International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 3, pp 137-140, March-2024

https://doi.org/10.47001/IRJIET/2024.803017

Efficiently Managing Storage across Different Cloud Services for Flexible Resource Allocation and Security Integration

[1]R. Nithin, [2]Dr. R. Nagarajan

[1]Student of PG & Research, Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore, Tamilnadu, India

[2]Professor of PG & Research, Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore, Tamilnadu, India

***Abstract* - In the modern landscape, exploiting multiple cloud services stands out as a potent strategy for enhancing both data privacy and accessibility. Our research delves into the cost-effective shift towards multi-cloud storage computing, with a key emphasis on seamlessly integrating on-demand resource provisioning and robust access control policies. By fragmenting datasets across diverse cloud platforms, we bolster privacy while adeptly managing complexities through cutting-edge Multi-Cloud technologies. Our approach dynamically allocates resources and enforces stringent access controls, thus optimizing security and resource utilization. This framework adeptly tackles the challenges associated with managing diverse cloud environments, offering organizations a comprehensive solution for secure and efficient data management in the multi-cloud era.**

Keywords: Multi-cloud computing, Data privacy, Accessibility, Cost-effectiveness, Resource provisioning, Access control policies, Data fragmentation, Security optimization, Resource utilization, Multi-cloud technologies.

I. INTRODUCTION

In the evolving landscape of cloud computing, the rise of data volume and security demands has spurred interest in innovative storage strategies. Multi-cloud storage computing, distributing data across multiple platforms enhances privacy and accessibility. Our research focuses on cost-effective implementation, dividing datasets for efficiency while integrating resource provisioning and access control. We aim to provide a streamlined framework for organizations, optimizing data management amidst the complexities of the multi-cloud era.

1.1 Literature Survey

Related work in the field provides valuable insights into cost-effective practices in single to multi-cloud storage computing environments. By synthesizing existing research, it identifies key methodologies and advancements in resource provisioning and access control policy integration. Future research directions may include the development of comprehensive cost optimization frameworks, the exploration of emerging technologies such as serverless computing, and the investigation of environmental sustainability considerations in cloud storage economics.

Bhardwaj. A. et al [1] introduce the Capturing-the-invisible (CTI): Behavior-based attacks recognition in IoT-oriented industrial control systems in 2020.This research focuses on the use of process analytics to detect attacks in industrial control infrastructure systems and compares the effectiveness of signature-based detection methods.

Kumar. M., et al [2] implement Image forensics based on lighting estimation. International Journal of Image and Graphics in 2019.By assessing the lighting parameters, the proposed technique identifies the manipulated object and returns angle of incidence w.r.t light source direction.

A cloud data de-duplication scheme based on certificateless proxy re-encryption, as in [3]. (2019) Xiaoyu Zheng, Yuyang Zhou, Yalan Ye, Fagen Li.

A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era, as in [4]. (2019) SI HAN, KE HAN, AND SHOUYI ZHANG.

Intelligent Secure Storage Mechanism for Big Data, as in [5]. (2021) K.R. Remesh Babu, K.P. Madhu.

Securing IoT-Empowered Fog Computing Systems: Machine Learning Perspective, as in [6]. (2022) Tariq Ahamed Ahanger, Usman Tariq, Atef Ibrahim, Imdad Ullah, Yassine Bouteraa and Fayez Gebali.

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 8, Issue 3, pp 137-140, March-2024
https://doi.org/10.47001/IRJIET/2024.803017

Data Distribution Optimization over Multi-Cloud Storage, as in [7]. (2022) Saif Saad Alnuaimi, Elankovan A Sundararajan , And Abdul Hadi Abd Rahman.

Perceived Security Risk Based on Moderating Factors for Blockchain Technology Applications in Cloud Storage to Achieve Secure Healthcare Systems, as in [8]. (2022) Malik Mustafa, Marwan Alshare, Deepshikha Bhargava, Rahul Neware , Balbir Singh, and Peter Ngulube.

A Systematic Literature Review on Blockchain-Enabled Federated Learning Framework for Internet of Vehicles, as in [9]. (2022) Mustain Billah, Sk. Tanzir Mehedi, Adnan Anwar, Ziaur Rahman, Rafiqul Islam.

An Intelligent and Secured Privacy-Preserving Framework for Wireless Body Area Networks (WBANs), as in [10]. (2022) Muhammad Shoaib Akhtar, Tao Feng.

II. METHODOLOGY

The proposed system aims to address the growing need for cost-effective and secure single to multi-cloud storage computing solutions, with a particular focus on on-demand resource provisioning and access control policy integration. At its core, the system employs Multi- Cloud technologies to divide a single data set into smaller fragments and distribute them across multiple cloud platforms. This fragmentation enhances data privacy while leveraging the benefits of multi-cloud environments. To overcome the complexities associated with managing diverse cloud accounts and communication channels, the system utilizes an edge device as a centralized management hub. This device streamlines the orchestration of data storage and communication across various clouds, thereby optimizing resource utilization and reducing operational overhead. Central to the proposed system is its emphasis on data security. Robust access control policies are integrated seamlessly within the multi-cloud storage infrastructure to safeguard against unauthorized access and ensure compliance with data privacy regulations. By enforcing stringent access controls, the system ensures that only authorized users can access and manipulate the distributed data fragments. The proposed system offers a comprehensive solution for managing and securing data across a multi-cloud environment. By combining cost-effectiveness, scalability, and robust security measures, it addresses the evolving needs of organizations seeking to leverage multi-cloud storage computing while ensuring data privacy and integrity.

In the context of cloud data security, the integration of robust access control policies plays a pivotal role in safeguarding sensitive data and minimizing the risk of cyberattacks. Access control policies dictate who can access specific resources within the cloud environment and what actions they can perform on those resources. By effectively integrating access control policies, organizations can enforce granular permissions, ensuring that only authorized individuals or entities can access sensitive data.

2.1 Flowchart

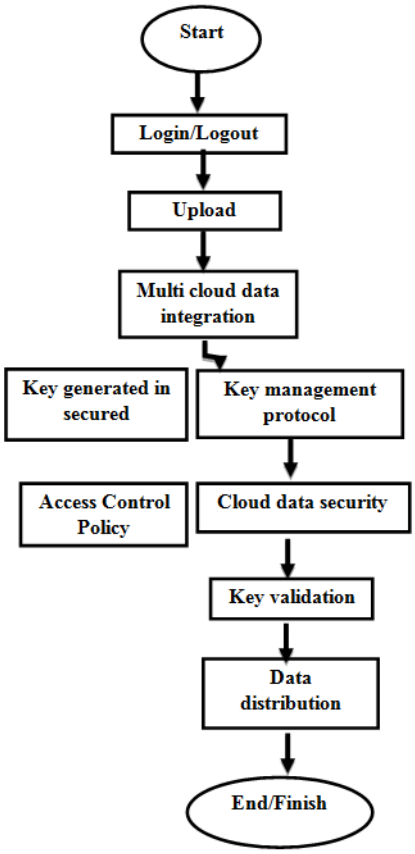

Figure 1: Flow chart

2.2 System Architecture

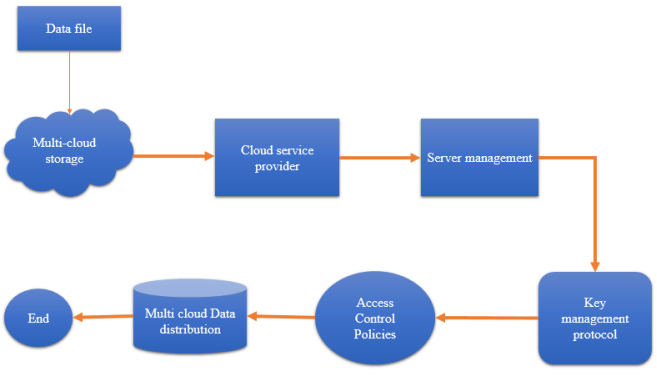

Figure 2: System architecture

Login / Logout

- In this module the user can login by using their unique username and graphical password.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 3, pp 137-140, March-2024

https://doi.org/10.47001/IRJIET/2024.803017

- The login module verifies the user's given username and password with the stored username and password in the cloud.
- If the username and password are matched the user can access the resources.
- If it does not match the user does not allowed to access the resource.

Upload / Download

- In this module the buyer and seller can post the ads and also able to download the data that are posted by other sellers.
- This module is mainly used to upload and also download the big data files.

Multi-Cloud Integration:

This module manages the integration of multiple cloud platforms within the system. It includes functionalities for establishing connections with various cloud service providers, managing authentication credentials and API keys, and orchestrating data transfer and synchronization across different clouds. The module ensures seamless interoperability and data consistency across the multi-cloud environment.

Key Management Protocol:

The Key Management Protocol module is responsible for the generation, distribution, and management of encryption keys used to secure data stored in the multi-cloud environment. It includes functionalities for key generation, encryption, decryption, and key rotation. The module ensures that encryption keys are securely stored and managed to protect sensitive data from unauthorized access or tampering.

Access Control Policy Management:

This module governs the enforcement of access control policies within the multi-cloud storage environment. It includes functionalities for defining and configuring access control rules, assigning user roles and permissions, and monitoring access activities. The module ensures that only authorized users have access to specific data resources and that access privileges are enforced consistently across the multi-cloud environment.

III. RESULTS AND DISCUSSIONS

Multi-cloud storage computing offers diverse services from different providers, enabling tailored solutions. It ensures fault tolerance and continuous access through data redundancy across clouds. By strategically distributing data and resources, latency is minimized, enhancing responsiveness. However, interoperability issues pose challenges for seamless data migration and integration. While multi-cloud setups offer cost optimization opportunities, careful monitoring is needed to control expenses. Robust security frameworks and compliance measures are essential across multiple environments. Managing relationships, monitoring, and troubleshooting across diverse environments pose challenges, necessitating automation and management tools.

IV. CONCLUSION

In conclusion, the proposed system signifies a significant stride forward in multi-cloud storage computing, presenting a cost-effective and secure approach to managing and safeguarding data across distributed environments. Through the amalgamation of Multi-Cloud technologies with on-demand resource provisioning and access control policies, the system effectively achieves the dual goals of enhancing data privacy and optimizing resource allocation. Fragmenting a single dataset across multiple clouds enhances data privacy while minimizing the risk of unauthorized access. The incorporation of an edge device facilitates streamlined management of diverse accounts and communication across clouds, boosting operational efficiency. Additionally, robust access control policies ensure sensitive data remains shielded from unauthorized access, fostering trust in data security and regulatory compliance. In essence, the proposed system offers a holistic solution for organizations aiming to leverage the advantages of multi-cloud storage computing while mitigating associated risks and complexities, thus ushering in a more secure and efficient data management landscape.

REFERENCES

[1] A.Bhardwaj, F. Al-Turjman, M. Kumar, T. Stephan, and L. Mostarda, ‘‘Capturing-the-invisible (CTI): Behavior-based attacks recognition in IoT-oriented industrial control systems,’’ IEEE Access, vol. 8, pp. 104956–104966, 2020.

[2] M. Kumar, A. Rani, and S. Srivastava, ‘‘Image forensics based on lighting estimation,’’ Int. J. Image Graph., vol. 19, no. 3, Jul. 2019, Art. No. 1950014.

[3] M. Kumar, S. Srivastava, and N. Uddin, ‘‘Image forensic based on lighting estimation,’’ Austral. J. Forensic Sci., vol. 51, no. 3, pp. 243–250, Aug. 2017.

[4] J. Li, Y. Zhang, X. Chen, and Y. Xiang, ‘‘Secure attribute-based data sharing for resource-limited users in cloud computing,’’ Comput. Secur., vol. 72, pp. 1–12, Jan. 2018.

[5] Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, and I. You, ‘‘Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing,’’ Inf. Sci., vol. 379, pp. 42–61, Feb. 2017.

ISSN (online): 2581-3048
Volume 8, Issue 3, pp 137-140, March-2024
https://doi.org/10.47001/IRJIET/2024.803017

[6] The OpenStack Project. OSSA-2015-006: Unauthorized Delete of Versioned Swift Object. Accessed: Apr. 14, 2015. [Online]Available: https://security.openstack.org/ossa/OSSA-2015-006.html

[7] The OpenStack Project. OSSA-2015-016: Information Leak Via Swift Tempurls. Accessed: Aug. 26, 2015. [Online]. Available: https://security.openstack.org/ossa/OSSA-2015-016.html

[8] The OpenStack Project. Possible Glance Image Exposure via Swift. Accessed: Feb. 23, 2015. [Online]. Available: https://wiki.openstack.org/wiki/OSSN/OSSN-0025

[9] Cloud Security Alliance. Top Threats to Cloud Computing: Deep Dive. Accessed: Aug. 8, 2018. [Online]. Available: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/top-threats-to-cloud computing-deep-dive.pdf

[10] The OpenStack Project. OpenStack Security Advisories. Accessed: Feb. 2, 2015. [Online]. Available: https://security.openstack.org/ossalist.html

Citation of this Article:

R. Nithin, Dr. R. Nagarajan, "Efficiently Managing Storage across Different Cloud Services for Flexible Resource Allocation and Security Integration" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 8, Issue 3, pp 137-140, March 2024. Article DOI https://doi.org/10.47001/IRJIET/2024.803017

****

