Check for updates

International Journal of Advanced Research and Interdisciplinary Scientific Endeavours, Vol. 2(5), 2025
DOI: 10.61359/11.2206-2528

Ensuring Data Integrity in Cloud Computing: A Review of Threats and Protection Strategies

Mrs. M. Sindhu [*1], Mrs. R. Divya [†2]

Email Correspondence*: conferencesrrcet@gmail.com

[1]Department of Computer Science and Engineering, Sri Raaja Raajan College of Engineering and Technology, Karaikudi, Tamil Nadu, India.

[2]Department of Computer Science and Engineering, Moogambikai College of Engineering, Trichy, Tamil Nadu, India.

Abstract:

Cloud computing has experienced significant growth in recent years, with many organizations transitioning from traditional computing models to cloud-based solutions due to their cost-effectiveness and scalability. While Cloud Service Providers (CSPs) assure data security and integrity, various challenges still persist, particularly concerning data integrity. In cloud environments, threats such as data theft, unavailability, and breaches pose significant risks. This paper presents a comprehensive review of existing studies on cloud data storage security, highlighting key integrity threats and vulnerabilities. Additionally, we provide an in-depth analysis of various data integrity attacks and explore effective mitigation techniques to enhance cloud security.

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

1. Introduction

As technology has developed over the past several years, Cloud Computing has completely changed how businesses operate by transferring their workload off-premises. Databases, bandwidth, software, servers, storage, and networking resources can be distributed across the internet in a flexible and cost-effective manner thanks to Cloud Computing. On-demand internet access to shared configurable computing resources (such as networks, servers, storage, applications, and services) is provided via the idea of "Cloud Computing," which may be swiftly provided and released with no administrative effort or service provider contact. This new technology is quite popular nowadays, and it has increased the curiosity of academic researchers and other industries. Many businesses cannot afford to run their own data centre or have huge amounts of secondary storage. Because of its customizable service model, cloud storage is indeed the greatest alternative for such enterprises. As indicated in Figure 1, there are three cloud storage models available, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

[*]1Department of Computer Science and Engineering, Sri Raaja Raajan College of Engineering and Technology, Karaikudi, Tamil Nadu, India.
[†]Department of Computer Science and Engineering, Moogambikai College of Engineering, Trichy, Tamil Nadu, India.

Article Timeline: Received: May 16, 2025; Revised: May 29, 2025; Published: May 30, 2025

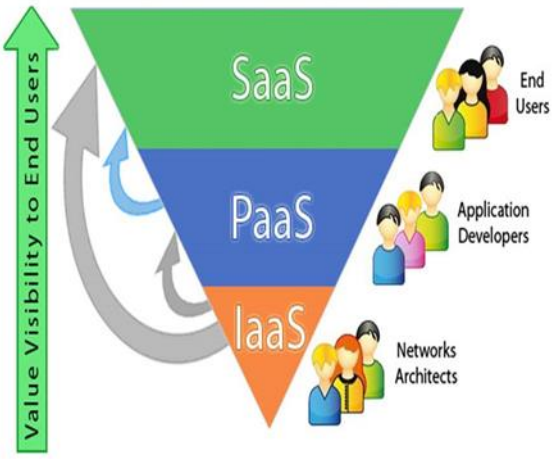

Fig 1- Cloud Service Models

Despite the numerous benefits of cloud computing, it comes with several technical and security challenges, such as issues related to data integrity, confidentiality, and privacy. Once a user or organization stores their data in cloud storage, they lose direct control over their confidential information. Cloud Service Providers (CSPs) must use various mechanisms to protect their customers' data from modification and corruption. Although CSPs are responsible for ensuring information security and are bound by service level agreements (SLAs), they cannot guarantee 100% data integrity. Many data integrity issues can confuse cloud providers and become a nightmare for users. For example, data can be manipulated intentionally or accidentally through malicious actions. Vulnerabilities in common multi-user models can be exploited, leading to damage to other users' data, data backup failures, breaches, and more. According to an International Data Corporation (IDC) survey, security is the number one concern in cloud computing. Addressing privacy issues and ensuring data integrity in the cloud is urgent. In this paper, we will discuss the possible data integrity attacks in cloud computing and the mechanisms used to detect and prevent them in detail.

Figure 2. Importance of Data Integrity

2. Cloud Data Storage Challenge and Issues

As cloud computing continues to evolve, cloud data storage remains a critical component of modern IT infrastructure. While cloud storage offers scalability, cost efficiency, and accessibility, several challenges and security risks persist in 2024. Emerging technologies, evolving cyber threats, and regulatory changes have further intensified concerns surrounding cloud data security and integrity. Below are the key challenges and issues faced in cloud data storage in 2024.

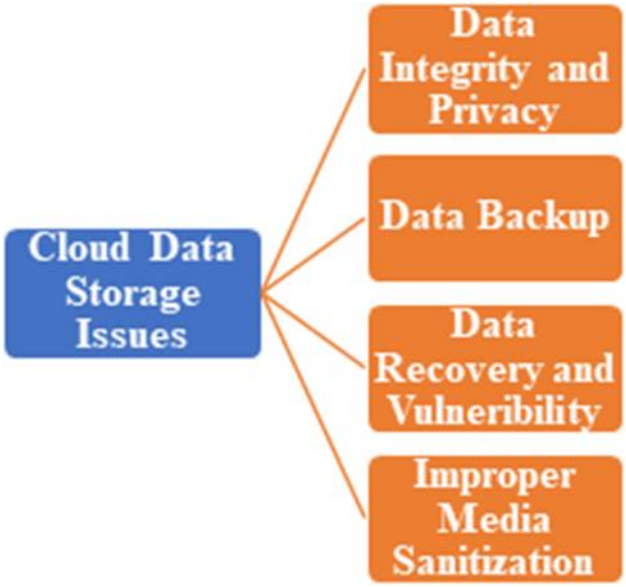

Figure 3. Cloud Data Storage Issues

Cost Effective

By using Pay-as you go Cloud model reduces the maintenance cost, personal training cost, security cost, operational cost, and software licensing cost.

Time and Flexibility

Using cloud storage, you can easily access data from anywhere any time through the internet. This can make people work on the same project at the same time globally. No time needs to be spent in management and maintenance.

Compatibility

Cloud makes it feasible to compatibility documents and between different operating systems.

Back-up and Restore Data

It is easy to restore and backup from the cloud once the information is stored in the cloud. Like the benefits mentioned above, cloud computing has also several disadvantages, discussed below:

Internet Connectivity

Even if the cloud service provider is offering the best quality cloud service to its customer, if the internet connection is down, one cannot access the data until it is back on. The longer the internet connection is lost, the more cost the customer must face.

Data Location

In cloud computing the cloud server's Physical location, where the data is stored is unknown. These details are not transparent to the customer. The servers might be in different countries.

Data Integrity & Trust Issues

Ensuring data integrity remains a top priority in cloud environments. Unauthorized modifications, data corruption, and malicious alterations can occur due to cyberattacks, insider threats, or system failures. Ensuring end-to-end data integrity verification mechanisms, such as blockchain-based auditing, is crucial.

Advanced Ransomware & Malware Attacks

Ransomware attacks targeting cloud storage have become more sophisticated in 2024. Cybercriminals encrypt cloud-stored data and demand ransom for decryption keys. The use of AI-driven malware makes detection and mitigation even more challenging, requiring stronger cybersecurity measures like AI-based threat detection and zero-trust architectures.

Data Privacy & Confidentiality Concerns

With an increasing reliance on cloud storage, data privacy remains a significant concern. Organizations must protect sensitive data from unauthorized access by both external attackers and cloud providers themselves. Privacy-enhancing technologies (PETs) such as homomorphic encryption and confidential computing are gaining traction to address these concerns.

Quantum Computing Threats

The rise of quantum computing poses a potential threat to traditional encryption algorithms used in cloud storage. As quantum advancements continue, cloud providers and enterprises must transition to quantum-resistant encryption techniques, such as post-quantum cryptography, to secure stored data.

Compliance with Evolving Regulations

New data protection regulations and stricter compliance requirements have emerged worldwide, making regulatory compliance a growing challenge. Laws such as GDPR, CCPA, and newer cloud security mandates in various regions require organizations to ensure proper data governance, sovereignty, and transparency in cloud storage operations.

Multi-Tenancy & Data Isolation Risks

As cloud platforms host multiple tenants on shared infrastructure, security vulnerabilities in one tenant's environment can affect others. Poor isolation mechanisms could lead to data leakage or unauthorized access, necessitating improved containerization and stronger tenant isolation policies.

Data Availability & Downtime Risks

Despite high availability claims by cloud providers, outages due to software bugs, misconfigurations, and cyber incidents still pose risks. Organizations must implement redundancy strategies, multi-cloud deployments, and automated failover mechanisms to mitigate downtime and ensure business continuity.

Insider Threats & Misconfigurations

In 2024, insider threats remain a major security risk. Employees with privileged access may intentionally or accidentally expose sensitive data. Misconfigurations, such as improperly set access controls or exposed APIs, continue to be one of the leading causes of cloud data breaches.

Edge Computing & Distributed Storage Challenges

With the growing adoption of edge computing, data is increasingly stored across multiple decentralized locations. While this improves performance, it also introduces new security and management challenges, including data synchronization, encryption at the edge, and secure communication between edge nodes and central cloud storage.

AI & Machine Learning Security Risks

AI-driven cloud storage automation enhances efficiency but also introduces security risks. Adversarial AI attacks can manipulate machine learning models to exploit vulnerabilities in cloud storage systems. Ensuring the security of AI-driven storage management tools is essential.

3. Types of Data Integrity Attacks

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

Unauthorized Access

In this attack, users are denied access to their files or data, and the data may be altered without their knowledge or control. Such incidents can originate from both internal and external sources relative to the cloud service provider's security environment. This is considered one of the most severe types of attacks, often resulting in data breaches due to factors such as outdated hardware or the reuse of compromised drivers.

SQL Injection Attack

This is one of the most common and widely exploited data attacks. It typically targets web applications that generate SQL queries and send them to a database. When the query is executed, the corresponding data is returned to the application. In an SQL injection attack, a malicious string or payload is embedded in the request, leading the system to perform unintended actions that it should not be authorized to execute.

Figure 4. SQL injection attack process

Data Lock-in: There are no rules or conditions for data storage that depend on CSPs in the cloud. Typically, pieces of data are spread across servers and systems. Corporations 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.

1. 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. User data is not secure on the CSP side. In addition to this, always-on data encryption protects data privacy.

2. Authentication Attacks: The following are a few authentication attacks:

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

Man in the Middle Attack (MiMA)

The insufficient encryptions can make users vulnerable to man in the middle attack which is an indirect one. TLS a cryptographic protocol allows a client server application in order to prevent eavesdropping from any sensitive information that is happening on HTTPS which makes use of TLS. If a person accesses the unknown network and do his work in HTTPs, the attacker who is acting as a middleman, will then take advantage by grabbing all the sensitive data through HTTPS packets. Few variations of MiMA are as follows:

Wrapping Attack

The attacker tries to copy the credentials of the user by SOAP messages where it is set as a mediator between the server and the browser.

Flooding Attack

Here a continuous flow of requests has been passed through the servers where the employee will not be able to focus on the problem and sometimes this will lead to the system crash.

Internet Attack

This deals with the data theft which is carried out through the SOAP messages encryption. When the internet LAN/WAN gets attack all the systems which are connected to that LAN/WAN will be attacked. Here the transparency will be affected.

SSL (Secure Socket Layer) Attack

This is the defense tool which is kept between the server and the user where the attacker can easily rob the information, and it is categorized into various forms.

DDOS Attack

This causes huge damage to the resources and access to the data of the user. "When there is a flood of requests passed through the system and HTTP is facing a serious threat to the resource centers". This is the most serious attack on today's Internet cloud environment. This attack cannot be solved completely as there are no sufficient resources in the client server. But there are some mitigation techniques where the risk can be reduced.

Tag forgery Attack

This attack takes place if the untrusted seller who cheats on their customers by showing a wrong barcode. If the customer scans this one on their devices, there he gets to access all the sensitive data which leads to the possible risks of cheating and privacy leakage.

Timeliness Attack

When a project is given in a company, it does have a deadline/time limit. If the team is very active and completes the work before the deadline, will they be able to submit it to the manager? If this attack occurs, the system will not be able to submit the project to their manager before the deal line. This will lead to some problems.

Roll back Attack

This attack always takes place when the during the update process. If the system is updated with some new software's, still the provider provides the oldest software. This will lead to the data loss and crashes. Sometimes this will also lead to the loss of the company's reputation. Roll back also occurs without proper deleting of the user's old data and updating the system with the new version.

Byzantine Attack

In this attack takes place in the various parts of the cloud computing by stopping or crashing the systems. This will happen when the request is not passed through the system correctly.

Domain Name System (DNS) Attack

DNS will resolve the domain names to IP addresses which works as a phone number. It is a query response protocol. This attack happens when your system gets attacked with some malicious software, here is the explanation of that. When you type www.google.com in your search bar, this link is translated into an IP address and sends queries to a server. So, what every you give in the address bar, you will not be able to see the desired one instead of some other website opening. Whenever the unknow webpage opens, the attacker will be easily able to access the personal information used in the servers.

Sniffer Attacks

When a person clicks some SOAP messages or links on the browser, then this attack will happen. Once the clicked link is activated, the program will capture the flow of packets in the network and gets access to the personal data of the users like passwords, bank account details etc. which is not encrypted.

SolarWinds Data Manipulation

- **Description:** A sophisticated supply chain attack where hackers injected malicious code into the SolarWinds software update, affecting government agencies and enterprises worldwide.
- **Impact:** Data manipulation, unauthorized access, and espionage.
- **Solution:**
    - **Zero-Trust Security Model** – Verifying all access requests.
    - **Continuous Monitoring & Threat Intelligence** – Early detection of malicious activities.

- **Software Integrity Verification** – Code-signing and vulnerability assessments before deployment.

AI-Powered Data Poisoning

- **Description:** Attackers injected manipulated or biased data into **machine learning (ML) models**, leading to incorrect AI-driven decision-making.
- **Impact:** AI-generated errors in fraud detection, healthcare, and financial predictions.
- **Solution:**
  - **AI Anomaly Detection** – Identifying data inconsistencies before training.
  - **Adversarial Training** – Strengthening AI models against manipulation.
  - **Real-Time Data Validation** – Ensuring dataset integrity before processing.

Ransomware with Data Tampering

- **Description:** A new ransomware variant encrypted data **after modifying critical files**, making backups unreliable.
- **Impact:** Financial loss, data corruption, and operational downtime.
- **Solution:**
  - **Immutable Backups** – Ensuring stored backups cannot be altered.
  - **Blockchain for Data Integrity** – Using **distributed ledger technology** to verify unaltered records.
  - **Advanced Endpoint Security** – Detecting ransomware before execution.

Cloud Supply Chain Attack

- **Description:** Attackers exploited vulnerabilities in **third-party cloud providers**, allowing them to inject malicious data into cloud storage systems.
- **Impact:** Data corruption in multiple organizations using the same cloud provider.
- **Solution:**
  - **Zero-Trust Cloud Security** – Restricting access to only verified sources.
  - **Vendor Risk Assessment** – Regular audits of third-party cloud services.
  - **Multi-Factor Authentication (MFA)** – Preventing unauthorized access.

Quantum Cryptography Breach

- **Description:** With the rise of **quantum computing**, traditional encryption methods became vulnerable to attacks, allowing hackers to modify encrypted cloud data.
- **Impact:** Loss of confidentiality and data tampering at a massive scale.
- **Solution:**

- **Post-Quantum Cryptography** – Implementing quantum-resistant encryption algorithms.
- **Blockchain-Based Data Verification** – Ensuring data immutability.
- **AI-Powered Threat Detection** – Monitoring for unusual access patterns.

Key Characteristics of Data Integrity Attacks:

AI-Powered Manipulation – Attackers use artificial intelligence to automate data corruption and disguise tampering.
Quantum Cryptography Threats – Quantum computers can break traditional encryption, making stored data vulnerable.
Supply Chain Data Poisoning – Malicious actors compromise third-party cloud services to alter critical datasets.
Time-Delay Attacks – Subtle data modifications accumulate over time, making detection difficult.
Cross-Cloud Attacks – Targeting multi-cloud and hybrid cloud infrastructures to spread data corruption.

Prevention & Défense Strategies for 2025

- **Post-Quantum Cryptography** – Next-gen encryption resistant to quantum attacks.
- **Blockchain-Based Data Integrity** – Secure, tamper-proof cloud record-keeping.
- **Zero-Trust Security Model** – Strict verification of every data request.
- **AI-Driven Threat Detection** – Real-time anomaly detection to identify unauthorized data changes.
- **Immutable Cloud Backups** – Write-once, read-many (WORM) storages prevent post-attack corruption.

4. Mechanisms for Detecting & Preventing Data Integrity Attacks in Cloud Environments

Ensuring data integrity in cloud environments is crucial for protecting sensitive information from unauthorized modifications, corruption, and deletion. Various mechanisms have been developed to detect and prevent data integrity attacks in cloud computing. Below are some of the most effective methods:

Mitigation of Tag Forgery and Data Leakage Attack

If the CSP attempts to cheat the user by using fraudulent data tags, the user might now know and get victimized. To prevent this attack, there is a scheme proposed by Yun Zhu et.al known as Cooperative Provable Data Possession (CPCP) which is used in combination of two other techniques (Homomorphic Verifiable Response and Hash Index Hierarchy), which provides transparent verification of data and strong security. Before the customer forwards the information to the CSP, the customer creates a challenge tag and then forward it to Cloud Service Provider later. They Challenge the Cloud Service Provider by validating the integrity of data with the help of Trusted Third Party (TTP).

Mitigation of Replay and Timeliness Attack

To prevent the data integrity from replay and timeliness attack, Jun Feng et.al has proposed a Non-Repudiation (NR) protocol. By using this protocol, the user can abort an execution when the other party does not respond. The evidence from data Originator and the data Recipient are encrypted using the receiver public key by the sender. Then a sequence number and a random number is also added to the sender's signature, which is increased in each process to avoid the replay attack. Additionally, timestamps

are also added to this protocol, to prevent from timeliness attack, where the process ends after the time limit.

Mitigation of Roll-Back Attack

In this proposed scheme, the roll back attack in the cloud environment is protected by implementing Merkle Hash Tree Method. In this method the data block tag and its counter value are get updated, whenever a new data is updated. If an attacker wants to modify the data, the counter value will also change. Data integrity can be verified using this method.

Mitigation of Byzantine Failure and Malicious Data Attack

A cryptosystem HAIL (High Availability and Integrity Layer) Protocol is proposed by Browers el.al . This protocol ensures that user data is stored intact and retrievable securely from servers. To provide redundancies and make sure that the data is available if the server is misbehaving, Erasure correcting code is used for file distribution. This prevents the Byzantine attacks and malicious data attacks.

Protecting Data Integrity Using Encryption

Data encryption is considered a better solution to protect the data in the cloud environment. Data should be encrypted before storing it to the cloud server, this will make the data unusable. Hash value of the data should also be calculated before storing it to the cloud server. This will ensure that data has not been modified.

Provable Data Possession (PDP) Technique

PDP technique uses the challenge response protocol to verify the integrity of the data stored on the cloud server. In this technique, symmetric encryption, MAC, or any other encryption is used. The file is filled with meta data before storing or sending it to the cloud server. Once the file is sent to the Cloud Service Provider, the user still saves the metadata of the file to verify its integrity. The user then deletes the local copy of file. The user then verifies the proof of the server's possession of the file using challenge response protocol. It has two stages: Set-up Stage and Challenge Stage.

Proofs of Retrievability (POR) Technique

Proof of Retrievability (POR) technique is used to validate the data remotely, which is stored on the Cloud Service Provider, using the authentication key. In this method data is not needed to be retrieved from the CSP and user also does not store the original copy of the file locally. User stores his file to the CSP along with the authentication key. User can then verify the integrity of the data using that authentication key, without retrieving back the file from the CSP.

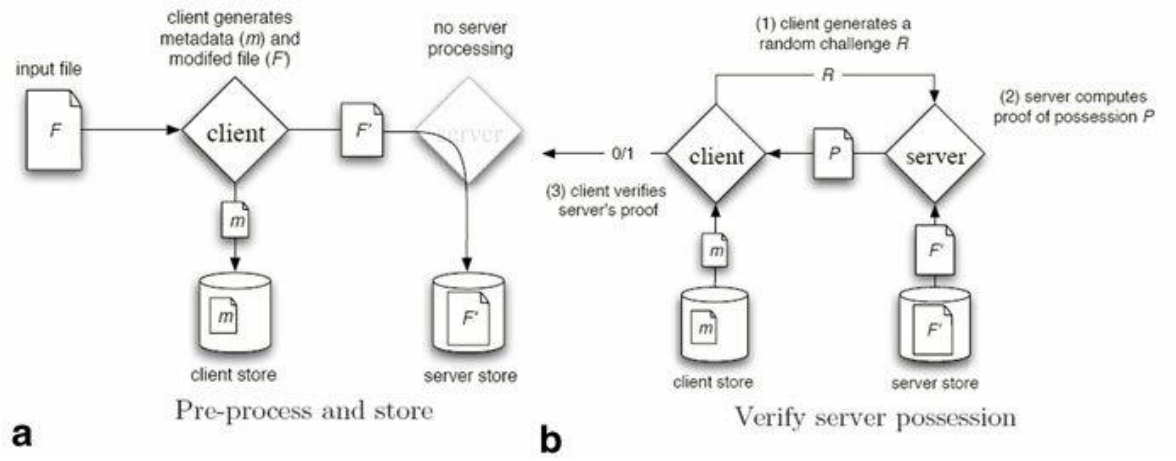

Figure 5. PDP – Setup Stage and Challenge Stage Process

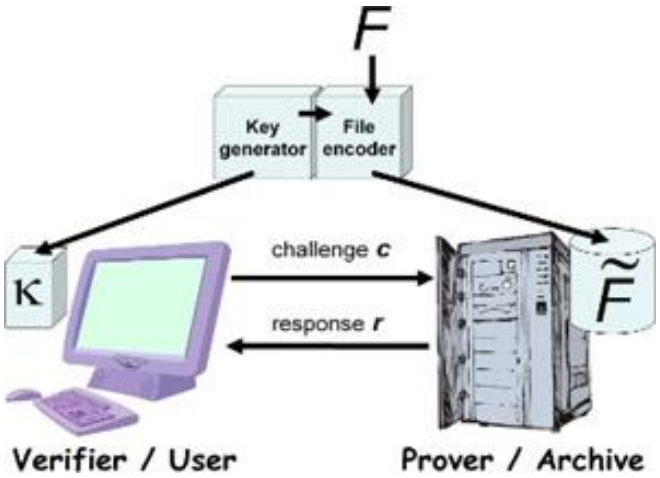

Figure 6. POR – Data Verification Process

Data Integrity Verification Mechanisms

a. Cryptographic Hash Functions

- Hashing algorithms like **SHA-256, SHA-3, and MD5** generate a fixed-size hash value for data.
- Any unauthorized modification changes the hash value, alerting users to integrity breaches.
- Used in cloud storage to verify data authenticity after transmission or retrieval.

b. Merkle Tree Authentication

- A hierarchical structure where each leaf node represents a hash of a data block.
- Any change in data results in a different root hash, enabling efficient integrity verification.
- Commonly used in blockchain and cloud storage integrity checks.

c. Digital Signatures

- Data is signed using **public-key cryptography (RSA, ECC)** to ensure authenticity and prevent tampering.
- Used in cloud applications to verify that stored or transmitted data remains unaltered.

Intrusion Detection & Monitoring Mechanisms

a. AI & Machine Learning-Based Anomaly Detection

- AI-driven systems analyze cloud activity patterns to detect anomalies.
- Machine learning models identify unusual file modifications or unauthorized access.
- Used in **SIEM (Security Information and Event Management) systems** for real-time threat detection.

b. Blockchain-Based Data Integrity Auditing

- Blockchain technology provides a tamper-proof ledger to store data transaction histories.
- Ensures immutable record-keeping, preventing unauthorized data alterations.
- Used in cloud forensics and secure data storage applications.

c. Log Monitoring & Auditing

- Cloud service providers maintain **log files** tracking data access, modification, and deletions.
- **Automated logging tools** like AWS CloudTrail, Azure Monitor, and Google Cloud Audit Logs help detect anomalies.

Access Control & Authentication Mechanisms

a. Zero-Trust Security Model

- Requires continuous verification of user identity before granting access to cloud resources.
- Prevents unauthorized modifications by enforcing strict access controls.

b. Multi-Factor Authentication (MFA)

- Adds an extra layer of security by requiring multiple authentication factors (password, biometrics, OTP).
- Reduces risks of unauthorized access and insider threats.

c. Role-Based & Attribute-Based Access Control (RBAC & ABAC)

- **RBAC:** Assigns user permissions based on predefined roles (e.g., admin, user, auditor).
- **ABAC:** Grants access based on attributes like location, device, and security clearance.
- Prevents unauthorized users from modifying sensitive data.

Data Redundancy & Backup Strategies

a. Data Replication & Cloud Backup

- Storing multiple copies of data across different cloud regions prevents loss from attacks.
- Cloud providers like AWS, Google Cloud, and Microsoft Azure offer automated backup solutions.

b. Immutable Storage Solutions

- Some cloud providers offer **write-once, read-many (WORM) storages**, preventing any modifications after data is written.

Used in compliance-heavy industries to maintain audit trails.

c. Erasure Coding & Checksums

- **Erasure coding** splits data into fragments and distributes them across multiple cloud servers.
- **Checksums** verify data integrity by detecting corruption during storage or transmission.

Secure Data Transmission & Encryption Techniques

a. End-to-End Data Encryption

- Encrypts data **before** uploading to the cloud and **after** retrieval.
- AES-256, RSA, and homomorphic encryption ensure data remains confidential and unaltered.

b. Transport Layer Security (TLS) & Secure APIs

- TLS ensures secure data transmission between cloud servers and users.
- **API security** mechanisms like OAuth 2.0 and OpenID prevent unauthorized access to cloud storage.

Threat Intelligence & Automated Response Mechanisms

a. Cloud Threat Intelligence Platforms

- Collects real-time threat data to detect ongoing data integrity attacks.
- Cloud providers use **AI-driven threat hunting** to identify and neutralize integrity threats.

b. Automated Incident Response & Remediation

- Cloud security automation tools can **quarantine** compromised accounts or block suspicious activities.

Used in **SOC (Security Operations Centers)** for rapid response to integrity breaches.

Table 1. Summary of Existing Attacks and its Solutions

S. No.	Problem Type	Available Solutions
1	Data Leakage	User Rank method
2	Denial of Service(DoS)	Encryption,SSL, identity-based encryption, Homomorphic encryption ,Multilevel algorithm, Signature based detection, deep packet inspection
3	XML Attack	Filter based Approach
4	Spoofing	Strong Authentication
5	Hypervisor–Layer Attack	hardware token
6	Repudiation	Audit logging, Digital Signature
7	Data Isolation Failure	Multi-tenant data isolation, Sharing Middleware Scheme
8	Data Tampering	Hashing/ Digital Signature
9	DE Duplication Attack	Multilevel Authentication
10	Intrusion Detection	Anomaly Detection System Statistical Anomaly Detection Systems Data Mining Based Anomaly Detection Systems, Machine Learning Based Anomaly Detection Systems, Adaptive Anomaly Detection Systems
11	CAPTCHA Breaking	Text Based Captcha ,Audio Captcha ,Puzzle Based Captcha ,Image Based Captcha
12	Flooding Attack	Digital signatures, Authentication Technology
13	SQL Injection Attacks	parameterized statements
14	Cross Site Scripting Attacks	XSS Prevention Rules
15	Man in the Middle Attack	Strict SSL
16	Sniffer Attacks	SSH, IPsec
17	Hopping attacks Cookie Poisoning	Encryption keys
18	Cross vm side channel attack	XML signatures, Elgamal Encryption

Figure 7. Detecting and Preventing data integrity attacks in cloud environments.

Recent Years Data Integrity Attacks and its Solution

Table 2. Key data integrity attacks in recent years and their corresponding solutions to mitigate risks.

Year	Attack Name	Description	Solution
2021	SolarWinds Data Manipulation	Attackers inserted malicious code into the SolarWinds update, affecting major organizations.	Implement **zero-trust security**, continuous monitoring, and threat intelligence.
2022	AI-Powered Data Poisoning	Attackers injected manipulated data into AI/ML models, leading to biased or incorrect predictions.	**AI anomaly detection**, real-time data validation, and adversarial training.
2023	Ransomware with Data Tampering	Ransomware attacks encrypted data after making small, undetectable modifications.	**Immutable backups**, blockchain for data integrity, and advanced threat detection.
2024	Cloud Supply Chain Attack	Hackers compromised third-party cloud service providers, leading to widespread data corruption.	**Zero-trust architecture**, vendor risk assessment, and **multi-factor authentication (MFA)**.
2025	Quantum Cryptography Breach	Emerging quantum computers exploited vulnerabilities in traditional encryption, allowing data tampering.	Adoption of **post-quantum cryptography**, quantum-safe encryption methods, and **blockchain verification**.

5. Results

This section provides an overview of the most prevalent data integrity attacks in cloud computing and outlines several mitigation techniques proposed by researchers in various academic publications and conferences. As summarized, some attack types have corresponding countermeasures that can effectively address the associated risks. For example, data leakage can be mitigated using the User Rank method; XML-based attacks can be prevented through a filter-based approach; data isolation failures may be addressed using multi-tenant data isolation or the Sharing Middleware Scheme; spoofing attacks can be countered with strong authentication mechanisms; SQL injection attacks can be mitigated through the use of parameterized statements; and sniffer attacks can be prevented using secure communication protocols such as SSH or IPsec. Additionally, quantum cryptography breaches can be addressed through the adoption of post-quantum cryptographic algorithms, quantum-safe encryption methods, and blockchain-based verification techniques. These mitigation strategies offer practical approaches to enhance data integrity and security in cloud computing environments.

6. Conclusion and Future Enhancements

In this article, we have explored various data integrity attacks that can be detected by cloud service providers. We provided an overview of cloud computing and data integrity, highlighting their significance in today's digital landscape. Through a review of existing research, we examined the challenges and threats faced by cloud environments, particularly in ensuring data confidentiality and integrity.

As more IT enterprises adopt cloud platforms like AWS and Microsoft Azure, the responsibility of securing sensitive data falls on cloud service providers. While cloud storage offers cost-effective and scalable solutions, it also introduces security vulnerabilities. Ensuring robust encryption, real-time monitoring, and advanced intrusion detection mechanisms is essential to mitigate data integrity risks.

To prevent data breaches and loss, implementing strong security frameworks, zero-trust architectures, and blockchain-based integrity verification can enhance the resilience of cloud computing. As cloud technology continues to evolve, the focus on data integrity remains a critical research opportunity for developing next-generation security solutions.

Thus, designing secure cloud architecture requires a holistic approach, addressing all possible vulnerabilities to build a trustworthy and resilient cloud ecosystem. Future advancements in AI-driven security, post-quantum cryptography, and decentralized data protection will play a crucial role in strengthening cloud Saas cloud computing continues to evolve, ensuring data integrity remains a critical challenge. Future advancements in security technologies will focus on enhanced threat detection, automated mitigation, and decentralized trust models. Below are some key future enhancements for protecting data integrity in cloud environment security against emerging threats.

7. Acknowledgement

I would like to express my special thanks of gratitude to my college management. I would like to give my thanks to the guide who gave me the golden opportunity to do this wonderful project on Ensuring Data Integrity In Cloud Computing: A Review Of Threats And Protection Strategies. In addition, I would also like to thank my parents who helped me a lot in finalizing this project within the limited time frame.

8. References

[1] Kaja, D. V. S., Fatima, Y., & Mailewa, A. B. (2022, February). Data integrity attacks in cloud computing: A review of identifying and protecting techniques. IJRPR, ISSN 2582-7421.

[2] Nepal, S., Chen, S., Yao, J., & Thilakanathan, D. (2011, July). DIaaS: Data integrity as a service in the cloud. In 2011 IEEE 4th International Conference on Cloud Computing (pp. 308–315). https://doi.org/10.1109/CLOUD.2011.35

[3] Dissanayaka, A. M., Mengel, S., Gittner, L., & Khan, H. (2020). 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).

[4] Mailewa, A., & Herath, J. (2014). 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

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

[6] Chen, Y., Li, L., & Chen, Z. (2017, December). An approach to verifying data integrity for cloud storage. In 2017 13th International Conference on Computational Intelligence and Security (CIS) (pp. 582–585). https://doi.org/10.1109/CIS.2017.00135

[7] Sevis, K. N., & Seker, E. (2016, June). Survey on data integrity in cloud. In 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 167–171). https://doi.org/10.1109/CSCloud.2016.35

[8] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications, 36(1), 42–57. https://doi.org/10.1016/j.jnca.2012.05.003

[9] Dissanayaka, A. M., Mengel, S., Gittner, L., & Khan, H. (2018). 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).

[10] Akintaro, M., Pare, T., & Dissanayaka, A. M. (2019). Darknet and black-market activities against the cybersecurity: A survey. In The Midwest Instruction and Computing Symposium (MICS), North Dakota State University, Fargo, ND.

[11] Vurukonda, N., & Rao, B. T. (2016). A study on data storage security issues in cloud computing. Procedia Computer Science, 92, 128–135. https://doi.org/10.1016/j.procs.2016.07.335

[12] Dissanayaka, A. M., Mengel, S., Gittner, L., & Khan, H. (2020). Security assurance of MongoDB in singularity LXCs: An elastic and convenient testbed using Linux containers to explore vulnerabilities. Cluster Computing, 23(3), 1955-1971.

[13] Jyoti, A., Shrimali, M., Tiwari, S., & Singh, H. P. (2020). Cloud computing using load balancing and service broker policy for IT service: A taxonomy and survey. Journal of Ambient Intelligence and Humanized Computing, 11(11), 4785–4814. https://doi.org/10.1007/s12652-020-01747-z

[14] Sudalai, S., & S., S. S. (2016, April). A survey on cloud security issues and challenges with possible measures.

[15] Lai, C.-I., Abad, A., Richmond, K., Yamagishi, J., Dehak, N., & King, S. (2019). 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.

8.Conflict of Interest

The authors declare that they have no conflicts of interest.

9.Funding

No external funding was received to support or conduct this study.