



International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

An Analytical Review of Cloud Storage Vulnerabilities and Their Implications on Cyber Security Architecture

Dr. Chitra S¹, Mr. Ravichandran D²

¹Department of Computer Applications SRM Trichy Arts and Science College Tiruchirappalli, India. Email: chithismca@gmail.com

²Department of Computer Science M.I.E.T Engineering College Tiruchirappalli, India. Email: ravichandran.d@miet.edu

Abstract—Cloud storage is generally used to store and manage digital data over the Internet. It offers several useful features, including easy access, scalability, and cost-effectiveness. However, storing sensitive data in the cloud also creates major cyber security issues. This paper explains common threats and vulnerabilities in cloud storage across various layers, including user devices, network access, authentication, encryption, and cloud infrastructure. Real-life examples illustrate how attacks such as data breaches, weak authentication, misconfigured access, and virtualization flaws can occur. The paper also discusses simple and effective security strategies, such as strong passwords, data encryption, multi-factor authentication, role-based access control, and user awareness. These methods help protect data from unauthorized access, loss, or theft. The goal of this paper is to improve the understanding of cloud storage security and provide practical strategies to make it safer for both users and institutions.

Index Terms—Cloud Storage, Cyber Attacks, Data Breaches, Multi-Tenant, Security API, and Encrypted Techniques.

I. INTRODUCTION

Cloud storage is a storage service that is used to store and access digital data via the Internet. The most common cloud platforms, such as Google, Dropbox, OneDrive, or Amazon S3, store data securely and retrieve them at anytime. In this storage, data are protected from unauthorized theft, loss, or corruption through strong cybersecurity measures. It also ensures Confidentiality, Integrity, and Availability (CIA) methods for digital data through cryptography techniques, authenticated measures, security Application Programming Interfaces (APIs), and audits. For example, in universities, student records are stored in cloud platforms like GoogleDrive or Amazon S3, where only authorized users are allowed to access the files. The data is encrypted during data storage and transmission. This secure process ensures continued access even during system failure or cyber attacks.

Although cloud storage offers great convenience and flexibility, it also brings serious cyber security concerns. Since cloud systems work over the Internet and often use shared infrastructure, they are exposed to new types of cyber threats. These risks require a move away from traditional security methods to more advanced and adaptive security models. Recent cases of data breaches and ransomware attacks on cloud platforms have shown the weaknesses that exist in these systems. Some examples are sensitive data being exposed due to wrongly configured cloud storage settings and weak login security allowing unauthorized access.

Considering the important role of cloud storage in the digital world of today, protecting it is highly essential. This paper focuses on identifying key vulnerabilities in cloud storage systems and examining the cybersecurity challenges they present. It also discusses possible solutions, frameworks, and technologies to reduce the serious attacks and ensure the CIA methods of data in the cloud.

II. ARCHITECTURAL OVERVIEW AND ATTACK SURFACES

A. Cloud Storage Architecture

Cloud storage architecture describes the design and structure of cloud services, storage, maintenance, and retrieval. It has various layers and components that work together to transmit data through the Internet. The following figure, Fig. 1, shows the layers of the architecture.

- 1) **User Interface Layer:** It acts as a front-end layer and also acts as an interface that interacts with clients such as web portals, mobile apps, and so on. This layer allows users to upload, download, and manage files easily.
- 2) **Data Services Layer:** It manages key functions of cloud storage services, including user management, billing, authentication, and APIs. For example, Google Drive accesses the stored files and checks the credentials when a user logs in.
- 3) **Data Storage Layer:** This layer, also referred to as a backend, stores data from multiple servers and locations. Typically, data is stored in formats like object or block storage, replicated across many areas, and divided into smaller pieces.
- 4) **Database Layer:** This layer gives the benefits of quick search, indexing, and file management. Metadata such as file names, user IDs, timestamps, and permissions is kept in organized databases.
- 5) **Data Transmission Layer:** It supervises data transmission through the Internet. It also facilitates safe data transport between users and cloud storage servers.



Fig.1.Layers of cloud storage architecture

B. Cloud Storage Security

The security in cloud storage plays an important role as data is stored off-site and also shared throughout the internet. It protects data from unauthorized access, leakage, data loss, and corruption. Further, it describes the important security features and practices as follows.

- 1) **Data Encryption:** The data is protected through an encryption technique, used at the time of storage and transmission. Various algorithms, such as AES (Advanced Encryption Standard), and TLS (Transport Layer Security), are used when the user uploads the documents to the cloud and the file is encrypted before it reaches the server.
- 2) **Access Control:** The data can be accessed only by authorized users. Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC) enhance login security and protect data from unwanted theft.
- 3) **Authentication and Identity Management:** Permissions are securely managed and ensure user identification using services such as Google identification and AWS IAM (Identity and Access Management).
- 4) **Data Redundancy and Backup:** Cloud providers keep multiple copies of data in various places to

prevent data loss caused by disasters or hardware failure.

5) **Monitoring and Logging:** Suspicious activities, such as repeated unsuccessful login attempts or illegal file downloads, can be found with the use of activity logs and continuous monitoring software.

6) **Compliance and Legal Requirement:** Cloud services must comply with data privacy rules such as GDPR (General Data Protection Regulation) or India's Digital Personal Data Protection Act to guarantee that data is handled properly.

C. Cloud Storage Reference Model

A threat vector refers to the method through which cyber-criminals obtain unauthorized entry to cloud storage services like Google Cloud, Amazon and others. It represents the phase during which the attack is executed. For example, if an attacker sends a fake email with a malicious link to a university employer and the employer clicks the link and provides the credentials. The most familiar and common threat vectors are phishing, malware, unsecured websites and software that have not been updated.

Cloud storage has a common architecture that includes client-side data management interfaces, internet communication layers, access control mechanisms, and back-end data stores hosted by cloud service providers (CSPs). Figure 2 depicts a framework that highlights key threat vectors. For example, in a university, student records, such as mark sheets and identification proofs, are stored in secure cloud storage. The information is encrypted, access is restricted to faculty members, and backup copies are generated automatically. If an unauthorized login is detected from an unfamiliar location, the system notifies the administrator and has the capability to prevent the attempt.



Fig.2.Key threat vectors of cloud storage

The above framework consists of five security sensitive layers, each with its potential threat and vulnerabilities. The description of each layer and its threat is as follows.

1) **User Devices:** Devices such as desktops, laptops and mobile phones serve as the user's entry point to cloud storage. Social engineering threats like phishing, emails, malware infections or fake login pages can affect these devices. For instance, a college student receives a fake email that appears to be a Google Drive notification. The student clicks the link and enters their login credentials on a fake website. The attacker steals the credentials and gains unauthorized access to the cloud account. Using MFA, educating users about phishing and installing antivirus software can prevent such attacks.

2) **Network Access Layer:** It plays an essential function in cloud storage environment. It acts as a bridge to carry data from the user device to the cloud server through the internet. It also ensures that data is securely transmitted across networks.

The most important risk in this layer is Man-in-the-Middle (MITM). In this attack, a cybercriminal, observes changes or steals the information between the user device and the cloud server. It is unsafe when authenticated data such as usernames, passwords or academic records is concerned. The next popular threat is Packet Sniffing. Cyber attackers use software tools to extract the data travelling in the network.

3) **Authentication Gateway:** It is an essential component to verify the identity of users accessing the cloud system. It serves as a front-line gatekeeper, allowing only authenticated and authorized users to interact with stored data or services. In this layer, there are two main challenges of weak authentication and insecure API. Weak authentication occurs when the system uses easily predictable username and password without adding any extra security measures like two-factor authentications (2FA). This method makes the system highly susceptible to brute-force attacks, credential stuffing or password reuse exploits.

Another important threat is insecure APIs. These interfaces act as a communicator between the users and the cloud system. If strong authentication methods are not used, attackers can easily manipulate the stored data. If APIs are not properly secured, hackers can use automated tools to try many login attempts (brute force attacks) and access information that is meant to be private.

4) **Data Encryption and Access Control:** The Data Encryption and Access Control layer of cloud storage systems is responsible for ensuring that data is kept private, secure, and only accessible by authorized users. The CIA principles of cyber security are primarily ensured by this layer. If this layer is not secured, there may be data breaches, consequences from the law and a reduction in confidence. Strong encryption techniques and strong access controls are two ways that educational institutions, in particular, must incorporate to safeguard student, institutional and research information.

There are two major risks in this layer- Key mis management and Misconfigured Access Control List (ACL). Generally, cloud storage uses encryption techniques to keep information safe. The process of creating, storing, allocating and deleting the key safely is known as key management. If the keys are not maintained properly, it leads to major risks, known as key mismanagement. This is the major challenge faced by cloud environments.

The examples of key mismanagement are encryption keys stored as plain text on the same server, embed private keys used in the source code and stored as public repository, lack of access controls on keys, and improper key rotations in cloud storage.

The other risk factor is Misconfigured Access Control Lists (ACLs). In Cloud Storage, ACL is used to read, write, delete or share files. The major challenge is to maintain the access rights in both shared and multi-user environments. The risk of a misconfigured ACL occurs when access rights are accidentally given to unauthorized individuals. Some examples are accessing cloud data publicly, access rights given to an unauthorized person, and outside sharing without any limitations.

5) **Cloud Storage Infrastructure:** The primary backbone of any cloud storage device is the Cloud Storage Infrastructure Layer. This layer comprises of both physical hardware and software that makes storage functions possible in a multi-tenant environment, representing multiple individual users who share common resources (servers, databases, and storage devices) and a virtualized environment that refers to multiple virtual machines (VMs) executing in a single system. The basic components of these layers are physical servers, storage devices, and hypervisors that determine a software layer to create virtual versions of hardware systems like servers, storage devices, and networks.

There are two common threats in this layer - Virtual Machine (VM) Escape and Privilege Escalation. VM Escape is a serious security issue in virtualized environments. The hacker breaks out of its isolated system and steals data from the host system or other tenants on the same physical server. Privilege Escalation is the most dangerous attack in both traditional and cloud-based environments. It happens due to weak passwords, poor access control, insecure endpoints and other software vulnerabilities. The attackers will be able to access sensitive data, modify or delete data from the cloud, disable security controls, and hide malicious activity.

III. CYBER SECURITY CHALLENGES IN CLOUD STORAGE

In the modern world, cloud storage plays a vital role in offering flexible and scalable data maintenance. More complicated cyber security issues are brought through resource sharing, remote access and reliance on third-party providers. It is essential to state the challenges of all layers of the cloud environment (shown in figure 3).

1) **Data Breaches:** Data breaches occur when an unauthorized person accesses sensitive information. It is caused due to poor access control and weak authentication systems.

2) **Insecure APIs and Interfaces:** A cloud service relies on functionality and communication. These APIs may become attack surfaces if insecure. Lack of authentication and encryption, or exposure to internal operations, can cause deletion of data or download of stored data.

3) **Data loss and Unavailability:** Cloud storage data can be deleted either accidentally or by a ransom

ware attack. The attack can occur due to a lack of recovery and backup mechanisms, system, or human errors.

4) **Insider threats:** An insider acts as a contractor or works among the other individuals of a firm and compromises data security either intentionally or unintentionally. This threat happens by weak policies of an organization, excessive permissions given to users, and inadequate performance monitoring and auditing the cloud storage.

5) **In sufficient Identity and Access Management (IAM):** If the roles and responsibilities in an organization are not properly defined, an unauthorized person can gain access controls. Lack of Role-Based Access Control (RBAC) and Multi Factor Authentication (MFA), and weak password policies cause these challenges.

6) **Vulnerability of shared resources:** The cloud storage service relies on multi-tenant architecture and shared VMs for resources. If a hacker attacks any one VM, it may affect the other tenant in the architecture. VM Escape and Privilege Escalation are the common threats in a virtual environment.

7) **Absence of transparency and control:** A third-party provider's support for storage and security in a cloud service poses difficulty in implementing security measures. It is due to the black box nature of cloud platforms and limited access control to systems.



Fig.3.Challenges in cloud storage

IV. PROPOSED APPROACH FOR SECURITY MEASURES

The cyber security challenges in cloud storage system can be solved by a defense-in-depth approach. The following policies are proposed in fig. 4 to solve each layer of the environment.

A. End User Device

Implementation of MFA adds an extra step during login to check whether the person logging in, is authorized or not. For instance, logging into a university's dashboard requires both password and an OTP sent to registered mobile number as credentials. Devices can be secured from viruses and harmful apps by installing Antivirus like ESS and Anti-malware soft-ware, and by utilizing Mobile Device Management Systems such as Microsoft Defender on student laptops. User awareness and training is essential to enable users to identify phishing messages, protect themselves from social engineering attacks, and use strong passwords. Any sensitive information that is protected or deleted will be secured by Remote Wipe and Device encryption.

B. Network Access Layer

In order to protect the Network Access Layer, all data transfer between the enduser and the cloud should be secured by using HTTPS (Hyper Text Transfer Protocol Secure) with TLS/ SSL encryption methods. For instance, students can upload their documents like assignments or project report on Google Drive through a browser. TLS guarantees that student data is encrypted during transmission. It is strongly advised to use VPN while using public Wi-Fi in places like railway stations, airports and hospital, to access cloud services. For example, if students want to check their mark statement through public Wi-Fi, the student should use a VPN to avert eavesdropping. IDPS is used to check and monitor network traffic and notify administrators about

any suspicious activity like repeated login attempts from unidentified IPs. Finally, secure DNS services and IP filtering help to block access of unsafe websites and restrict access to cloud storage. Only authorized users and trusted networks can access internal cloud storage using College Campus IPs.

C. Authentication Gateway

Organizations can strengthen the authentication gateway by implementing strong password policies, like a longer combination of letters, numbers and special characters. Users can be asked to change their password more frequently, for example, once in 60 days, to protect their sensitive data. By using OAuth2orOpenIDConnect, users can login securely without storing their credentials. The primary components of a secure API design to stop brute force attack are rate limiting, input validation to avoid injection attacks and token expiration to limit the life time of access tokens. For example, an API that allows access to student reports must discard unexpected inputs and expire tokens after 10 minutes of idleness. Further, to protect their mobile applications, users can access the content of the cloud storage by implementing biometric authentication through iris, fingerprint and face IDs. This can be implemented in sectors like healthcare and education, where confidentiality is essential.

D. Data Encryption and Access Control

RBAC is a technique that organizations should use to secure data in cloud storage. It allows users to only access the files and functions to which they have permission according to their roles. For instance, in college, students will be able to view their attendance, but they cannot edit those records. Encryption of data at rest and in transit is crucial. Files should be encrypted using robust algorithms like AES-256 when stored and connections should be secured using TLS when data is being sent over the internet. Effective key management is essential to centralized control of encryption keys. Tools like AWS Key Management Service and Azure Key Vault can be used to reduce the risk of loss or misuse of keys. Regular access reviews help to maintain user permissions and access control lists are regularly updated, such as removing staff that depart from the institutions or students who have graduated.

E. Cloud Storage Infrastructure Layer

Strict tenant isolation is an important technique in the cloud storage infrastructure layer to make sure that a user's VM

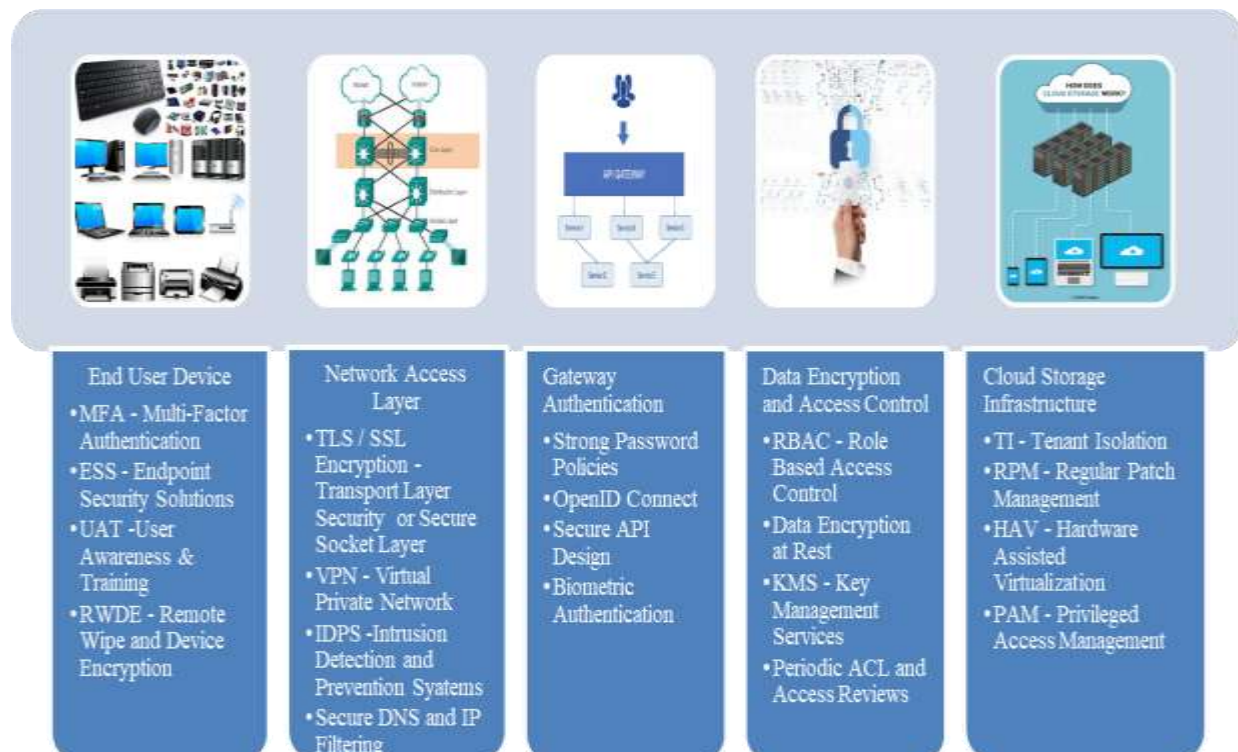


Fig.4.Layer-wise proposed policies

Cannot access another VM. It can be achieved by implementing robust hypervisor rules to separate workloads, like isolating databases from various universities on a shared cloud server. Regular patch management improves security against known flaws. For example, VM Escape attempts can be avoided by updating the cloud provider's hypervisor software. Hardware-assisted virtualization technologies enable the hardware to be more safe and securely handle the functions of VM. AMD-V and Intel VT-x improve isolation of different VMs. Finally, privileged access management confirms that only authorized administrators access settings related to key facilities, and also ensures that every activity is recorded and tracked. For example, tools like Cyber Ark or Beyond Trust can track admin actions and prevent misuse and insider threats.

V. CONCLUSION

Cloud storage has grown to become an essential component of the modern digital network. It provides scalable, affordable and accessible solutions to manage data. However, the convenience and flexibility of cloud services also have serious cyber security challenges over the multiple architectural layers, ranging from end-user device to cloud storage infrastructure. Challenges like unauthorized access, data breaches, misconfigured access controls and virtualization vulnerabilities demand a proactive and layered security approach. This paper has highlighted the threat at each level and also proposed practical strategies to overcome each of them. Some suggested approaches include Multi-Factor Authentication, Encryption services like TLS/SSL, Tenant Isolation and User Awareness. Regular Tracking, Advanced Security Procedures and Shared responsibilities between cloud storage and users are necessary to ensure the CIA of data in cloud environments. The proposed security frameworks help to handle new threats and safely protect sensitive data in an interrelated world.

REFERENCES

- [1] T.Jung,X.-Y.Li,Z.Wan, and M.Wan, "Privacy Preserving Cloud Data Access with Multi-Authorities," in Proc. IEEE INFOCOM, 2013.
- [2] N.H.Sultan, V.Varadharajan, L.Zhou, and F.A.Barbhuiya, "A Role-Based Encryption Scheme for Securing Outsourced Cloud Data in a Multi-Organization Context," IEEE, 2020.
- [3] J. Liu et al., "vFAC: Fine-Grained Access Control with Versatility for Cloud Storage," arXiv pre-print, 2018.
- [4] F.Zhang, X.Fan,P. Zhou, and W.Zhou, "On the Security of A Remote Cloud Storage Integrity Checking Protocol," arXiv pre-print, 2019.
- [5] S. K. Sood, "A Combined Approach to Ensure Data Security in Cloud Computing," J. Netw. Comput. Appl., 2012.
- [6] A. I. Tahirkheli et al., "A Survey on Modern Cloud Computing Security over Smart City Networks," Electronics, vol. 10, no. 15, 2021.
- [7] IEEE, "IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices (IEEE1619)," IEEE,2007 & revisions.
- [8] ISO/IEC, "ISO/IEC 27040: Storage Security – Technical Standard," ISO/IEC, 2015.
- [9] Gartner, "Top Cloud Security Threats and Trends in 2023," Gartner Insights, 2023.
- [10] NIST, "SP 800-210: General Access Control Guidance for Cloud Systems," 2023.
- [11] S. M. Risten part et al., "Hey, You, Get Off of My Cloud," ACM CCS, 2022.
- [12] S. Subashini and V. Kavitha, "A survey on security issues,"J. of Network and Computer Applications, 2023.