e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
Volume:04/Issue:06/June-2022 Impact Factor- 6.752 www.irjmets.com

# A REVIEW OF PROFICIENT SECURE TEAM SHARING AND PRECISE GRAINED DEPENDENT DISPERSION WITH MULTIPLE USERS BY USING CLOUD SERVICES

**Pallavi Dilip Waghmare*1, Prof. K.U. Rahane*2**

*1Research Scholar, Department Of Computer Engineering, Amrutvahini College Of Engineering, Maharashtra, India.

*2Assistant Professor, Department Of Computer Engineering, Amrutvahini College Of Engineering, Maharashtra, India.

## ABSTRACT

Cloud computing is becoming a prominent computing paradigm that allows users to store their data into a cloud server to enjoy scalable and on-demand services. Group data sharing and multi-keyword search in cloud environments has become a hot topic in recent. With the popularity of cloud computing, how to achieve secure group data sharing and Multi- keyword search on encrypted data in cloud environments is an urgent problem to be solved. Although encryption techniques have been used to provide data confidentiality and data security in cloud computing, current technique cannot enforce privacy concerns over encrypted data associated with multiple data owners, which makes co-owners unable to appropriately control whether data distributor can actually distribute their data. In this paper, propose An Efficient Data Group Sharing and multi- keyword search in Cloud Computing, in which data owner can share private data with a group of users via the cloud in a secure way, and data distributor can distribute the data to a new group of users if the attributes satisfy the access policies in the encrypted data. Further present a multiparty access control mechanism over the distributed encrypted data, in which the data co-owners can append new access policies to the encrypted data due to their privacy preferences.

**Keywords:** Cloud Data Sharing, Searchable Encryption, Attribute-Based Proxy Re-Encryption, ECC(Elliptic Curve Cryptography, TFIDT(Term Frequency Inverse, Key Generation, CP-ABSE(Cipher Text-Policy Attribute-Based Searchable Encryption),IB-CPRE(Identity-Based Conditional Proxy Re-Encryption Scheme ),CSP(Cloud Service Provider) .

## I. INTRODUCTION

Compared with the traditional information sharing and communication technology, cloud computing has attracted the interest of most researchers because a lot services are provided by the cloud service providers which helps to reduce costs needed for various resources. Cloud storage is one of the most vital service in cloud computing. Scalability is another attracting factor which allows user to scale up and scale down the resources as required. Cloud computing also convenient and flexible ways for data sharing. There are two ways to share data in cloud storage. The first case refers to the scenario where one client authorizes access to his/her data for many clients known as one-to-many pattern and the second case refers to a situation in which many clients in the same group authorize access to their data for many clients at the same time known as many-to- many pattern.

## II. METHODOLOGY

It is an early stage in the more general activity of requirements engineering which encompasses all activities concerned with eliciting, analyzing, documenting, validating and managing software or system requirements. Requirements analysis is critical to the success of systems or software project. The requirements should be documented, actionable, measurable, testable, traceable, related to identified needs to a level of detail sufficient for system design.

**1. External Interface Requirements**

**User Interface**

Data owner and co-owner registration and login

Upload File

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
Volume:04/Issue:06/June-2022 Impact Factor- 6.752 www.irjmets.com

Encrypt File

Re-Encrypt File

Download File

**Hardware Interfaces**

The entire software requires a completely equipped computer system including monitor, keyboard, and other input output devices.

**Software Interfaces**

The system can use Microsoft as the operating system platform. System also makes use of certain GUI tools. To run this application we need JDK 1.8 and above as java platform and Apache tomcat as server. To store data we need MySQL database.

**Communication Interfaces**

We will use JSP and Servlets.

**Non-Functional Requirements:**

Nonfunctional requirements are the properties that your product must have. Think of these properties as the characteristics or qualities that make the product attractive, or usable, or fast, or reliable. They are fundamental activities of the product activities such as computations, manipulating data, and so on but are there because the client wants the fundamental activities to perform in a certain manner. They are not part of the fundamental reason for the product's existence, but are needed to make the product perform in the desired.

## III. MODELING AND ANALYSIS

We achieve fine-grained conditional data distribution over the cipher text in cloud computing with attribute based CPRE. The encrypted data is firstly deployed with an initial access policy customized by data owner. Our proposed multiparty access control mechanism allows the data co-owners to append new access policies to the encrypted data due to their privacy preferences. Hence, the encrypted data can be re- encrypted by the data distributor only if the attributes satisfy enough access policies.

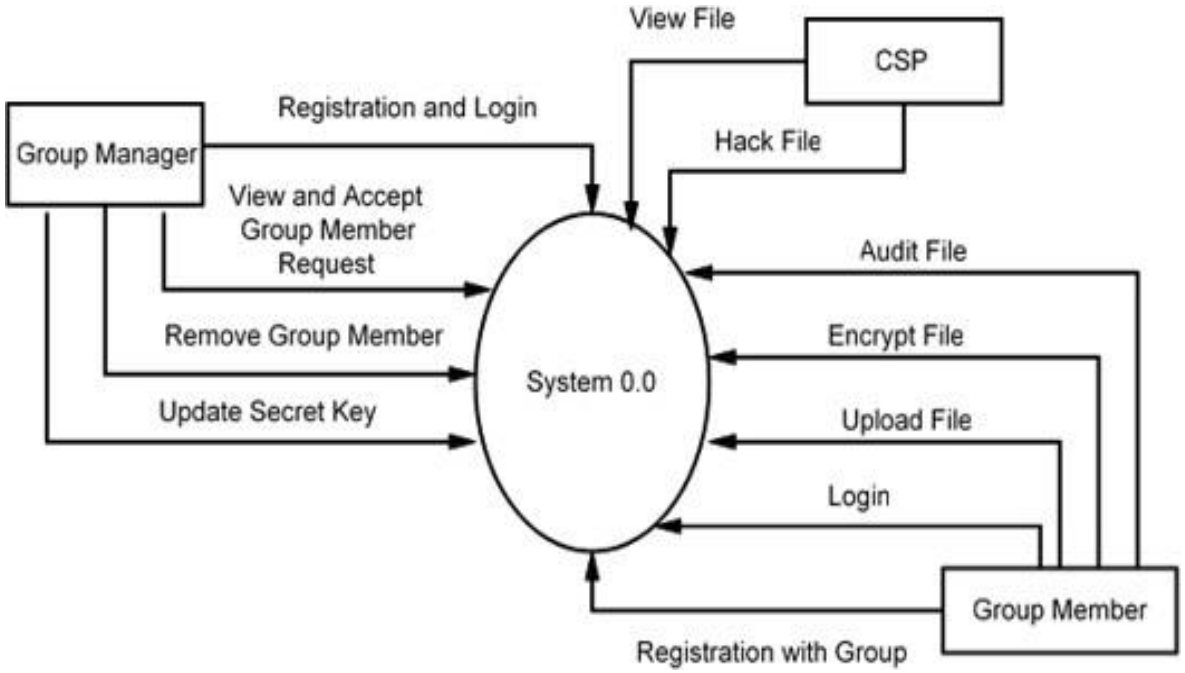


**Fig 1**: Data Flow Diagram(Level 0)

We provide three strategies including full permit, owner priority and majority permit to solve the privacy conflicts problem. Specially, in full permit strategy, data distributor must satisfy all the access policies defined by data owner and co- owners. With the majority permit strategy, data owner can firstly choose a threshold value for data co-owners, and the encrypted data can be disseminated if and only if the sum of the access policies satisfied by data disseminator's attributes is greater than or equal to this fixed threshold.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
Volume:04/Issue:06/June-2022 Impact Factor- 6.752 www.irjmets.com

## IV. RESULTS AND DISCUSSION

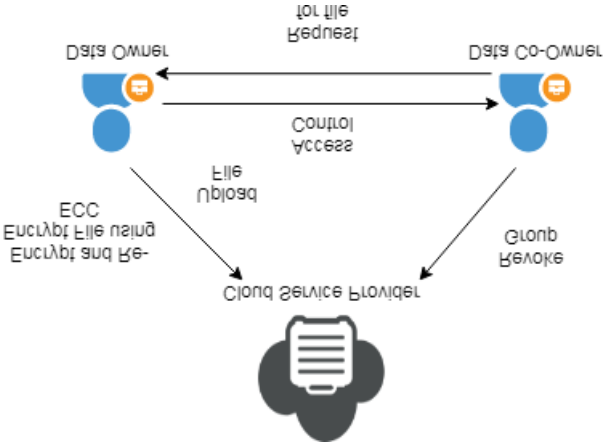


**Fig 2**: System Architecture

In the proposed scheme, members are people with the same interests (e.g.,bidder, doctors, and businessmen) and want to share data in the cloud. The most worrying problem when users store data in the cloud server is the confidentiality of the outsourced data. In this system, users of the same group conduct a key agreement. Subsequently,a common conference key can be used to encrypt the data that will be uploaded to the cloud to ensure the confidentiality of the outsourced data. Attackers or the semi-trusted cloud server cannot learn any content of the out- sourced data without the common conference key.

## V. CONCLUSION

Data security and privacy is a concern for users in cloud computing In particular, how to apply privacy concerns of multiple owners and protection of data privacy It becomes a challenge. In this paper, present a secure group for data exchange and conditional distribution Multi- owner cloud computing scheme. In our schema, the data owner could encrypt his private data and share them with a group of data access devices simultaneously time conveniently based on the proposed technique. The data owner can specify specific access Attribute-based encrypted text therefore, the encrypted text can be encrypted only by data diffuser whose attributes satisfy the access policy in the encrypted text we also have a multi-part.

## VI. REFERENCES

[1] Qinlong Huang, Member, IEEE, Yixian Yang, Wei Yue and YueHe" Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Com- puting", IEEE TRANSACTIONS ON LOUD COMPUTING , APRIL 2019

[2] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 485-498, 2017.

[3] H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control over encrypted data for edge computing networks," IEEE Access, vol. 6, pp. 30049–30059, 2018.

[4] K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining data owner-side and cloud-side access control for encrypted cloud storage," IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2062–2074, 2018.

[5] N. Paladi, C. Gehrmann, and A. Michalas, "Pro user security guaranteesin public infrastructure clouds," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 405-419, 2017.

[6] L. Jiang, and D. Guo "Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage," IEEE Access, vol. 5, pp. 13336 – 13345, 2017.

[7] K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: control of photo sharing on online social networks," IEEE Trans. On Dependable and Secure Computing, vol. 14, no. 2, pp. 99-210, 2017.