a disastrous to the organization. In current times we might have number of concerns related to the maintenance, storage, utilization, data warehousing of these assets. However, the biggest one still remains the security.

Anything available on Cloud or in layman terms available on internet is prone to threats. These threats on data could broadly be classified on the basis of CIA triad: Confidentiality, Integrity and Availability. Whatsoever the protocols, policies and whosoever the vendor be the main criteria is maintaining CIA of data.


Confidentiality
The information is safe from accidental or international disclosure
Integrity
The information is safe from accidental or intentional modification or alteration
C-I-A
Availability
The information is available to authorized users when needed.

Cloud Computing Security also known as Cloud Security collectively refers to the measures taken to safeguard the resources available on cloud. These resources could be data, infrastructure or applications. These measures not only ensure authentication and access control but also privacy protection. Cloud security follows the concept of responsibility sharing where the Cloud provider looks after the hardware and the software part and the client is supposed to maintain the privacy of Data.

Data breaches mostly across the cloud platforms in no new problem and that is the reason which led to the concept of cloud security. Hence to assure the client that their sensitive information is no more at risk. Proper auditing process provided a framework for top cloud service providers to aim at five key areas of Cloud security:

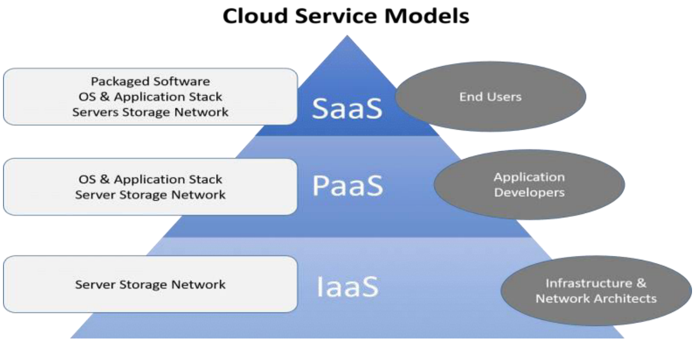
- IAM (Identity and Access Management)
- Securing Data in Cloud
- Securing the Platform (Operating system)
- Protecting the Network layer
- Managing Security Monitoring, Alerting, Audit Trial, and Incident Response.

Cloud Computing and Data Integrity:

In a very small span of time concept of cloud computing by mere transferring the data premises has changed the whole dynamics of the working procedures followed at organizations. Cloud computing not just provides cost effective and flexible IT services delivered but also provides servers, storage, networking, database, bandwidth etc over internet.

Many organizations cannot afford large storages or management of private data that efficiently but cloud storage made it possible due to its flexible service model. These storage models are:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)



Undoubtedly, cloud computing ensures numerous benefits but it does pose to some serious technical and security hurdles such as confidentiality, data integrity and privacy. Once the data is stored by the organization on the cloud platform it loses its control over the confidentiality of data. Now, it remains the job of the cloud service provider (CSP) that the data remains authentic, unaltered and uncompromised. Even though the CSP is bound by SLA (Service Level Agreement) to ensure the security of the data but it is never 100%.

Suppose data altered accidentally or by some malicious activity could turn out to be a nightmare for the user and the CSP. Or suppose in case of shared multi tenancy, there are always vulnerabilities such as data leakage, backup failure that could be taken advantage of.

In a survey conducted by International Data Corporation (IDC) the biggest challenge is the Cloud Security. On such platforms it is a must to not just address the data integrity verification but also privacy preserving issues.

Cloud Data Storage - Challenges and Issues:

As from Clients or user's view the biggest disadvantage of such platform is that once the data is transferred to cloud platform the control to the confidentiality of the data is compromised. It now remains in the hands of the CSP who can manipulate, destroy, alter, copy the data as per convenience without user having any knowledge of same. Although the cloud platform is advantageous in terms of flexibility, storage, cost-effective. However, it comes with a tradeoff and here the tradeoff is with the data integrity threats. Multi tenancy architecture lets multiple users access same resource and hence exposes data to various threats.

The main issues with cloud storage can broadly be summarized as:

- Data Integrity and Privacy
- Data Backup
- Data Recovery and Vulnerability
- Improper Media sanitization

Improper media sanitization of the storage device (disk) can lead to the risk of storing of data on the multi-tenant cloud.

Unintentional or Intentional data backups can lead to unavailability of data which violates the data availability policy which says data should be available 24*7.

Hence the security mechanism that is employed must ensure data prevention from tampering and unauthorized access on cloud platform.

These threats cover all the aspects of data security issues in Cloud Computing internal as well as external aspects. This violates:

1. Data Integrity
2. Data Privacy and Confidentiality
3. Location of Data
4. Availability of Data
5. Data Authentication
6. Data Storage, Backups and Recovery

Like any other coin, Cloud Computing too has a share of advantages and disadvantages. Although it enables tremendous amounts of services and flexibilities, it does have an ugly side. These advantages make data vulnerable to attacks. These advantages and the challenges of cloud computing may be enlisted as:

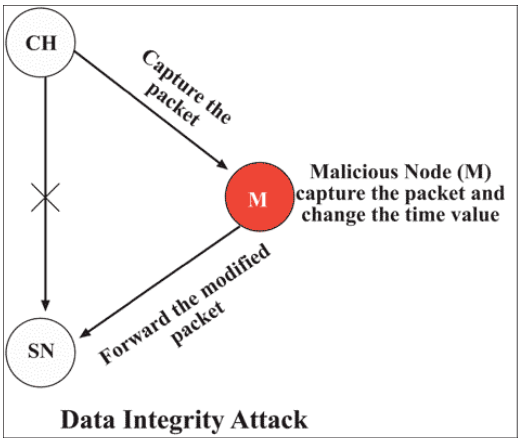
- Cost Effective
- Time and Flexibility
- Compatibility
- Backup and Restore Data
- Internet Connectivity
- Data Integrity
- Data Confidentiality and Privacy
- Data Location

Data Integrity Attacks:

Maintaining Data Integrity in simpler terms may be defined as the information that cannot be altered or manipulated by any third person who does not have permission to access same. Data/ information is the most valuable asset of an organization. It consists of all the critical information be it fundamentals, strategies, resources, projects etc that an organization is based upon.

The attack on the integrity would mean corrupting the data. Such type of attack is always intentional. There are number of ways in which these attacks are carried out but the most common one is through malwares. These malwares tend to delete or modify the existing data thereby leading to data discrepancies. These types of attacks are believed to be the emerging potential security threats yet difficult to be traced.

One simple illustration for Data Integrity attack can be explained as a source forwarding data to sink. In a normal case transfer is supposed to be direct but due to malware this data packet is received by Malicious node and then the data is altered/modified and then forwarded to destination without source and destination node being aware of any such activity in between.

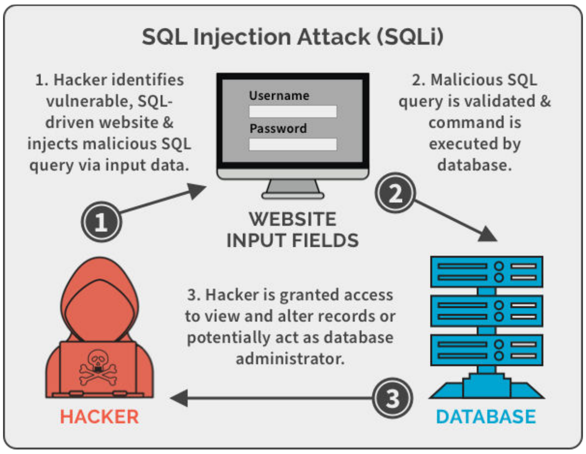

CH
Capture the packet
M
Malicious Node (M) capture the packet and change the time value
Forward the modified packet
SN
Data Integrity Attack

There are various attacks that could target data integrity on available on cloud. Some of these can be enlisted as:

- **Unauthorized Access:**
  In this situation, user loses access to the files and the data starts modifying uncontrollably. It could be internal or external. It is one of the serious attacks and is followed by data breach.
- **Data Lock-in:**
  How the data is stored on cloud is not based on some rules or conditions. It is upto Cloud Service Provider. Mostly it is scatttered over the server. Hence moving between different service providers will lead to loss of data.

- **Security against Internal and External Attacks:**
  Not being careful can prove to be hazardous. Suppose a person/user doesn’t log off properly from system. The attacker might conduct some malicious activity that can expose data to internal or external attack.

- **SQL injection:**
  This common web based attack requires a web application and a database. A query is sent to the database and the relevant data is returned. In this attack, a malicious string is sent to the database as a query resulting in modification/alteration of the system.


SQL Injection Attack (SQLi)
1. Hacker identifies vulnerable, SQL-driven website & injects malicious SQL query via input data.
Username
Password
2. Malicious SQL query is validated & command is executed by database.
1
2
WEBSITE INPUT FIELDS
3. Hacker is granted access to view and alter records or potentially act as database administrator.
3
HACKER
DATABASE

❖ **Man in the Middle attack:**

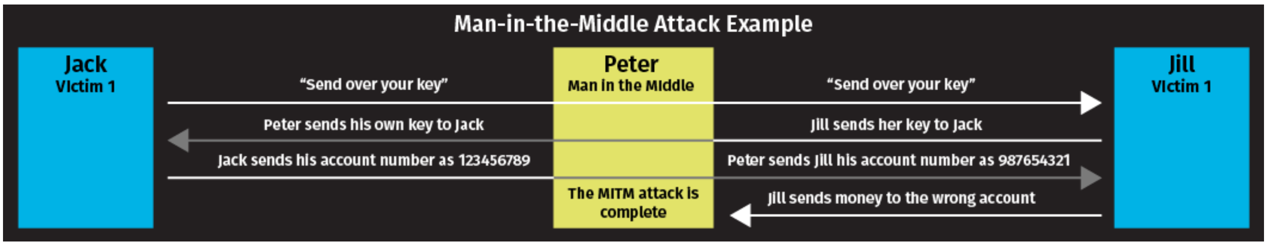
While the data packets are tranferred, a proper encryption is must in order to prevent eavesdropping from any sensitive information. This Man in the Middle attack can be carried out in number of ways:

□ Wrapping Attack: Attacker tries to get access to credentials by copying them.

□ Flooding Attack: Channel is flooded with requests so that the focus is shifted from main problem and results in system crash

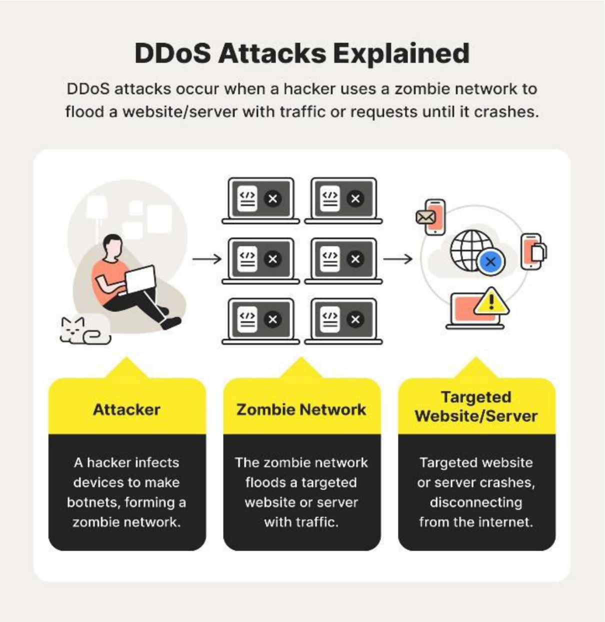
□ Internet Attack: This is the attack on transparency. It is carried out on LAN/ WAN so the systems that are connected over this network are equally affected.

□ SSL: Also known as Secure socket Layer attack is an attack on defense layer so to steal the information.


Man-in-the-Middle Attack Example
Jack
Victim 1
Peter
Man in the Middle
Jill
Victim 1
"Send over your key"
"Send over your key"
Peter sends his own key to Jack
Jill sends her key to Jack
Jack sends his account number as 123456789
Peter sends Jill his account number as 987654321
The MITM attack is complete
Jill sends money to the wrong account

❖ **DDOS attack:**

It is also known as Distributed Denial of Service is an attack where the system is flooded with requests. It is a threat to resource centre. This is the most deadliest attack on internet and cannot be solved completely due to inefficient resources on client side. However, few techniques can reduce the chances of attack.



DDoS Attacks Explained

DDoS attacks occur when a hacker uses a zombie network to flood a website/server with traffic or requests until it crashes.

A hacker infects devices to make botnets, forming a zombie network.

The zombie network floods a targeted website or server with traffic.

Targeted website or server crashes, disconnecting from the internet.

- **Authentication attacks:**
  It is a type of social engineering attacks where the attacker tries to gain access to information without having correct credentials. These attacks are classisfied as:
  - □ Replay attack: In this type of authentication attack, Attacker observes the data traffic and then mimics the original sender. However, such attacks can be prevented by using timestamps and sequence numbers on data packets.
  - □ Brute Force attack: Brute force or dictionary attack are the basic attacks where a person tries the combination of passwords to gain access. These could be birthdates, anniversary dates, nicknames, combination of name and dates etc. Longer the password hard is to crack.
  - □ Phising attack: It is a brute force mechanism where the attacker tries to gain access by trying various code combinations to gain access.

- **Tag Frogery attack:**
  This kind of attack has become the most common one these days. This attack is carried out via some barcodes shared with the consumers and once it is scanned it gives attacker access to the sensitive and personal data of the user.

- **Timeliness attack:**
  Every project provided to a company or a firm has a proper timeline to complete the project. If the project is completed on time it is submitted to the authority. However, if there is an attack on the system, it fails to accept the project submission.

- **Roll Back attack:** This kind of attack is mostly possible during the updation of infrastructure. If the software is updated and still the CSP provides older version, it leads to data loss and crashes. Roll back attack is also possible if the old user's data is not removed efficiently.

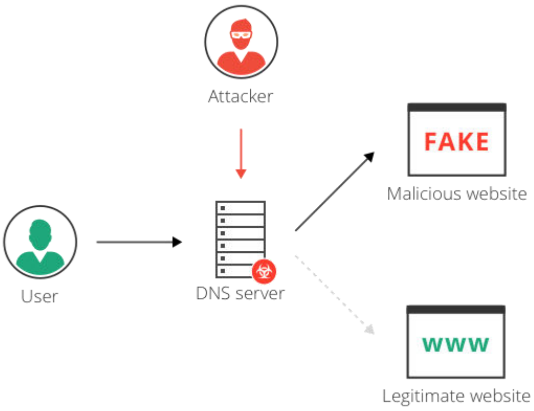
- **Byzantine attack:**
  This attack is distributed over the Cloud. It stops and crashes the system. Mostly such attack is carried out when the request is not passed properly through the system.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 8, August 2023 |

| DOI:10.15680/IJMRSET.2023.0608014 |

- **DNS attack:**
  It is also known as Domain Name System Attack. As DNS converts Domain names to IP addresses which are more like numbers. These are fetched to servers as query and the website is loaded. When the malicious software is used for same the process is carried out in similar fashion. While the websites are loaded on the client side, attacker gets access to the sensitive information available on user's end.



- **Sniffer attack:**
  Sniffer attack is yet another type of attack to gain confidential, personal information from user's end. Once the user receives some spam messages. The single click on link activates the link and lets either attacker to take control over device or gives access to personal information mostly not encrypted.

Surveys on Challenges and Privacy Aspects of Cloud Computing:

In a survey various challenges and privacy aspects of cloud computing and possible solutions were studied, three main areas were highlighted viz:

□ **Managers and users' trust on cloud storage**

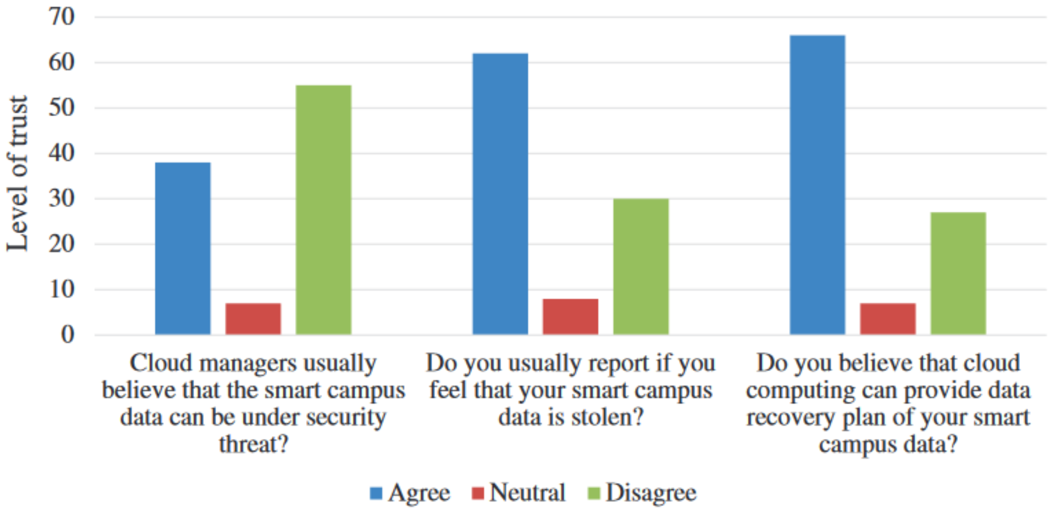


Figure 1: Managers and users' level of trust in cloud storage

- **Security aspects of cloud storage**

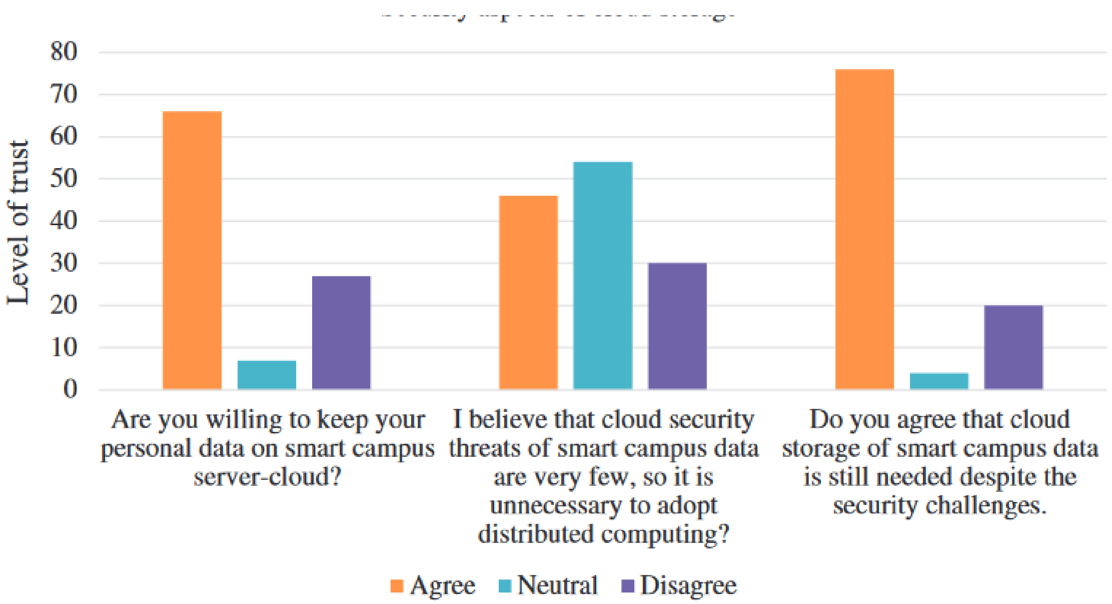


Figure 2: Security aspects of cloud storage

- **Scalability aspects of cloud servers**

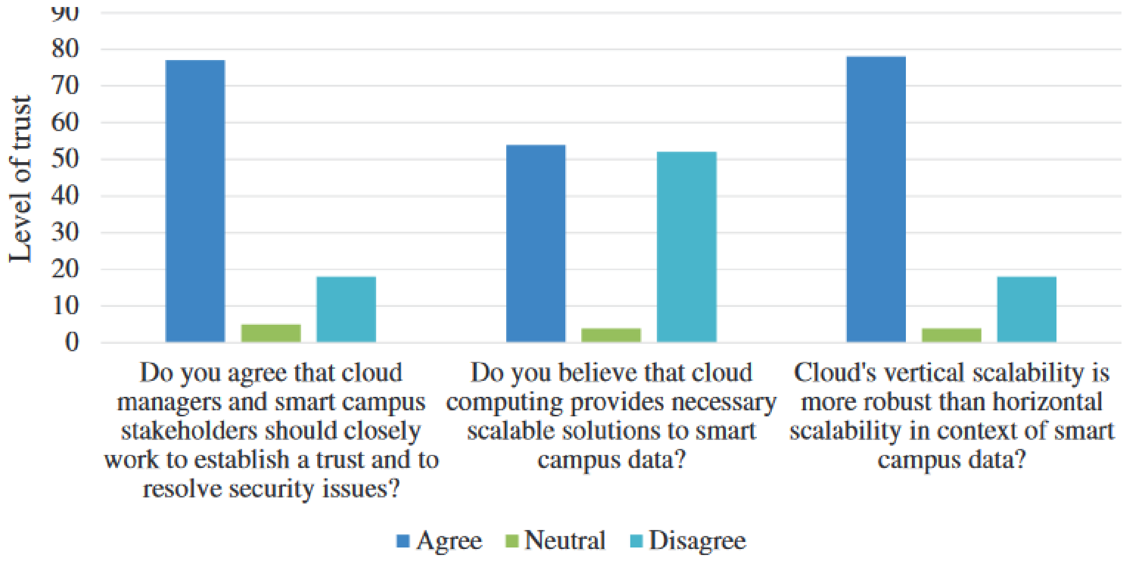


Figure 3: Scalability aspects of cloud storage

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 8, August 2023 |

| DOI:10.15680/IJMRSET.2023.0608014 |

Prevention of Data Integrity Attacks on Cloud:

Cloud is exposed to numerous threats and vulnerabilities, which can exploit the data integrity of data stored. An attacker can be external or internal. It can be anyone from owner having access to data to the malicious user or untrusted third party to the Cloud Service Provider.

From time to time, security has been the prime goal and uncompromised aspect and hence several mechanism, techniques and schemes have been put forward to protect and prevent the data from possession and maintaining the data integrity on Cloud.

From the research conducted time and again, there are various schemes to protect the integrity of data online. Some of the most common and effective proposals can be listed as:

1. **Mitigation of Tag Forgery and Data Leakage Attack:**

   It is impossible for a user to trace the attack if it is carried out be the Cloud Service Provider itself. Cooperative Provable Data Possession (CPCP) was thus put forward to help users by providing strong security and transparency of data. It is based on Homomorphic Verifiable Response and Hash Index Hierarchy and was put forward by Yun Zhu et.al. It prevents CSP from using fraudulent tags and cheating clients. Client itself creates a challenge tag and forwards to CSP later on. Trusted Third Party helps client to validate data the integrity of data.

2. **Mitigation of Replay and Timeliness Attack:**

   As the name suggests, this technique was put forward as a protection to integrity from timeliness and replay attack. It uses Non-Repudiation (NR) protocol proposed by Jun Feng et.al.
   It allows client to end or abort the execution when there is no response from other party. It is based on encryption which allows sender to share the public key with receiver and shares a sequence of random number that acts as a signature which makes it difficult for attacker to decrypt the message. For more secure purpose timestamps are also added which prevents timeliness attack.

3. **Mitigation of Roll-Back Attack:**

   This scheme is applied to prevent roll back attack by implementation of Merkle Hash Tree Method. In the process followed here, with the data getting updated data block tag and respective Counter value gets updated. So, if in case there is attack to data integrity the Counter value keeps changing hence lets user see if the data is compromised.

4. **Mitigation of Byzantine Failure and Malicious Data Attack:**

   This technique is based on HAIL Protocol (High Availability and Integrity Layer) put forward by Browers et.al. It aims at keeping stored data intact and ensuring secure retrieval from servers. It implements Erasure correcting code for file distribution to make data available even if servers act up.

5. **Protecting Data Integrity Using Encryption:**

   The safest way to secure data from any attack is encrypting it. It is considered as an optimal solution mostly when data is available on cloud. Before shifting data premise to cloud it must be encrypted and then stored on cloud. For better evaluation the hash values for the data must be calculated and then checked if they are modified. Thereby tracing and preventing attack on Data integrity.

6. **Provable Data Possession (PDP) Technique:**

   This technique is based on challenge response protocol that verifies the data integrity stored on cloud. In this process, encryption techniques are used. Before, availing data on cloud the files are loaded with meta data.

This meta data on files is stored first on cloud and the data integrity is verified. Then the client deletes the copy and checks for the server's possession of data copy using challenge response protocol. It is based on two stages:

- Set-up Stage
- Challenge Stage

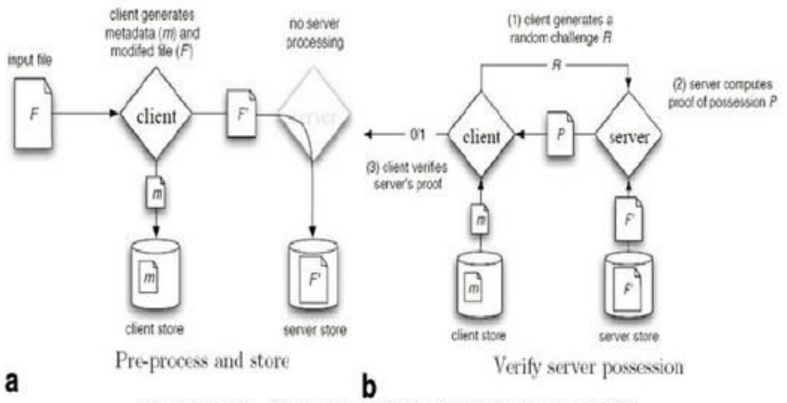
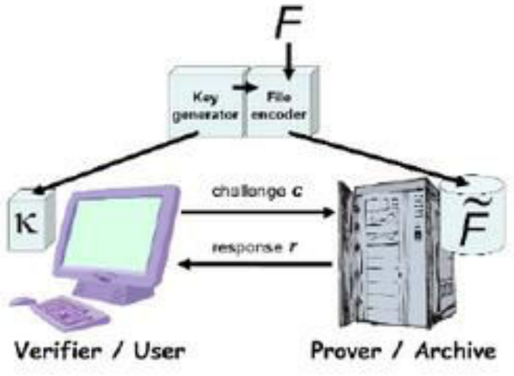

input file
F
client generates metadata (m) and modifed file (F')
client
F'
no server processing
server
m
client store
server store
Pre-process and store
a
(1) client generates a random challenge R
R
(2) server computes proof of possession P
0/1
(3) client verifies server's proof
client
P
server
m
F'
client store
server store
Verify server possession
b

Figure 7. PDP – Setup Stage and Challenge Stage Process [32]

7. **Proofs of Retrievability (POR) Technique:**

Data stored on Cloud can be validated remotely. This technique is based on same using the authentication key. Original copies of file locally are not stored and the retrieval is not required from Cloud Service provider. These authentication keys are used to verify later on the data integrity without retrieving the file from CSP.



POR-Data Verification Process

II. CONCLUSION

This article explains how cloud provides numerous advantages along with the various challenges. It explains how the advantageous nature of Cloud in terms of cost effective and flexiblity exposes the Data to the most vulnerablities. It leads data to risk in terms of integrity, authenticity and confidentiality. Many of these attacks are prevented while most of the attacks are difficult to be traced and prevented.

Indeed, cloud storage is cheaper, faster, flexible, easily maintainable it has its mere share of challenges as well. Major concern still remains the confidentiality and data integrity. Few mechanism did mitigate the risk to prevent data from attack and protect data from loss.

However in a broader perspective cloud needs to designed in a better manner where the user and CSP both are ensured Data Integrity. It remains a wide open area of challenges and opportunities for research work. Security needs to ensured to the maximum possible limit so that the assets are not just shifted for the storage purpose on cloud but for the privacy purpose as well.

REFERENCES

[1] S. Nepal, S. Chen, J. Yao, and D. Thilakanathan, “DIaaS: Data Integrity as a Service in the Cloud,” in 2011 IEEE 4th Internat ional Conference on
Cloud Computing, Jul. 2011, pp. 308–315, doi: 10.1109/CLOUD.2011.35.
[2] 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.
[3] 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.
[4] “Types of Cloud Services. Cloud computing has three most common… | by IDM | Medium.” https://medium.com/@IDMdatasecurity/types-of-cloud-
services-b54e5b574f6 (accessed Feb. 05, 2021).
[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.
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 blackmarket activities against the cybersecurity: a survey."
In The Midwest Instruction and Computing Symposium (MICS), North Dakota State University, Fargo, ND. 2019.

BIOGRAPHY

Banazir Imtiyaz is currently a PG student at SVIET (I.K GUJRAL PUNJAB TECHNICAL UNIVERSITY, KAPURTHALA JALANDHAR) and working with one of the top Cloud Service Providers across globe. She pursued her B.Tech in Computer Science and Engineering from one of the renowned University, Islamic University of Science and Technology Awantipora, J&K (India) in 2020. Her research area mostly focuses on Data on cloud and Cloud Security.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor
7.54

ISSN
INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com