IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cloud Data Security

[1]Ashwini Chandalwar, [2]Pragati Chandekar,[3]Khushi Dorlikar, [4]Ashish Benjanin

[1, 2, 3, 4] Department of Computer Science Enigineering
Department Of Computer Science Engineering College
Rajiv Gandhi College of Engineering Search and Technology, Chandrapur.

ABTRACT:

Cloud data security refers to the set of procedures and technologies used to protect data that is stored, processed, and transmitted in cloud computing environments. Since data is stored on remote servers owned by third-party vendors, organizations must rely on cloud service providers (CSPs) to implement and maintain adequate security measures to protect their sensitive data. Some of the notable security challenges associated with cloud computing include unauthorized access, data breaches, data loss, data corruption, insider threats, and lack of visibility into cloud environments. To mitigate these risks, CSPs use a combination of encryption, authentication, access control, and monitoring tools to secure their clients' data. In addition to CSPs' efforts, organizations must also take measures to protect their data while it resides in the cloud. This includes implementing robust identity and access management (IAM) policies, data classification frameworks, and data retention policies. Organizations should also conduct regular audits and security assessments to identify vulnerabilities and mitigate risks that they may face. Overall, cloud data security requires a collaborative effort between CSPs and organizations to ensure that data is properly secured and protected in the cloud. With the right measures in place, organizations can reap the benefits of cloud computing without sacrificing security.

Keywords:1.Cloud computing 2. Cloud service provider (CSP)3. Data security 4. Access control

I. INTRODUCTION

Cloud computing has become a popular technology for businesses due to its many benefits, including scalability, cost efficiency, and flexibility. However, with businesses storing valuable data on the cloud, including sensitive customer information, it has become crucial to ensure cloud data security is a top priority. Improperly secured cloud infrastructure can lead to data breaches, data loss, and other critical security issues. Cloud data security refers to the measures taken to protect cloud-based data from unauthorized access, theft, or destruction. To ensure cloud data security, businesses must rely on cloud service providers (CSPs) to implement robust security measures, including encryption, access control, identity and access management (IAM), monitoring tools, and other practices.

II. LITERATURE SURVE

There are numerous security mechanism that have been proposed by different researchers. In thissection we will provide the literature survey of work done in this field.In 2011, Jan de Muijnck-Hughes proposed a security technique which is known as Predicate Based Encryption (PBE). PBE represents a family of asymmetric encryption and originates from IdentityBased Encryption [1]. This technique integrates Attribute Based Access Control (ABAC) withasymmetric encryption, thereby permitting a single encryptor/multi decryptor environment to berealized using a single scheme. This Predicate Based Encryption focuses its implementation at bothPlatform as a service and Software as a service. This proposed technique also precludes unwantedexposure, unwanted leakage and other unwanted breaches of confidentiality of cloud resident data.In 2011 Venkata Sravan et.al wrote a paper titled Security Techniques for Protecting Data in Cloud. Theaim of this paper is to understand the security threats and identify the appropriate security techniquesused to mitigate them in Cloud computing [2]. The research identified a total number of 43 securitychallenges and 43 security techniques. The most measured attribute is Confidentiality (31%) followedby Integrity (24%) and Availability (19%) [2] In 2011 Ali Asghary Karahroudy wrote a paper titled Security Analysis and Framework of CloudComputing with Parity Based Partially Distributed File System. This paper proposed a technique calledPartially Distributed File System with Parity (PDFSP) which is a protocol developed as a modificationon the existing GFS/HDFS [3]. This PDFSP has four main components; Client Access Machine, UserPublic Machine, Cloud Management Server and File Retrieval Server. All these components worktogether to ensure data being transmitted does not get into wrong hands. This paper addressed the threeaspects of security which are Confidentiality, Integrity and Availability. In 2013 Nabil Giweli proposed a solution based approach referred as Data Centric Security approach.This approach aims at providing security at the data level hence the data are self-describing, self-defending and self-protecting during their lifecycle in the cloud environments. This approach gives theentire responsibility to the data owner to set and manage the data privacy and security measures. Thisproposed solution is based on Chinese Remainder Theorem (CRT) and it utilizes symmetric andasymmetric encryption techniques. In this paper, the proposed solution is proven to be very efficient as7

it does not require complex key derivation methods and the data file does not need to be encryptedmore than once [4].In 2013 Miao Zhou outlined 5 techniques to provide security and integrity of data in cloud computing.These techniques include; Innovative tree-based key management scheme, Privacy enhanced dataoutsourcing in the cloud, Privacy preserved access control for cloud computing, Privacy enhancedkeyword search in clouds and Public remote integrity check for private data. This paper adopted Keyword Searching Mechanism which enables efficient multi-user keyword searches and hides theprivate information in the search queries [5]. An encryption scheme for a two-tier system was presentedto achieve flexible and fine-grained access control in the cloud.

III. METHODOLOGIES AND TECHNOLOGY

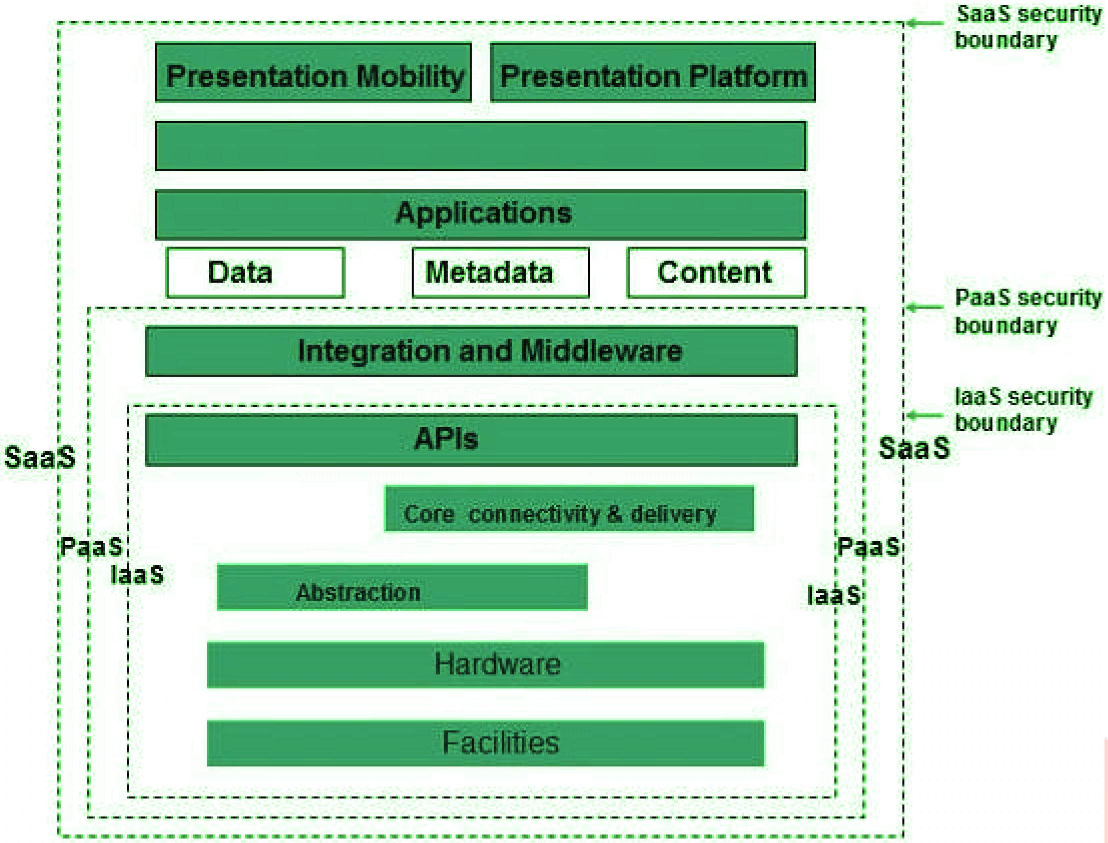
1. Risk Assessment: Identify potential risks that may affect business operations and define strategies to minimize or remove them.

2. Data Classification: Categorize data based on its sensitivity, value and the level of protection required. Classifying data helps to define the appropriate security and control measures that need to be implemented.

3. Encryption: Implement encryption techniques to protect data transmitted and stored in the cloud. Encrypting sensitive data keeps it secure from unauthorized access or attack. methodology for ensuring cloud data security typically follows a multi-layered approach to protect data from unauthorized access, theft, or destruction. Here are the general steps involved in the cloud data security methodology: Security of Cloud

Security Boundaries

The Cloud Security Alliance (CSA) stack model defines the boundaries between each service model and shows how different functional units relate. A particular service model defines the boundary between the service provider's responsibilities and the customer. The following diagram shows the CSA stack model:



Key Points to CSA Model

- IaaS is the most basic level of service, with PaaS and SaaS next two above levels of services.
- Moving upwards, each service inherits the capabilities and security concerns of the model beneath.
- IaaS provides the infrastructure, PaaS provides the platform development environment, and SaaS provides the operating environment.
- IaaS has the lowest integrated functionality and security level, while SaaS has the highest.
- This model describes the security boundaries at which cloud service providers' responsibilities end and customers' responsibilities begin.
- Any protection mechanism below the security limit must be built into the system and maintained by the customer.

Although each service model has a security mechanism, security requirements also depend on where these services are located, private, public, hybrid, or community cloud. data security

Since all data is transferred using the Internet, data security in the cloud is a major concern. Here are the key mechanisms to protect the data.

- access control
- audit trail
- certification
- authority

The service model should include security mechanisms working in all of the above areas.

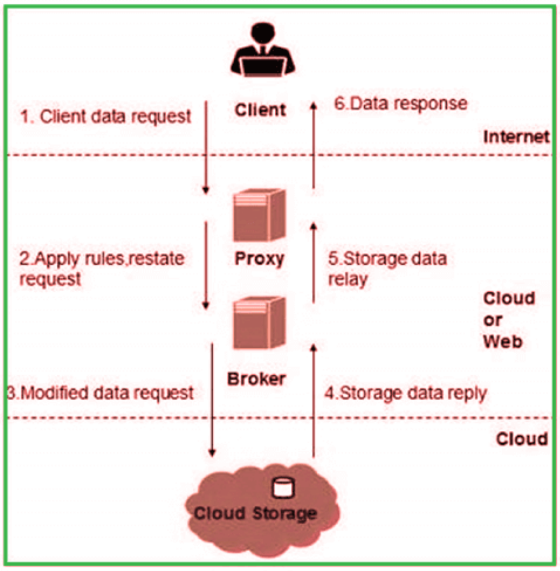
Separate access to data

Since the data stored in the cloud can be accessed from anywhere, we need to have a mechanism to isolate the data and protect it from the client's direct access.

Broker cloud storage is a way of separating storage in the Access Cloud. In this approach, two services are created:

1. A broker has full access to the storage but does not have access to the client.
2. A proxy does not have access to storage but has access to both the client and the broker.
3. Working on a Brocade cloud storage access system
4. When the client issues a request to access data:
5. The client data request goes to the external service interface of the proxy.
6. The proxy forwards the request to the broker.
7. The broker requests the data from the cloud storage system.
8. The cloud storage system returns the data to the broker.
9. The broker returns the data to the proxy.
10. Finally, the proxy sends the data to the client.

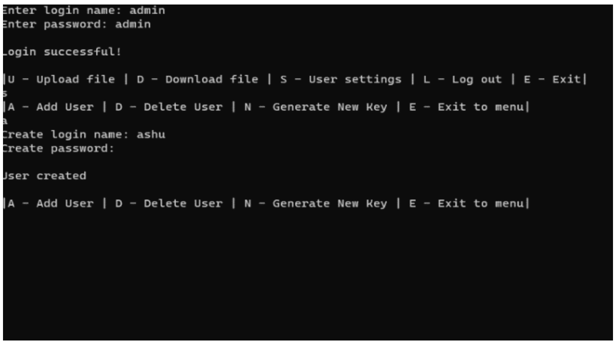
All the above steps are shown in the following diagram:



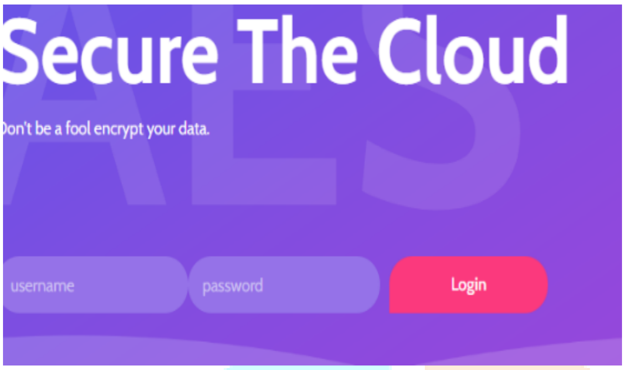
Encoding

Encryption helps to protect the data from being hacked. It protects the data being transferred and the data stored in the cloud. Although encryption helps protect data from unauthorized access, it does not prevent data loss.

Result:

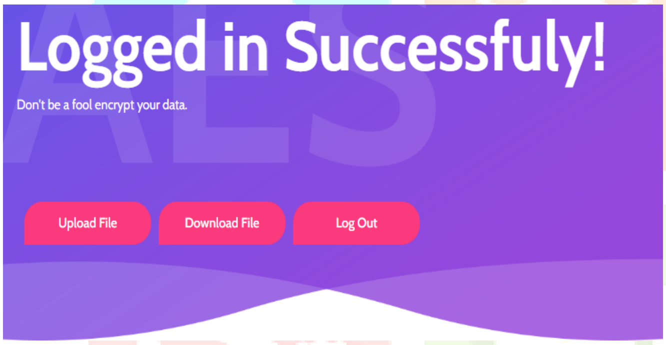


```
Enter login name: admin
Enter password: admin

Login successful!

|U - Upload file | D - Download file | S - User settings | L - Log out | E - Exit|
s
|A - Add User | D - Delete User | N - Generate New Key | E - Exit to menu|
a
Create login name: ashu
Create password:

User created

|A - Add User | D - Delete User | N - Generate New Key | E - Exit to menu|
```



Secure The Cloud

Don't be a fool encrypt your data.



Logged in Successfuly!

Don't be a fool encrypt your data.

IV. CHALLENGES AND LIMITETIOND

1. Data Breaches: Despite advanced security measures, breaches can occur due to vulnerabilities in cloud infrastructure or misconfigured settings, leading to unauthorized access to sensitive data.

2. Compliance and Regulations: Adhering to various data protection regulations (like GDPR, HIPAA) across different regions can be challenging, as cloud providers must ensure compliance while serving diverse clients.

3. Shared Responsibility Model: Understanding the division of security responsibilities between the cloud service provider and the user is crucial. Misinterpretation or misunderstanding of these responsibilities can lead to security gaps.

4. Data Loss: Factors like accidental deletion, data corruption, or service provider outages can result in data loss, emphasizing the need for robust backup and recovery strategies.

5. Encryption Challenges: Encrypting data both in transit and at rest is essential. However, managing encryption keys securely and consistently across various cloud services can be complex.

6. Identity and Access Management (IAM): Managing user access, permissions, and authentication protocols across multiple cloud environments requires robust IAM solutions to prevent unauthorized access.

7. Vendor Lock-In: Switching between cloud service providers can be challenging due to differences in data formats, proprietary technologies, and dependencies, leading to potential vendor lock-in.

Addressing these challenges involves employing a combination of strong encryption practices, robust access controls, regular security audits, and continuous monitoring to protect data in the cloud.

Cloud data security refers to the set of procedures and technologies used to protect data that is stored, processed, and transmitted in cloud computing environments. Since data is stored on remote servers owned by third-party vendors, organizations must rely on cloud service providers (CSPs) to implement and maintain adequate security measures to protect their sensitive data . Some of the notable security challenges associated with cloud computing include unauthorized access, data breaches, data loss, data corruption, insider threats, and lack of visibility into cloud environments. To mitigate these risks, CSPs use a combination of encryption, authentication, access control, and monitoring tools to secure their clients' data . In addition to CSPs' efforts, organizations must also take measures to protect their data while it resides in the cloud. This includes implementing robust identity and access management (IAM) policies, data classification frameworks, and data retention policies. Organizations should also conduct regular audits and security assessments to identify vulnerabilities and mitigate risks that they may face . Overall, cloud data security requires a collaborative effort between CSPs and organizations to ensure that data is properly secured and protected in the cloud. With the right measures in place, organizations can reap the benefits of cloud computing without sacrificing security.

V. IMPLEMENTATION AND EXPERIMENT

Implementing and experimenting with cloud data security involves several key steps and practices:

1. Encryption: Utilize encryption techniques to protect data both in transit and at rest. Experiment with different encryption methods (e.g., AES, RSA) to find the most suitable ones for your specific data and applications.

2. Access Control: Implement robust access controls and authentication mechanisms. Experiment with multi-factor authentication (MFA) and role-based access control (RBAC) to limit access based on user roles and permissions.

3. Data Classification: Experiment with data classification tools to categorize data based on sensitivity. Apply different security measures based on the classification level to ensure appropriate protection.

4. Security Protocols: Test and implement secure communication protocols (e.g., SSL/TLS) to safeguard data during transmission between users and the cloud environment.

5. Security Monitoring: Deploy monitoring tools to track and analyze system logs, user activities, and potential security threats. Experiment with security information and event management (SIEM) solutions for real-time threat detection.

6. Backup and Recovery: Develop and test backup and recovery strategies regularly to ensure data availability in case of data loss or system failure. Experiment with different backup methods (e.g., incremental, differential) to optimize data recovery.

7. Compliance Adherence: Experiment with compliance automation tools to ensure adherence to relevant data protection regulations and industry standards. Test compliance checks and audits to maintain regulatory compliance.

8. Training and Awareness: Conduct security awareness programs and training sessions for employees to educate them about best practices and potential security threats associated with cloud data.

9. Incident Response Plan: Develop and experiment with an incident response plan to effectively respond to security incidents or breaches. Regularly test the plan through simulations and drills.

By implementing these practices and conducting experiments to test their effectiveness, organizations can strengthen their cloud data security posture and better protect sensitive information stored and processed in the cloud. Regular evaluation and adaptation of security measures are essential to stay ahead of evolving threats.

VI. CONCLUSION

Cloud Computing is the delivery of computing services; servers, storage, databases, networking, software, analytics, intelligence and more over the internet to offer faster innovation, flexible resourcesand economies of scale. Cloud computing is an emerging social phenomenon that is been patronize byindividuals almost every day. For any important emerging technology, it comes with its own issues thathinder its adoption. Currently, cloud computing is seen as a fast developing area that can instantlysupply extensible service by using internet with the help of hardware and software virtualization.[12]The phenomenon of Cloud Computing is very promising which ensures businesses increase efficiency alongside reducing their cost of production. Data protection and security in cloud computing is stillcrawling on its knees and needs more research attention although it has been deployed and used inproduction environment.[11]Data Security in Cloud Computing is an important area that should be given much attention.

VII. FUTURE SCOPE

Future cloud data security will likely continue to evolve with advancements in encryption techniques, zero-trust architectures, AI-driven threat detection, and enhanced identity and access management systems. Technologies like homomorphic encryption, secure multi-party computation, and decentralized storage may also play pivotal roles in ensuring stronger data protection in the cloud. As cyber threats evolve, so will security measures, aiming to provide robust defense mechanisms to safeguard sensitive data stored and processed in cloud environments.

ACKNOWLEDGMENT

I would like to express my profound gratitude to Dr. Nitin Janwe (H.O.D.), of CSE department, and Mrs. Madhavi Sadu (Mini Project Incharge) for their contributions to the completion of my project “Cloud Data Security".

I would like to express my special thanks to our mentor Dr. Devashri Kodgire for her time and efforts she provided throughout the semester. Your useful advice and suggestions were really helpful to us during the project’s completion. In this aspect, I am eternally grateful to you.

I would like to acknowledge that this project was completed entirely by us and not by someone else.

Your name

Ashwini Chandalwar

Pragati Chandekar

Khushi Dorlikar

Ashish Benjamin

VIII. REFERENCES

1. http://www.ru.nl/ds

2. https://www.bth.se/com