International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8470
***Article Received:** 24 July 2023 **Revised:** 22 September 2023 **Accepted:** 03 October 2023*

The Analysis of Data Tampering and Forensics in a Cloud Environment

Vibha Upadhya[1], Dr. A.A. Bhusari[2], Zaid Ibrahim Shaikh[3], Arshia AH Tamboli[4]
[1]Department of MCA
Trinity Academy of Engineering
Pune, India.
vibhaupadhyay0610@gmail.com
[2]Department of MCA
Trinity Academy of Engineering
Pune, India.
aabhusari@gmail.com
[3]Department of MCA
Trinity Academy of Engineering
Pune, India.
zaid.rh29@gmail.com
[4]Department of MCA
Trinity Academy of Engineering
Pune, India.
arshiatamboli@gmail.com

Abstract— In cloud systems, where sensitive data is stored and processed remotely, data manipulation is a serious security problem. The issues of data tampering in cloud environments are explored in this research, along with the importance of forensic investigation in reducing its effects. We explore several data tampering techniques and illustrate the need for strong security measures to guard against unlawful behavior. This paper also covers forensic analysis methods, tools, and techniques that are crucial in locating, analyzing, and minimizing data tampering instances in cloud systems. The security posture associated with cloud infrastructures can be greatly improved by integrating cutting-edge forensic procedures, ensuring data integrity, confidentiality, and overall system dependability.
Keywords-cloud, tampering, forensics analysis, data manipulation.

I. INTRODUCTION

Cloud computing refers to the use of full digital capabilities given through the internet by organisations in order to operate, innovate, and serve customers. It reduces the need for businesses to host digital apps on their own servers and instead allows them to access computer resources on demand, paying just for the utilisation and capacity they require without making upfront infrastructure investments. Since the cloud is a shared and distributed environment where data is stored and accessed by multiple users and applications, data integrity becomes one of the crucial aspects because it provides accuracy, reliability, and consistency of data stored and processed in the cloud computing environment. Every year, there is a significant growth in cloud breaches. Attackers unveil malicious files that alter log files, modify user credentials to access sensitive data, or change the configuration of a network or system. Imagine if an intruder gained access to the servers of your business, changed the data of your clients, and then tampered with the log files to hide their traces. In order to overcome these barriers, preserve assets, and maintain consumer trust, forensic analysis is essential.

II. DATA TAMPERING: METHODS AND THREATS

Data tampering is one dangerous hazard that poses a serious risk to the integrity and confidentiality of data in cloud systems. This part describes the various techniques and dangers that attackers use to alter or compromise cloud-based data. Understanding these strategies and associated risks can help businesses create strong security measures to protect their data from hacking attempts, maintaining the confidence and dependability of cloud infrastructures. Following are some ways in which the activity can be concluded.

A. Unauthorized access and modification.

- Unauthorized Entry: Unauthorized access can be described as gaining access to cloud resources, applications, or data without authorization. Attackers use flaws in authentication protocols, unsecured

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8470
***Article Received:** 24 July 2023 **Revised:** 22 September 2023 **Accepted:** 03 October 2023*

passwords, or stolen credentials to evade security protections and gain access to sensitive information.
Impact: Unauthorized access may end in data breaches, unauthorized data absorbing or alteration, private information loss, and violations of privacy and compliance requirements.

- Unauthorized Modification: Unauthorized modification is the act of changing data, configurations, or applications without permission. Attackers may change data for harmful reasons by exploiting vulnerabilities, lax security procedures, or insider privileges.
  Impact: Unauthorized change can result in corrupted data, misleading or erroneous information, service disruptions, financial losses, and reputational damage to an organization.

B. Data interception and eavesdropping.

- Data Interception: When an attacker intercepts and captures data flow between a user and a cloud service, this is referred to as data interception. This can happen through a variety of methods, such as sniffing unencrypted network traffic or exploiting network device deficiencies.
  Impact: Data interception can disclose sensitive information such as passwords, credit card numbers, and confidential corporate data, resulting in identity theft, financial fraud, and privacy violations.
- Eavesdropping: It is an act of listening in on or monitoring conversations or data exchanges without the parties' knowledge or consent. Listening to data transfer between a user and a cloud server in an environment with clouds.
  Impact: Eavesdropping can result in unauthorized access to sensitive information, intellectual property theft, and violations of privacy laws and regulations.

C. Man in middle.

In a MitM attack, the attacker intercepts data being sent between a user and a cloud service and potentially modifies it without the user's knowledge. The attacker can stand in the way of a conversation between two parties and gain access to private data. MitM attacks can lead to data breaches, identity theft, financial fraud, unauthorized access to sensitive information, and data manipulation.

III. CHALLENGES IN DETECTING AND PREVENTING DATA TAMPERING

Assuring the integrity of data has grown to be of utmost importance in the constantly changing world of cloud computing. The detection and prevention of data tampering present significant difficulties in this area. This section goes into the specifics of these difficulties, illuminating the numerous obstacles that obstruct both the identification and mitigation of data tampering in cloud systems. Understanding these issues is a vital first step in enhancing cloud security and maintaining data integrity.

A. Lack of physical control over the infrastructure.

Users in the significantly hampered by this absence of physical control.
The physical systems, including the servers, storage, or networking components, is managed and maintained by cloud service providers. Regarding the integrity and security of their data, users depend on the provider's security precautions and guarantees.
Impact: Users are unable to immediately deploy or validate security measures on the hardware without physical control. Due to users' dependence on the provider's security solutions, it is difficult to cloud do not have physical control over or direct access to the underlying hardware and infrastructure that hosts their data and apps. The detection and prevention of data manipulation are to identify and prevent data tampering because of this lack of control.

B. Encryption and Decryption complexities.

Encryption is a critical tool for protecting data in environments like the cloud. It does, however, add complications in terms of computational expenses and key management, affecting system efficiency and usability.
Encryption is the process of converting plaintext data into cipher text using encryption methods, rendering it unreadable in the absence of the right decryption key. Decryption is the process of transforming cipher text to plaintext in the opposite direction.
Impact: Overheads for computation: Encryption and decryption use additional computer resources, slowing data processing and lowering system performance, particularly for large-scale data operations.
Key Personnel: It is difficult and vital to ensure data security to manage encryption keys effectively, including protected generation, storage, distribution, and rotation.

C. Multi-tenancy and Shared Resources.

Multi-tenancy is a fundamental feature of cloud computing that allows several users or tenants to share identical physical and/or virtual assets. Sharing resources raises issues of isolation, security, and performance.
Users in a multi-tenant system share infrastructure such as servers, storage, and networking. This sharing has the potential to pose security problems as well as performance issues.
Impact:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8470
***Article Received:** 24 July 2023 **Revised:** 22 September 2023 **Accepted:** 03 October 2023*

- Isolation: It is critical to ensure robust isolation between tenants in order to avoid unauthorized access and data breaches.
- Security Risks: Sharing resources broadens the attack surface, and a security compromise in one tenant's environment can have ramifications for others.
- Performance Degradation: If one tenant uses an overabundance of resources, it might lead to performance degradation.

IV. FORENSIC ANALYSIS IN CLOUD ENVIRONMENT

In the context of cloud security, forensic analysis is the methodical investigation and inspection of digital evidence within cloud environments with the aim to locate, preserve, analyze, and present data pertaining to security incidents, breaches, or possible threats. To comprehend the scope and nature of security incidents, collecting evidence for legal proceedings, and enhance security protocols to avoid recurrences are the primary goals of forensic analysis.

In order to detect and reduce data tampering occurrences, forensic analysis is essential in the following ways:

- Prevention and Early Detection: By continuously scanning systems and network traffic for questionable activity, forensic analysis aids in the early discovery of data manipulation occurrences. Early detection of tampering enables a speedier response and the ability to stop additional harm.
- Evidence Gathering and Preservation: Forensic analysts gather and preserve evidence relating to data tampering, making sure it is handled properly to protect its integrity and admissibility in court cases. This evidence may be essential for determining the tampering techniques and estimating the harm.
- Root Cause Analysis: A detailed root cause analysis is conducted with the assistance of forensic analysis to determine how the data tampering took place. This entails looking through logs, system configurations, and other artifacts to identify the weaknesses or vulnerabilities that were exploited, allowing businesses to fix the problems and stop further instances.
- Legal Action and Accountability: Forensic analysis is essential for legal actions and holding the guilty parties accountable in the event of data tampering. To support legal actions against offenders, discourage potential malicious actors, and seek proper legal compensation, forensic investigations can gather material that can be used as evidence in court.
- Improvement of Incident Response: Organizations can enhance their incident response strategies and practices by conducting forensic analyses of situations involving data manipulation. It is possible to improve incident response plans, update security measures, and create better methods for resisting and limiting future tampering attempts using the lessons learnt from the analysis.
- Data Integrity Restoration: By discovering impacted data and authenticating unmodified data, forensic analysis offers a foundation for data integrity restoration. This procedure aids in restoring the data to its original, undamaged state and ensures the reliability and accuracy of the information.

A variety of procedures and technologies are used in forensic analysis techniques and methodologies in cloud environments to look into and examine digital evidence in cloud-based systems. Effective investigations, the preservation of evidence, and the mitigation of security issues inside cloud systems all depend on the adoption of a complete strategy that includes forensic analytical methodology and procedures such as live forensics, Memory Analysis, Disk and file system analysis, network forensics, malware analysis etc.

V. FORENSIC ANALYSIS PROCEDURES

Conducting forensic analysis in cloud environments requires a systematic and thorough approach to gather and analyze digital evidence while adhering to legal, ethical, and technical considerations. Forensic analysts can conduct a thorough forensic analysis in cloud environments, aiding in the identification, investigation, and reconstruction of security incidents to determine the extent of data tampering and potential security breaches. The comprehensive procedures for performing forensic analysis in cloud environments include:

A. Data collection and preservation.

- Identify Relevant Data Sources: Find the network elements, virtual machines, storage locations, and cloud services that are pertinent to the study. Consider logs, configurations, file systems, RAM, and network traffic as potential sources of evidence.
- Coordinate with Cloud Service Providers (CSPs): Notify the cloud service providers and work with them to ensure proper evidence preservation and adherence to their policies. Request the retention of any relevant information, virtual machine snapshots, or other important incident-related records.
- Forensic Imaging and Snapshot Creation: To preserve the status of virtual machines, storage volumes, and related devices at a certain time, create forensic images or snapshots of such objects. To ensure the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8470
***Article Received:** 24 July 2023 **Revised:** 22 September 2023 **Accepted:** 03 October 2023*

integrity and validity of the collected photos, use forensically sound techniques.

- Secure Evidence Storage: To preserve the chain of custody, keep forensic photos and gathered evidence in a safe, controlled environment with limited access.
- Keep a record of the evidence's storage location, date, time, and the people in charge of keeping it safe.

B. Analytics of logs and metadata.

- Collect Logs and Metadata: Obtain the appropriate cloud service logs and information from the applications, networks, and virtual machines that were used during the incident. Include details from logs related to the incident, such as access logs, authentication logs, system logs, and any others.
- Consolidate and Normalize Logs: To construct a comprehensive log repository, combine logs from several sources, normalize timestamps, and connect related events. For accurate analysis, make sure log formats and structures are consistent.
- Log Analysis and Correlation: To correlate events and find trends, abnormalities, or indicators of compromise (IoCs), use log analysis tools. Check for any odd or suspicious activity by analyzing login attempts, network connections, access patterns, and any other data.

C. Digital evidence extraction and analysis.

- File System and Artifact Analysis: Determine whether there have been any alterations, deletions, or unauthorized access by examining file system metadata, timestamps, and file properties. Investigate artifacts like event logs, registry entries, and prefetch files for any relevant forensic evidence.
- Memory Forensics: To find active processes, open network connections, and any malware artifacts, do memory analysis on the memory pictures that have been acquired. Extract e volatile data for additional study, including process listings, network connections, and cryptographic keys.
- Network Traffic Analysis: To find communication patterns, potential assaults, and data exfiltration efforts, analyze network traffic records and packets. Analyze the incident's scope and effects on the network infrastructure.

D. Incident reconstruction and determination of tampering extent.

- Timeline Creation: By combining information from logs, file system analysis, memory analysis, and network traffic analysis, create a chronological timeline of events. Reconstruct the incident timeline by mapping the sequence of events and activities.
- Attack Path and Extent Assessment: To ascertain the initial attack vector, lateral movement, and the degree of tampering or compromise, analyze the reconstructed timeline. Determine the affected systems, the data, and possible points of entrance and exit for the attacker.

Document and Report Findings: Record the findings of the inquiry, including the timeline of the incident, the specifics of the forensic study, and the degree of tampering. Summarize the findings, analysis, and suggestions for additional action and mitigation in a thorough forensic report.

VI. CASE STUDIES DEPICTING DATA TAMPERING IN CLOUD ENVIRONMENT

In the context of cloud security, forensic analysis is the methodical investigation and inspection of digital evidence within cloud environments with the aim to locate, preserve, analyze, and present data pertaining to security incidents, breaches, or possible threats. To comprehend the scope and nature of security incidents, collecting evidence for legal proceedings, and enhance security protocols to avoid recurrences are the primary goals of forensic analysis.

A. Toyota motor company (June 2023).

Toyota reported that owing to a misconfigured cloud environment, the data of about 260,000 consumers was exposed online. In addition to clients in Japan, data from customers across Asia and Oceania was exposed.

Customers who subscribed to G-BOOK with a G-BOOK mX or G-BOOK mX Pro compatible navigation system, as well as select customers who subscribed to G-Link / G-Link Lite*1 and renewed their Maps on Demand subscription between February 9, 2015, and March 31, 2022, are among those eligible, according to Toyota.

Toyota has taken steps to prevent unauthorized access to the data and is investigating the situation, which includes all cloud environments administered by Toyota Connect (TC).

B. Accenture (August 2021).

In August of 2021, Accenture fell prey to a LockBit ransomware attack. The culprits claimed to have stolen 6TB worth of data, for which they requested a ransom of $50 million. Accenture discovered abnormal behavior in one of the settings during the fourth quarter of fiscal 2021, including the extraction of proprietary information by a third party, some of which was made public by the third party. Furthermore, the clients have

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8470
***Article Received:** 24 July 2023 **Revised:** 22 September 2023 **Accepted:** 03 October 2023*

suffered, and may experience in the future, breaches of systems and cloud-based services enabled or provided by them.

After failing to obtain the demanded ransom payment from Accenture, the hackers eventually uploaded the stolen data to the internet.

C. LinkedIn (April 2021).

According to the report, the alleged hacker revealed the breach on a forum on June 22 and offered the data of 700 million members for sale. Restore Privacy was also able to validate a sample of the data released by the hacker, which contained the details of one million LinkedIn users.

Email addresses, full names, phone numbers, physical addresses, geolocation records, LinkedIn username and profile URL, personal and professional experience or background, genders, and other social media accounts and usernames are reportedly included.

CONCLUSION

The necessity of preemptive measures and advanced forensic analysis in properly securing cloud environments against data manipulation cannot be overstated. Here's a rundown of their relevance.

- Unauthorized access and alteration, data interception, eavesdropping, man-in-the-middle attacks, and malicious software are all means of data manipulation in cloud systems. These can have a significant impact on businesses and users by jeopardizing data integrity and confidentiality and resulting in financial losses.
- Physical control concerns, encryption complications, multi-tenancy issues, and a variety of attack routes are all challenges in cloud systems. Addressing these issues is critical for efficient data tamper detection and prevention.
- Forensic analysis is critical for detecting and minimizing cloud data manipulation problems. To understand the extent of tampering, it requires analyzing digital data, detecting tampering methods, and assisting in incident reconstruction.
- In cloud systems, forensic analysis follows a defined approach that includes data gathering, log and metadata analysis, digital evidence extraction, and incident reconstruction. These steps are required for a thorough examination.
- Real-world case studies demonstrate how forensic analysis may be used to successfully investigate and mitigate data tampering events in cloud systems.

REFERENCES

[1] Tim Mather, Subra Kumaraswamy, and Shahed Latif "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance"
[2] John R. Vacca "Computer and Information Security Handbook"
[3] Mell, P., & Grance, T. (2011). "The NIST Definition of Cloud Computing." National Institute of Standards and Technology (NIST) Special Publication, 800-145.
[4] Kandukuri, B. R., & Rakshit, A. (2009). "Cloud Security Issues." In Proceedings of the 2009 IEEE International Conference on Services Computing.
[5] NIST. (2012). "Guide to Security for Full Virtualization Technologies." National Institute of Standards and Technology (NIST) Special Publication, 800-125
[6] Stallings, W. (2017). "Cryptography and Network Security: Principles and Practice." Pearson.
[7] Schneier, B. (1996). "Applied Cryptography: Protocols, Algorithms, and Source Code in C." John Wiley & Sons.
[8] Dierks, T., & Rescorla, E. (2008). "The Transport Layer Security (TLS) Protocol Version 1.2." IETF RFC 5246.