International Journal of Research in Computer Science Engineering and Technology
ISSN: 3049-1665(Online) IJRCET-2024-December Paper, Vol1 Issue 1,pp:1:9, www.ijrcet.in

A Secure and Approved Data Resharing System for Hierarchical Data Sharing in Cloud Environments

[1] Mendi Rohith Nagendra Kumar M.Tech(CSE) Student, Eluru College of Engineering and Technology, rohitnagendra9@gmail.com

[2] Gandi Pranith, Assistant Professor, Department of CSE, Eluru College of Engineering and Technology

Abstract-

Sharing data is really important for working together and coming up with new ideas in today's connected world. However, it comes with big challenges like keeping information safe, following the rules, and running things smoothly. This paper looks at what we need to keep in mind for safe and effective data sharing. It talks about things like protecting data, following regulations, ensuring data is correct, controlling who has access, making sure different systems can work together, and being able to grow as needed. One new idea it introduces is called attribute-based admin-approved data sharing. This means that access to data is linked to certain traits and permissions, making it safer and easier to manage. The paper also suggests a model for sharing data at different levels. This model includes controls that decide who can access what, how sensitive the data is, and ways to share it dynamically. It also has strong processes for checking and keeping track of what happens with the data.Additionally, this model requires that every step of sharing data gets approval from an administrator. This way, decisions are in line with the organization's rules and values. This method encourages openness, responsibility, and teamwork while reducing risks like unauthorized access and data leaks. By tackling the issues we face with data sharing today and focusing on flexibility and safety, the paper offers a clear plan for handling sensitive information, especially in cloud settings and among multiple users.

Intex Terms: Data Sharing, Data Security, Regulatory Compliance, Data Integrity, Access Control, Data Privacy.

1. Introduction

Storing data in the cloud has changed how people and businesses handle their information. Instead of just using local storage like hard drives or servers in their offices, cloud storage lets users save their data on remote servers managed by service providers. This comes with several important benefits. One main benefit is security. Keeping data safe in the cloud is very important for protecting private information and building trust with users. Cloud providers use various security methods to protect the data stored in the cloud. These include encryption, access controls, and regular checks to ensure safety. Encryption is a key way to keep data secure. It transforms data into a form that can only be read with a special key. Access controls are also vital for cloud security. They involve enforcing strict rules about who can see or use sensitive information. For example, using multi-factor authentication ensures that only approved users can access certain data. Role-based access controls limit who can see what, based on their job roles, reducing the chance of unauthorized access. Regular checks help find any weaknesses and make sure safety measures follow the rules.

Many cloud providers offer tools to monitor and track who accesses data, helping organizations spot and respond to any security problems. When sharing data in the cloud, organizations need to carefully plan how to keep it secure and ensure everyone follows the guidelines. To start, it's important to define who can access shared data, what they can do with it, and when it can be shared. This involves setting up access controls based on user roles. Using encryption to protect data during transfer and storage is also essential. This keeps sensitive information safe, even if it is intercepted while being shared. Organizations must also make sure their data-sharing practices follow legal rules, especially when dealing with personal or sensitive information. This might require regular checks and ensuring that all third-party vendors meet the same standards. Keeping track of who accesses shared data is also important. By logging and tracking access, organizations can know who accessed what data and when. This not only increases accountability but also helps uncover any unauthorized access or unusual activity.

Finally, it's important to maintain clear communication with partners who receive the shared data. Regular updates about data-sharing practices can help build trust and keep everything transparent. By carefully managing data sharing in the cloud, organizations can work together effectively while protecting important information.

2. Related Work

Sharing data can really help people work together and come up with new ideas, but there are also problems that organizations need to deal with to keep things safe and effective. One big issue is keeping data secure. It's important to protect private information from getting into the wrong hands, especially when data moves around different platforms and networks. Another important thing is following the rules. Different areas have their own laws about data protection, like GDPR in Europe or HIPAA in the U.S. Companies need to make sure they follow these rules to avoid getting fined or facing legal troubles. Keeping data accurate is also very important. We need to make sure that shared data remains correct and reliable because any mistakes or unauthorized changes can lead to wrong conclusions and bad choices. Setting up strong checks can help reduce this risk. Deciding who can see certain data adds another layer of difficulty. It's necessary to figure out who should access specific information and under what circumstances to keep sensitive data safe. Organizations often find it hard to set up proper access controls, which can either make it too hard to get in or leave them open to risks.

Moreover, sharing data can get tricky when different systems and platforms use various formats and standards. This can make it hard to share data smoothly across different technologies. There must be clear guidelines so everyone understands their roles and how to use shared data properly. If this isn’t clear, organizations might face issues with misuse or misunderstandings. As companies grow and change, they may need to adjust how they share data. Solutions should be flexible enough to handle more data without losing security or performance. It’s also important to make sure data is not only secure but also available when needed. Problems like outages or data corruption during transfer can cause access issues, so organizations should have good backup and recovery plans in place.

In the past, security for data sharing over the cloud has changed to deal with risks from remote access and storage. Some key strategies included turning data into secure formats before sending or storing it, which stops unauthorized users from seeing it. Access control systems helped determine who could view certain data by clearly defining roles and permissions. Additionally, requiring multiple forms of verification before granting access provided extra security. Regular checks on security and rules helped organizations find weaknesses and ensure they were following necessary regulations. Tools to prevent data loss were also used to keep sensitive information safe from unauthorized sharing or access.

With these strategies, companies effectively managed the challenges of sharing data in the cloud while keeping security high and trust strong.

3. Proposed System

Sharing data based on specific traits approved by an administrator is a smart way to handle sensitive information in the cloud. This method improves security and control by allowing access to data according to certain traits and permissions instead of just using traditional roles. In this setup, administrators choose traits like user skills, department, or project involvement. Access to data is given based on these traits. For example, a user with traits linked to a project may see private files that others cannot, making sure only those who really need the information can get it. The fact that this needs admin approval adds another level of safety. Before sharing any data, administrators check and approve requests based on the traits they set up. This review process makes sure data-sharing rules align with safety standards. This way of sharing also makes it easier to track who accessed which data and why, as decisions are linked to specific traits and admin approvals. Organizations can keep clear records, perform audits, and follow data protection rules.

Moreover, access based on traits can change as needed. As a user's role or project changes, their traits can be updated. Using this method not only boosts security and compliance but also creates a more efficient and flexible way to share data. It helps organizations manage their data while reducing the risks of unauthorized access.

3.1. System Architecture Model

Multilevel sharing is a way to access and share information where different users or groups have varying permissions. This is important in places that need strict control over who can see what data, protecting sensitive information while allowing teamwork.

1. Hierarchical Access Control

At the heart of multilevel sharing is hierarchical access control, which splits users into different levels based on their roles. For example, in a company, executives might see all data, while

managers only see what their department needs. This setup ensures users can only interact with data related to their jobs, lowering the chance of unauthorized access.

2. Data Sensitivity Classification

Data is labeled based on its sensitivity, from public to highly confidential. Each level of sensitivity determines who can share or see the data. For instance, public data can be shared freely, while confidential data might only be available to certain roles or departments. This classification helps organizations follow rules and protect sensitive information.

3. Dynamic Sharing Mechanisms

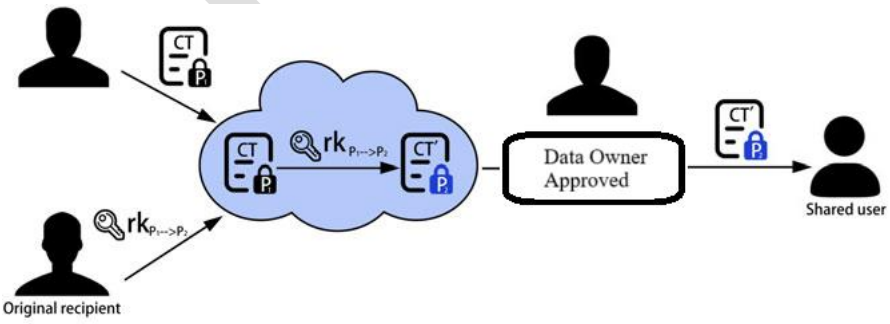
Multilevel sharing also includes flexible methods that let data owners change permissions based on changing needs. For instance, a data owner might give someone limited access to certain data for a project while keeping control over broader access. This flexibility is key for encouraging teamwork without risking security.

4. Auditing and Monitoring

To keep multilevel sharing safe, organizations use auditing and monitoring processes. These track who accesses which data and when, showing usage patterns and possible security issues. Regular audits help organizations keep an eye on things and adjust their sharing rules as needed to tackle new risks.

3.2. Proposed Multilevel Sharing

Let’s look at a situation where a data owner shares data with someone, who then passes it to a shared user, needing the data owner's approval at each step.



1. **Role of the Data Owner**

The data owner is the main person in charge of the data. They can decide how and with whom to share it. When they choose to share data, they check if the person needing access is trustworthy and if sharing follows the organization's rules.

2. Data Sharing with the Recipient

first step usually involves setting specific rules about what the recipient can do, like whether they can only read the data or also edit it, depending on their role and the type of data. The data owner may also outline how the recipient can use or share the data further.

3. Sharing with the Shared User

Once the recipient has the data, they might need to share it with someone else, like a coworker, to work together or finish a task. However, before doing this, they need to get permission from the data owner to make sure the owner’s wishes and security concerns are taken into account.

4. Role of the Administrator

The administrator helps with this sharing process. They act as a link between the recipient and the data owner. When the recipient wants to share data with another user, the administrator checks the request, looks at its importance, and presents it to the data owner. This adds another step to make sure all sharing requests are properly recorded and justified.

5. Approval Process

The data owner looks over the request from the administrator. They think about things like who the shared user is, why they need access, and what might happen if the data is shared. Once the data owner gives their okay, the recipient can share the data with the shared user according to the agreed rules.

4. Conclusion

This way of sharing data involves the data owner, the person receiving the data, the users sharing it, and the admin working together. This teamwork helps make sure that information is shared safely and responsibly. With a system that requires approval from an admin, the data

owner keeps control over their data. This helps them make sure that their sharing choices follow the rules of the organization and are ethical. At the same time, the recipients can work well with the shared users, which builds trust and makes things more efficient. This approach not only encourages openness and responsibility but also helps reduce risks related to unauthorized access, data leaks, or the wrong use of sensitive information. This way, it strengthens how data is shared overall.

References

[1] **M. Ali, S. U. Khan, and A. V. Vasilakos**, "Security in cloud computing: Opportunities and challenges," *Information Sciences*, vol. 305, pp. 357–383, 2015.

[2] **V. Goyal, O. Pandey, A. Sahai, and B. Waters**, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS)*, Alexandria, VA, USA, 2006, pp. 89–98.

[3] **K. Ren, C. Wang, and Q. Wang**, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, Jan.–Feb. 2012.

[4] **Y. Zhang, Z. Chen, and W. He**, "Secure data sharing in cloud computing using revocable-storage identity-based encryption," *IEEE Transactions on Cloud Computing*, vol. 9, no. 1, pp. 74–86, Jan.–Feb. 2021.

[5] **P. Mell and T. Grance**, "The NIST definition of cloud computing," *National Institute of Standards and Technology*, Special Publication 800-145, 2011.

[6] **L. Wang, J. Tao, M. Kunze, et al.**, "Scientific cloud computing: Early definition and experience," in *Proceedings of the 10th IEEE/ACM International Conference on Grid Computing*, Banff, AB, Canada, 2009, pp. 177–184.

[7] **J. Bethencourt, A. Sahai, and B. Waters**, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2007, pp. 321–334.

[8] **S. Kamara and K. Lauter**, "Cryptographic cloud storage," in *Proceedings of the 14th International Conference on Financial Cryptography and Data Security*, Tenerife, Spain, 2010, pp. 136–149.

[9] **D. Boneh and M. Franklin**, "Identity-based encryption from the Weil pairing," in *Proceedings of the 21st Annual International Cryptology Conference (CRYPTO)*, Santa Barbara, CA, USA, 2001, pp. 213–229.

[10] **Z. Xia, X. Wang, X. Sun, and Q. Wang**, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 340–352, Feb. 2016.