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

Srushti Pravin Watekar¹, Prof. Neha Mittal ²

¹Student, Department of Master of Computer Application, ²Assistant 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, 2022

Abstract- Cloud Computing is a range of services delivered over the internet or ‘the cloud’. In recent years, Cloud Computing has become the fastest emerging technology. Because of its low cost and pay-as-you-go manner, many organizations 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 the cloud environment is a serious concern. In this paper, I have surveyed previous studies which identify issues related to cloud data storage security like unavailability, data breach of cloud server data and data theft.

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

1- INTRODUCTION

Cloud computing is a range of services 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 new technology today is so popular that academic researchers and industries take interest in it [4]. For many organizations, running a private data center or having large secondary storage is over budget. Cloud storage is the best option for these organizations due to its flexible service model [5]. As shown in Figure 1, there are three cloud storage 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 organization stores 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 nightmare for users. For example,
information can be manipulated intentionally or accidentally through 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 previous research 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 have no control over the data. Instead, cloud service providers (CSPs) have full control over information stored in cloud data centers. CSP may modify, 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 resource management, 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 becomes unusable due to accidental or intentional data backup failures. Security mechanisms could be used to forestall data falsification and unauthorized access to cloud environments [12].

Some organizations today 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 costs a lot in terms of security, maintenance, space, employment, etc. After years of research, IT companies found a solution that could store company data at a lower cost, can be available and accessed by anyone over a network using cloud computing [13,8]. Some benefits of cloud computing are discussed below:

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 the Internet. This could force people around the world to work on the same project at the same time. No need to waste time on management and maintenance.
3. Cost Effective:
   Cloud model reduces the maintenance cost, security cost, software license cost, personal training 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 easily restored and backed up from the cloud.

In addition, to the benefits mentioned above, the cloud computing also has some drawbacks, which are discussed below:

1. Internet Connectivity:
   Even if the cloud service provider provides 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 not known, and these details are not transparent to the 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 client safe. However, when data is stored on an external server, the main concern of the 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 organization 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 sends it to the database, and when the query is executed on the database, the corresponding data is returned to the
application. This is what usually 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 should not do [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 should not switch from one provider to another as this person can lead to loss of user data and cause problems on 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 without logging out, the risk of an attack increases. Someone else can open the system and perform malicious actions that can expose internal and external attacks [14]. User data is not secure on the CSP side. In addition, this always-on data encryption protects data privacy [3].

5. **Authentication Attacks**: Following are few authentication attacks:

   - **Phishing Attack**: It is about how an attacker finds every combination of code and more the complex code, the longer it takes an attacker to learn it [18].
   - **Replay Attack**: It occurs when unknown person views the data stream and then sends the communication data to this location as the original sender. Timestamps and sequence numbers must be implemented to prevent this attack [16].
   - **Brute Force Attack or Dictionary Attack**: It is a basic attack in which attacker attempts any combination of passwords to again access to user data. Lengthy passwords take longer for the user to crack to guess the correct password [17].

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

Attackers can be anything from owners to malicious users or untrusted third parties in the CSP. Several mechanisms 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 solution for protecting data in the cloud. Data must be encrypted before being stored on servers, which renders the data unusable. The hash value of data must also be computed before being stored on servers. This ensures that the data has not 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 service providers by verifying data integrity via trusted third-party (TPP) [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 some other authors in various research articles and meetings as solutions to these attacks as described in previous sections. To sum up the summary some problem typeshavene an unavailable solution to solve like: Data Leakage can be solved by UserRank method, XML attack can be solved by Filter based Approach, Data Isolation Failure can be solved by multi-tenant data isolation or Sharing middleware scheme. Spoofing can be solved by Strong Authentication, SQL Injection Attacks can be solved by Parameterized Statements, Sniffer Attacks can be solved by SSH or IP see and so on.

**VI-COnCLUSION**
In this article, we have discussed some of the attack stats that cloud service providers (CSPs) can detect. A short note on Cloud Computing and Data Integrity has been discussed. This article is discussed in relation to related work by other authors. A lot of organizations 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. Several mitigation techniques have 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


