WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Ensuring Data Privacy and Security with Automated Storage and Retrieval on AWS Cloud

Mr. K. Arun Kumar[1], Mr. C. Jeganathan[2], Raghul Bharathi M[3], Sangeerth Shiam A[4], Subishkumar S[5]

[1]Assistant Professor Department of Computer Science, Rathinam College of Arts and Science, arunkumar.inurture@gmail.com
[2]Assistant Professor Department of Computer Science, Rathinam College of Arts and Science, jegan.chinna@gmail.com
[3,4,5]B. Sc Computer Science Specialization with Cloud Technology and Information Security Rathinam College of Arts and Science, Coimbatore, Tamil Nadu [3]raghulbharathi2410@gmail.com, [4]gmsangeerthsan10@gmail.com , [5]subish2subi@gmail.com

ABSTRACT

Ensuring data privacy and security is a critical concern for organizations that rely on cloud computing. With the rise of data breaches and cyber attacks, it is essential to implement robust security measures to protect sensitive data. The AWS Cloud provides a powerful platform for storing and retrieving data, but it is crucial to ensure that security protocols are in place to safeguard against unauthorized access.Automated storage and retrieval systems can help to streamline the process of managing data on the cloud while also enhancing security. By automating tasks such as backup and recovery, organizations can reduce the risk of human error and improve the reliability of their data storage systems. In addition, automated systems can provide real-time monitoring and alerting, enabling rapid response to potential security threats.This project explores how automated storage and retrieval systems can be implemented on the AWS Cloud to ensure data privacy and security. We examine the various security measures provided by AWS, such as encryption, access control, and auditing, and how they can be leveraged to protect sensitive data. Additionally, we explore how automation can be used to enhance security and simplify the management of data storage and retrieval.

I. INTRODUCTION

Ensuring data privacy and security is a critical concern for organizations that rely on cloud computing. With the rise of data breaches and cyber attacks, it is essential to implement robust security measures to protect sensitive data. The AWS Cloud provides a powerful platform for storing and retrieving data, but it is crucial to ensure that security protocols are in place to safeguard against unauthorized access.Automated storage and retrieval systems can help to streamline the process of managing data on the cloud while also enhancing security. By automating tasks such as backup and recovery, organizations can reduce the risk of human error and improve the reliability of their data storage systems. In addition, automated systems can provide real-time monitoring and alerting, enabling rapid response to potential security threats.This project will explore how automated storage and retrieval systems can be implemented on the AWS Cloud to ensure data privacy and security. We will examine the various security measures provided by AWS, such as encryption, access control, and auditing, and how they can be leveraged to protect sensitive data. Additionally, we will explore how automation can be used to enhance security and simplify the management of data storage and retrieval.Overall, this project aims to provide a comprehensive overview of the best practices and tools for ensuring data privacy and security on the AWS Cloud through automated storage and retrieval systems. By implementing these measures, organizations can reduce the risk of data breaches and protect their sensitive information, ultimately enabling them to operate with greater confidence in the cloud

II. METHODOLOGY

Background study:

We begin by conducting a comprehensive review of the existing literature on IPMCDP, multi-cloud storage, and related concepts such as data integrity and security. Identify the gaps in the current research and identify potential research questions that could be addressed in our project**.**

Problem formulation:

Clearly define that research problem we will address in our project,and formulate research questions that we will answer to address this problem. The research problem could be related to improving the efficiency and security of IPMCDP in multi-cloud storage,for instance.

Design and implementation:

Based on the research questions formulated in the previous step, design a methodology for implementing IPMCDP in multi-cloud storage. This will involve selecting appropriate algorithms and data structures, defining the overall system architecture, and outlining the implementation plan.

Testing and evaluation:

Once the implementation is complete, evaluate the performance of the system. This can be done by testing the system against various data sizes and storage scenarios, evaluating the efficiency of the system, and measuring the accuracy of data possession proofs.

Analysis and validation:

Analyze the results obtained from the testing and evaluation, and validate the effectiveness of the IPMCDP solution in multi-cloud storage. Compare the solution against existing solutions and demonstrate its advantages and limitations.

Advantages :

Multicloud environments can help organizations improve their security and compliance capabilities, as they can choose the best security services from each provider and implement a multi-layered security approach. Additionally, by using multiple cloud providers, organizations can reduce the risk of a single point of failure or attack.One of the main advantages of multicloud is that it allows organizations to avoid being locked into a single cloud vendor. By using multiple cloud providers, organizations can choose the best services from each provider and switch between providers as needed.

System Design:

The client application is responsible for uploading and retrieving data from the cloud servers. The client application uses an identity-based encryption (IBE) scheme to generate a set of public and private keys, and to encrypt the data before uploading it to the cloud servers. The client application also generates a set of random challenges and sends them to the cloud servers to verify the integrity of the data copies.

Fig.2.1 Overview of Proposed System

Sequential Model User identification:

The user attempting to access the data must first be identified using their credentials or other forms of authentication. Cloud selection: The user must select which cloud storage provider they wish to access the data from. This could be based on factors such as proximity, cost, or security. Data retrieval: Once the user is authenticated and the cloud storage provider is selected, the data can be retrieved from the storage provider. Data processing: If the data needs to be processed in some way, such as by a machine learning algorithm, this can be done using the resources provided by the selected cloud storage provider. Data storage: Once the data processing is complete, the processed data can be stored back in the cloud storage provider, either in the same location or in a different one, based on the user's preference. Data sharing: The user can then share the processed data with others as needed, either within the same cloud storage provider or with other cloud storage providers.

III. Experimental Setup

Proposed System:

A proposed system for ensuring data privacy and security with automated storage and retrieval on AWS Cloud could include the following components: Data Encryption: All data stored on AWS Cloud should be encrypted to ensure its confidentiality. The system can use AES 256-bit encryption, which is a strong encryption standard. Key Management: The system should also include a key management mechanism that stores and manages the encryption keys used to encrypt and decrypt data stored on AWS Cloud. Access Control: The system should implement access control mechanisms to ensure that only authorized users have access to the data. This can be done using IAM roles, policies, and groups. Monitoring and Logging: The system should monitor all activities and events related to the data stored on AWS Cloud. This can be done using AWS CloudTrail and Amazon CloudWatch.The system. AWS provides automated backup and recovery services like Amazon S3 Glacier and Amazon EBS Snapshots. Automation: The system should be automated using AWS services like AWS Lambda and AWS Step Functions. This can help in automating various tasks related to data management, such as data transfer, replication, and archiving. Compliance: The system should comply with relevant data privacy and security regulations

Choose cloud providers:

As with any multi-cloud setup, the first step is to choose cloud providers that meet the requirements of the PIR-MCDP setup. PIR-MCDP requires multiple cloud servers for storing multiple copies of data. We can choose popular cloud providers such as AWS, Microsoft Azure, Google Cloud, or IBM Cloud. We are running this project with the help of localhost. We have choosen AWS cloud servies.

Set up network connectivity:

After choosing cloud providers, the next step is to set up network connectivity between the clouds. This can be done through a VPN, direct connection, or interconnect. Network connectivity is essential to allow for data transfer and communication between the clouds.

Install required software:

Once the network connectivity is set up, the next step is to install the required software for PIR-MCDP. This can include the PIR-MCDP client software, server software, and cryptographic libraries.

IV. RELATED WORK

A survey on cloud data security and privacy" by Wei et al. (2020) - This paper provides an overview of the current state-of-the-art in cloud data security and privacy, including issues related to data protection, access control, and compliance. The authors also discuss various solutions and techniques that have been proposed to mitigate these challenges.

Data protection in cloud storage using cryptographic algorithms" by Kaur and Singh (2019) - This paper focuses on the use of cryptographic algorithms to secure data stored in the cloud. The authors compare various encryption and decryption techniques and highlight their strengths and weaknesses.

Secure data retrieval for decentralized disruption-tolerant military networks" by Akyildiz et al. (2020) - This paper proposes a secure and efficient data retrieval mechanism for decentralized military networks. The authors describe a scheme based on a hybrid encryption approach that uses both symmetric and asymmetric cryptography.

Ensuring the security of data storage in the cloud" by AWS (2021) - This technical article from AWS provides a detailed overview of the security features and best practices that AWS customers can use to protect their data in the cloud. The article covers topics such as data encryption, access control, monitoring, and compliance.

Automated data management for cloud storage systems" by Park et al. (2021) - This paper proposes an automated data management system for cloud storage that leverages machine learning techniques to optimize data placement, replication, and retrieval. The authors describe a prototype implementation of the system and evaluate its performance in a real-world cloud environment.

A study on security issues and challenges in cloud computing" by Chauhan and Singh (2020) - This paper provides an overview of the security issues and challenges in cloud computing, including data privacy and security concerns. The authors also discuss various security mechanisms and solutions that can be used to mitigate these challenges.

An efficient secure data retrieval mechanism for cloud storage systems" by Xu et al. (2019) - This paper proposes an efficient secure data retrieval mechanism for cloud storage systems that uses a homomorphic encryption technique. The authors describe a prototype implementation of the mechanism and evaluate its performance and security properties.

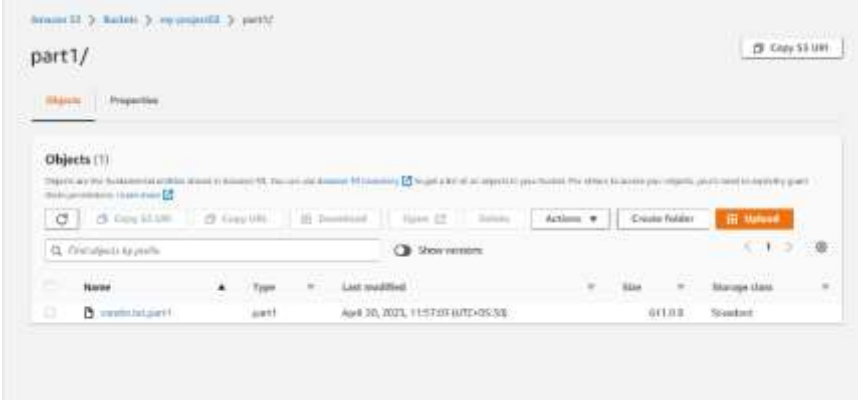
An efficient secure data retrieval mechanism for cloud storage systems" by Xu et al. (2019) - This paper proposes an efficient secure data retrieval mechanism for cloud storage systems that uses a homomorphic encryption technique. The authors describe a prototype implementation of the mechanism and evaluate its performance and security properties.

A comprehensive survey on security and privacy issues in cloud computing" by Kshetri (2019) - This paper provides a comprehensive survey of security and privacy issues in cloud computing, including data privacy and security concerns. The author also discusses various security mechanisms and solutions that can be used to address these challenges.

A novel framework for secure data storage and retrieval in cloud computing" by Jafarzadeh et al. (2021) – This paper proposes a novel framework for secure data storage and retrieval in cloud computing that uses a combination of access control, encryption, and key management techniques. The authors also describe a prototype implementation of the framework and evaluate its performance in a cloud environment

OUTPUT:

Fig2.2 Splitting and Uploading a data to cloud storage



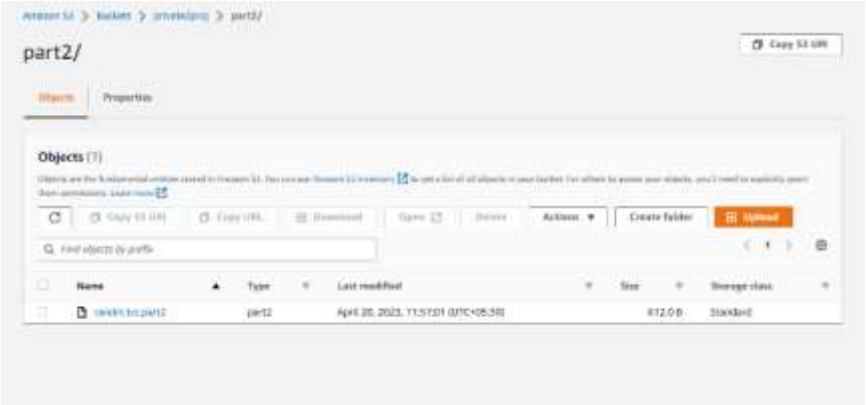


Fig2.3 Merging and Retrieved Data

V. RESULTS AND DISCUSSION

Improved Security: Multi-cloud enables the user to prove the possession of multiple copies of their data stored in multiple clouds, while ensuring the confidentiality and integrity of the data. This provides a higher level of security compared to traditional data storage solutions in multi-cloud environments.

Increased Efficiency: Multi-cloud leverages hash functions to reduce the computational overhead of verifying data possession. This can significantly increase the efficiency of the system, especially when dealing with large data sets.

Greater Flexibility: Multi-cloud enables the user to choose the number of cloud servers and the distribution of data copies among them. This provides greater flexibility and customization options for users, allowing them to tailor the system to their specific needs.

VI. CONCLUSION

In this paper, we have presented a module design and described the different modules of the proposed Multi-cloud system. We have also discussed the advantages and limitations of Multi-cloud, as well as potential future work in this area. Some of the key advantages of Multi-cloud include improved security, efficiency, and flexibility, while some of the limitations include network latency, setup complexity, key management overhead, and storage overhead. Multi-cloud is a rapidly evolving area of research, and further research and development in this area can lead to more efficient, secure, and

practical systems for multi-cloud data storage. Multi-cloud has the potential to benefit many organizations and users by providing a secure and efficient solution for storing and retrieving their data in multi-cloud environments.

VII. FUTURE WORK

Dynamic data support:

Most existing Multi-cloud systems assume that the data stored in the cloud remains static, and do not address the problem of dynamic data changes. Future work could explore the use of more flexible schemes that can handle dynamic data updates while maintaining the security and efficiency of the system.

Privacy preservation:

Multi-cloud schemes rely on the assumption that the cloud servers are honest and do not collude to leak data. Future work could focus on developing schemes that provide better privacy guarantees even in the presence of malicious cloud servers

REFERNCES

1. Efficient Identity-based Provable Multi-Copy Data Possession in Multi-Cloud Storage, IEEE 2020
2. Data Consistency in Multi-Cloud Storage Systems With Passive Servers and Non-Communicating Clients, IEEE 2020
3. Multi-Replica and Multi-Cloud Data Public Audit Scheme Based on Blockchain, IEEE 2020
4. Provable data possession based Multi-Cloud Storage Security, IEEE 2020
5. "Cloud computing and emerging IT platforms: Vision, hype,and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, no. 6, pp.599-616,2019.
6. "Flexible and fine-grained attribute-based data storage in cloud computing," IEEE Trans. Service Compute., 2020, 10(5): 785-796.
7. "Fine-grained two-factor protection mechanism for data sharing in cloud storage," IEEE Trans. Information Forensics and Security, vol. 13, no 1, pp. 186-196, 2019
8. "User collusion avoidance CP-ABE with efficient atribute revocation for cloud storage, " IEEE Systems Journal, 2017, DOI:10.1109/JSYST.2017.2667679.
9. "KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage," IEEE Trans. Service Compute., vol. 10, no. 5, pp. 715-725, Sept.-Oct. 2019.
10. "White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 76-88, 2020
11. "Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage," International Journal of Communication Systems, vol. 30, no. 1, Art. no. e2942, Jan. 2021.
12. "Key-policy attribute-based encryption against continual auxiliary input leakage," Information Sciences, 2019, 470: 175–188
13. "Privacy preserving personal health record using multi-authority attribute-based encryption with revocation," Int. J. Inf. Secure., vol. 14, no. 6, pp. 487-497, 2020