Data Security on Cloud Services: Threats and Mitigation

Pranjal
Muurgan R, Professor,
School of Commerce Science and Information Technology,
Jain (Deemed-to-be University
Bengaluru, India

Abstract: ***We try to examine the state of cloud computing today and the difficulties in protecting data across several cloud services. The rapid increase in the adoption of public and private cloud services by organizations poses a significant security risk for organizations. We examine various security challenges unique to the cloud environment and various mitigation techniques to deal with the threats. Our paper delves into the collaborative aspect of cloud security, highlighting the shared responsibility model between cloud providers and customers. Additionally, we also investigate various mechanisms adopted by cloud service providers to mitigate security risks.***
This widespread and accelerated adoption of a new cloud environment has inadvertently led to security threats. Increasingly, cyber attackers are choosing to leverage cloud services rather than develop their own attack infrastructure

For example, Code Spaces, a provider of source code hosting services, was compelled to shut down after hackers hacked into their AWS credentials and erased customer data.

Cyber analytics company Cognyte's database was left unsecured in June 2021, resulting in the exposure of 5 billion records documenting past data breaches. The sensitive data in the database was accessible without the need for authentication for a duration of 4 days.

Keywords— Cloud computing, Data threats, Data Protection,Cloud security,

I. INTRODUCTION

Cloud services utilize services that are hosted online, including storage of data, servers, databases, networking, and software. The data is maintained on physical servers, which are owned and operated by cloud service providers. This eliminates the need for customers to manage the physical aspect themselves. This not only helps them avoid getting involved in complex maintenance but also helps them save money. As of 2024, cloud services host nearly all the applications we use, both big and small, which aids in saving storage, costs, and time for companies.

The benefits that attract users or companies are: (i) Trade capital expense for variable expense; (ii) Scalability; (iii) Global in minutes; (iv) Increased speed and agility of resources deployed; (v) Innovation on cloud platforms

The current definition of a cloud According to the **National Institute of Standards and Technology (NIST)**, a framework exists that allows for easy, immediate access to a communal pool of virtual memory blocks. The resources are quickly set up and deployed, requiring little management involvement or interaction with service providers. [1]

Furthermore, groups like the **Cloud Security Alliance (CSA) and the European Telecommunications Standards Institute (ETSI)** have their own frameworks and criteria for cloud computing. These frameworks may correspond with NIST's model but can include further features or slightly alternative interpretations. [2]

Table1. Cloud Provider Services

Service Name	**Amazon Web Services (AWS)**	**Azure**	**Google Cloud Platform (GCP)**
Object Storage	Simple Storage Service (S3) Bucket	Block Blob	Cloud Storage Bucket
Compute Instance	Elastic Compute Engine (EC2)	Virtual Machine	ComputeEngine
Load Balancer	Application Load Balancer	Load Balancer Application Gateway	Cloud Load Balancing
Databases •**Relational** •**Warehouse** •**No-SQL**	• Relational Database Service (RDS) • Redshift • DynamoDB	• SQL Database • SQL Data Warehouse • Cosmos	• Cloud SQL • Big Query • Cloud Bigtable

II. CLOUD ARCHITECTURE AND SECURITY NEED

Cloud architecture consists of two fundamental parts: The front end is what the user or client interacts with, including client-side interfaces and applications. Cloud service providers maintain the backend. They provide large-scale data storage, which is an important feature. Furthermore, using virtual machines and deploying models on servers are critical components of modern computing infrastructure., and more. [3]

A. Cloud Deployment Models

Private cloud is specifically built for one organization. The organization can choose to host the cloud infrastructure in its own data center on-premises or opt for a cloud service provider who would provide a dedicated infrastructure for theorganization.

Public cloud is a type of cloud computing model in which computational resources like servers, storage, and networking, are offered to the public by a third-party provider via the internet. Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) are among the most prominent public cloud providers. It is based on subscription service to users who wish to use it.

Hybrid cloud is type of cloud in which both public and private cloud elements are combined in a computing environment. In this configuration, companies usually use a combination of infrastructure located on-site, private cloud services, and public cloud services from various providers. Cloud delivery models:

1) Infrastructure as a Service (IaaS)- In the Infrastructure as a Service (IaaS) model, the cloud provider manages IT infrastructures such as storage, servers, and networking resource and makes them available to subscriber companies via virtual computers that can be accessed via the internet. IaaS could provide businesses with a number of advantages, including reduced costs, increased flexibility, streamlined processes, and accelerated workloads. Examples include Amazon (EC2), Google Compute Engine (GCE), and Rackspace.

2) Software as a Service (SaaS)- The most extensively utilized service is when software applications are made available over the internet in a ready-to-use state. Individuals use the application via a web browser or mobile app without authority over the underlying infrastructure or operating system. SaaS applications generally have prices determined by a subscription model.
Office365, Salesforce, and Zoom are some examples of significant providers.

3) Platform as a Service (PaaS)- Platform-as-a-service (PaaS) is a cloud computing model in which a third party provides an application software platform. A PaaS, designed primarily for developers and programmers, enables users to create, run, and manage their own apps without having to construct and maintain the infrastructure or platform that is often involved with the process.

Community clouds are utilized by a specific group of organizations within a community. It is a type of cloud infrastructure that allows numerous businesses to share resources and services based on common operational and regulatory needs.

Multi-cloud, which is utilized by multiple organizations that share common interests, needs, or issues. Community clouds are designed to cater to the requirements of a group of users, such as government agencies, healthcare, educational institutions, or businesses in a specific industry, unlike public clouds serving multiple organizations or private clouds dedicated to a single organization.

B. Cloud Service Model

In cloud computing, both the cloud service provider and the customer must share responsibilities for security controls. The data to be migrated to the cloud involves the adoption of the shared responsibility model for protecting data.

Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Data	Customer responsibility	Customer responsibility	Customer responsibility
Application	Customer responsibility	Customer responsibility	Cloud provider responsibility
Operating system	Customer responsibility	Cloud provider responsibility	Cloud provider responsibility
Virtualization	Cloud provider responsibility	Cloud provider responsibility	Cloud provider responsibility
Servers	Cloud provider responsibility	Cloud provider responsibility	Cloud provider responsibility
Storage	Cloud provider responsibility	Cloud provider responsibility	Cloud provider responsibility
Network	Cloud provider responsibility	Cloud provider responsibility	Cloud provider responsibility
Physical	Cloud provider responsibility	Cloud provider responsibility	Cloud provider responsibility

Fig. Shared Responsibility Model

Major cloud companies spend billions of dollars on data centre maintenance, security services, and training their employees to quickly identify and address security concerns. Many organizations do not dedicate enough resources to properly maintaining their on-premises data centres, which require significant investment, attention, and expertise. If any hyper-scale cloud provider experiences a security breach, trust in cloud providers will diminish, resulting in a loss of business for them.
Cloud security enables our organization to achieve enhanced data protection, improved regulatory compliance, business continuity, and disaster recovery.
Secure cloud architecture for organizations to strengthen the security is required to prevent security breaches from happening. [4]

III. LITERATURE REVIEW

A. Adoption

Ratnakumari Challah and Kanusu Srinivasa Rao discuss the various services provided by cloud computing, such as PaaS, SaaS, and IaaS, which are crucial for developing applications and utilizing data centers efficiently. It offers additional services, providing dynamically scalable resources over the Internet. [6]

This research [5] conducted by Chen and colleagues (2016) investigates the advantages of cloud computing as seen through the lens of business. It takes an investigative method to grasp how companies view the benefits of cloud computing and how factors such as the type of cloud service and value chain activity impact these views. Chen and Zhao state that security concerns are a primary reason why big businesses are reluctant to move their information to the cloud.

Alharthi, Yahya, Walters, and Wills discuss the major adoption challenges in adopting the cloud. They find that the main issue with the cloud is ensuring data security and privacy. [7]

B. Security Issues

The Cloud Security Alliance (CSA) and the European Network and Information Security Agency (ENISA) [8] are two bodies working to create awareness on various security issues in the cloud. They regularly publish reports and guidelines for security guidance.

Various papers, including Joshi et al. [9], highlight that the primary concern in information security and cloud computing is attacks and threats.

Adeel [10] discusses vulnerabilities and top threats that raise several security concerns in cloud computing.

Kumar's et al. [11] paper discusses security concerns in cloud computing. Their study focuses specifically on identifying information security challenges and explores various methods for protecting data and privacy.

C. Mitigation Proposals

Mohamed [12] suggested an improved security model for cloud computing that emphasizes protecting data both in transit and at rest. The algorithm, through padding, salting, hashing, and encryption, produces a larger encrypted message that is nearly impossible to decipher or crack.

Similarly, Chauhan [13] proposes a security model through the cryptographic algorithm AES 256 with stenography. It is suggested that this model will not only be much harder to crack but will also save time in uploading and downloading text contents.

IV. THREATS AND ATTACKS

A. Few Types of Threats

1) Data Breaches

A data breach occurs when information is revealed that was not intended to be made public. Data breaches may occur because of a targeted attack. The primary impact of data breaches is the loss of customer faith in the firm.

2) Account Hijacking

Account hijacking occurs when hostile individuals acquire unauthorized access to crucial or confidential accounts and use them for their own benefit. Phishing, unauthorized access to cloud servers, or stolen login credentials could all lead to the compromise of these accounts. These diverse and powerful threats can cause considerable disruption to the cloud environment, resulting in data loss, asset compromise, and stopped operations.

3) Insider Threat

An insider threat is when people within a company, like staff, vendors, or collaborators, abuse their access and permissions to damage the organization's information, technology, or activities. Insider threats can cause the loss of sensitive information and intellectual property. Insider dangers can result from both purposeful and unintentional actions.

4) Identity Theft

Identity theft happens when thieves obtain unauthorized access to a person's or business's cloud account login credentials. Their ability to mimic the genuine user and gain unauthorized access to confidential data or carry out malicious activities in the cloud environment is made possible by their stolen identity.

5) IAM Mismanagement

Identity federation, SSO, and MFA are examples of security techniques that help guarantee safe user access and lower the possibility of unwanted access. To guarantee that users and applications can only access the resources and data that are required in accordance with the principle of least privilege, IAM platforms provide comprehensive access controls and authorization rules.

6) Misconfigurations

Misconfiguration occurs when errors are made during the setup or management of cloud resources. These mistakes may result in weak areas that hackers may exploit to gain unauthorized access to information or systems.

A. Few Types of Attacks

1) DDoS Attacks

During a DDoS attack, the attacker floods the cloud service with so much traffic that it overflows its capacity and is inaccessible to authorized users. This can lead to a disruption in operations and result in downtime. [14]

2) Man-in-the-Middle Attacks

Man-in-the-Middle Attacks happen when a hacker positions themselves between two parties to intercept their communication and data exchange to conduct unauthorized actions like hacking or online shopping. These attacks take advantage of weaknesses in network, web, or browser security protocols to redirect genuine traffic and pilfer information from targets. [15]

3) Malware Injection

The process of malware injection includes the insertion of harmful software into the cloud infrastructure or applications. Once activated, malware can propagate throughout the cloud system, undermine data security, and interrupt regular activities. Phishing attacks, insecure APIs, and unpatched vulnerabilities are typical vectors for malware injection.

4) SQL Injection

Attacks in cloud computing entail inserting malicious SQL code into an application to take advantage of weaknesses and obtain unauthorized access to databases or cloud resources. Perpetrators can utilize SQL Injection to carry out commands, access confidential information, alter transactions, or even achieve administrator access to systems in cloud environments.

5) Phishing Attack

Phishing is a common cyber danger that focuses on cloud networks by using misleading emails, websites, or messagesto deceive users into disclosing sensitive data, downloading malware, or clicking on harmful links. These cyber-attacks may result in serious outcomes like data breaches, identity theft, ransomware, or denial-of-service attacks. [16]

Attack type	Effects	Mitigation Techniques
DDoS Attack	-Overwhelms cloudinfrastructure with excessive traffic - Disrupts service availability for legitimateusers - May result in monetary losses and harm to one's reputation	- Provision adequate bandwidth and computingresources to handle trafficspikes - Put DDoS mitigation and detection systems in place
(MITM) Attacks	-Enables the attacker to intercept and alter communication between the client and cloud service. - May result in databreaches, account takeovers, and other harmful activities	-Utilize end-to-end encryption (such as HTTPS) for all interactions with cloud services. reliable techniques for authentication, like multi-factor authentication. - Observe network traffic to spot any odd activity.

Malware Injection	-Enables a malicious actor to run harmful code on cloud systems. - Could cause data breaches, system compromise, andadditional attacks	- Make sure strong antivirus and anti-malware protections are in place for every cloud instance . -Frequently conduct scans on cloud resources to detect both familiar and unfamiliar malware. -Make sure that the most recent security fixes are routinely applied to cloud software and its dependencies**.**
SQL Injection	-Permits the attacker to run harmful SQL queries on cloud-based databases. - Can result in data breaches, data tampering, and system vulnerability.	Employ parameterized queries and prepared statements forcommunicating with databases. -Apply validation and sanitization measures to all dataprovided by users.
Phishing Attacks	-Tricks users into revealing login credentials or other sensitive information. - Can lead to compromised accounts, breaches of data, and further cyber attacks	Train staff on how to recognize and report phishing scams. -Enable multi-factor authentication for every cloud account.

Table 2. Mitigating Different Attacks in the Cloud

V. DEALING WITH THREATS

Proactive measures to deal with the threats are discussed in this section

1) Identity and Access Management (IAM)

Identity and Access Management (IAM) in cloud computing includes controlling user access to cloud resources. Verification, authorization, accountability, rules, and tracking are all part of it for safe and authorized entrance. Access control management ensures that data can only be accessed by those who are authorized. Among the components of IAM are Single Sign-On (SSO), Multi-Factor Authentication (MFA), and Role-Based Access Control (RBAC).

2) Encryption Techniques

Methods of encryption like AES (Advanced Encryption Standard) are commonly used for securing data before storing it to prevent unauthorized people from decoding it without the encryption key, even if they gain access to the storage device. Network data is frequently encoded using the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols.

3) Firewalls

Public cloud firewalls are digital network security tools that are utilized in public cloud environments. They offer featurescomparable to hardware firewalls but have benefits in scalability, availability, and extensibility, particularly in hybrid cloud setups. Public cloud firewalls provide security for software-defined environments, protect private cloud assets, and deliver advantages such as simple scalability, strong availability, and effective threat response, including defense from bandwidth-consuming threats such as DDoS attacks.

4) Systems for detecting and preventing unauthorized access or security breaches.

Cloud security solutions utilize proactive monitoring, threat detection, access controls, encryption, and incident response methods to protect against unauthorized access and security breaches. Cloud Security Incident and Event Management (SIEM) platforms, along with Security Orchestration, Automation, and Response (SOAR) tools, and incident response teams, are essential in coordinating response activities, examining security incidents, and bringing operations back to normal.

5) Backup and Recovery

The practice of storing client data off-site for security purposes within an organization's IT policy is known as Backup. Customers need to regularly perform audits to confirm adherence to the set protocols and guarantee the efficiency and thorough evaluation of their recovery strategy. Cloud-based backup and disaster recovery options offer scalability, cost-effectiveness, and geographical redundancy to protect data and ensure quick restoration in case of disasters. It is the sole responsibility of organizations to implement backup solutions.

VI. CONCLUSION

Most companies are now shifting to cloud services to store their data because of the overwhelming benefits they offer. Still, we cannot ignore the risk factors and security concerns. The paper briefly discussed carious types of threats and attacks that can affect cloud resources and services. Various security architectures and guidelines by NIST and CFA were advised to be followed. The security needs of clients and mitigation proposals were looked at in the literature review of various journals and papers. The mitigation techniques discussed are viable for maintaining a trustworthy cloud environment.

.

REFERENCES

[1] Eric, D., Simmon. (2018). Evaluation of Cloud Computing Services Based on NIST SP 800145. doi:10.1002/HTTPS://DX.DOI.ORG/10.6028/NIST.SP.500-322.

[2] (2023). Cloud Security Governance Guidelines. doi:10.14293/pr2199. 000062.v1

[3] S. B. Mallisetty, G. A. Tripuramallu, K. Kamada, P. Devineni, S. Kavitha and A. V. P. Krishna, "A Review on Cloud Security and Its Challenges," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2023, pp. 798-804, doi: 10.1109/IDCIoT56793.2023.10053520.

[4] Biniam, Fisseha, Demissie., Silvio, Ranise. (2021). Assessing the Effectiveness of the Shared Responsibility Model for Cloud Databases: the Case of Google's Firebase. 121-131. doi: 10.1109/SMDS53860.2021.00026

[5] Chen, T., T.-T. Chuang, and K. Nakatani The Perceived Business Benefit of Cloud Computing: An Exploratory Study CSUSB ScholarWorks <https://scholarworks.lib.csusb.edu/jitim/vol25/iss4/7/>.,

[6] Ratnakumari, Challa., Kanusu, Srinivasa, Rao. (2022). Services of cloud computing. International Research Journal of Modernization in Engineering Technology and Science,
doi: 10.56726/irjmets31489

[7] Alshdadi, Abdulrahman & Yahya, Fara & Wills, Gary & Walters, Robert. (2015). An Overview of Cloud Services Adoption Challenges in Higher Education Institutions. doi: 10.5220/0005529701020109.

[8] Cloud computing: benefits, risks and recommendations for information security ENISA

[9] M. Joshi, S. Budhani, N. Tewari and S. Prakash, "Analytical Review of Data Security in Cloud Computing," *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, London, United Kingdom, 2021, pp. 362-366, doi: 10.1109/ICIEM51511.2021.9445355.

[10] Javaid, A. Top Threats to Cloud Computing Security Social Science Research Network (2013) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325234> (DOI: 10.2139/ssrn.2325234)..

[11] Kumar, Ravi & Raj, Herbert & Perianayagam, Jelciana. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. Procedia Computer Science. 125. 691-697. 10.1016/j.procs.2017.12.089.

[12] (2023). An Improved End-to-End Data Security Approach for Cloud Computing. doi: 10.36227/techrxiv.23553489

[13] Shweta, Chauhan. (2023). Exploring Innovative Methods for Enhancing Data Security in Computing.doi:10.1109/ICSMDI57622.2023.00019

[14] Bojović, Petar & Basicevic, Ilija & Ocovaj, Stanislav & Popovic, Miroslav. (2019). A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method. Computers & Electrical Engineering. 73. 84-96. 10.1016/j.compeleceng.2018.11.004..

[15] Gupta, I., et al.. *Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions*. Jan. 2022, doi:10.1109/access.2022.3188110.

[16] Mittal, Sweta & R, Jayasimha. (2020). Detection of Phishing Attacks using Content Analysis in the Cloud. International Journal of Recent Technology and Engineering (IJRTE). 9. 2622-2625. 10.35940/ijrte.A3066.059120.