IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

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

[1]PALLAVI DILIP WAGHMARE, [2]PROF. K. U. RAHANE

[*1] Research Scholar, Department of Computer Engineering, Amrutvahini College of Engineering, Maharashtra, India.

[*2] Assistant 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 techniqueshave 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. Inthis 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 anew 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 thedata 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) .

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 provides 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. As the data shared on the cloud is valuable, various security methods are provided by cloud. In current cloud applications various algorithms are used for data encryption and decryption. In encryption is based on ABE [Attribute Based Encryption. Symmetric- key cryptography is used in to enable efficient encryption. Practical group key management algorithm based on a proxy re-encryption technology. In existing system when a user is revoked from a group, he is still able to access files from his previous group which leads to collision attack. Another gap is that a user is not allowed to upload multiple files of same name.

I. METHODOLOGY

In Cloud based group sharing to maintain the data security the private keysof co members of group need to be updated after the revocation of any group member, also to restrict the malicious members from accessing the data in group file upload constraints will be introduced. Data confidentiality will be maintained using double encryption when uploading data on cloud.

The main goals of the proposed scheme includes access control, data confidentiality, data security, data sharing and efficiency. To achieve Access Control within the group private keys are generated for every user to provide access to files. To achieve data confidentiality after revocation of any member the private keysof existing members of that group will be updated.To maintain the private keys of every user and provide them access to their resources without any Certificate Authorities.

The main goals of the proposed scheme includes access control, data confidentiality, data security, data sharing, and efficiency. To achieve Access Control within the group private keys are generated for everyuser to provide access to files.

II. MODELING AND ANALYSIS

Group Member

1) In the proposed scheme, members are people with interests (e.g., bidder, doctors, and businessmen)and want to share data in the cloud.
2) The most worrying problem when users store data in the cloud server is the confidentiality of the outsourced data.
3) 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.
4) Attackers or the semi-trusted cloud server cannot learn any content of the outsourced data without the key.
5) Our scheme uses a technique called group signatures, which allows users in the same group to anonymously share data in the cloud.
6) Group members search files using multi-keyword search.

A. Group Manager

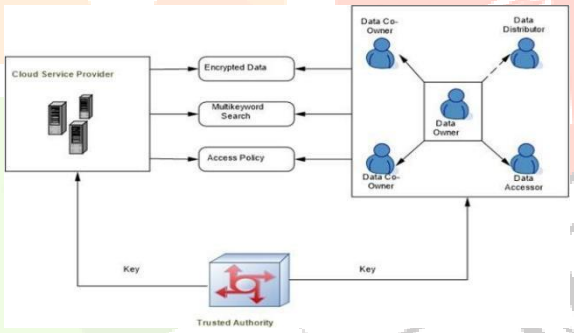
1) Group Manager is responsible for generating system parameters, managing group members (i.e., uploading member‘s encrypted data, authorizing group members)and for the fault tolerance detection.
2) The group manager in our scheme is a fully trusted third party to both the cloud and group members.
3) If an external user tries to access files from a different group more than three times then the manager will remove that particular user from the applications.

B. Cloud Service Provider (CSP)

1) CSP provides users with seemingly unlimited storage services.
2) In addition to providing efficient and convenient storage services for users, the cloud can also provide data sharing services.
3) However, the cloud has the characteristic of honest but curious.
4) In other words, the cloud will not deliberately delete or modify the uploaded data of users, but it will be curious to understand the contents of the stored data and the user‘s identity.

Architecture

Dynamic Groups:



The Main Concepts of Dynamic Group users select the Particular group when user Register with Group. Groups are created by the Group Manager.

USER REVOKED OR USER JOIN:

1. When new user joins or revoked from particular group then the Private Key of particular user and other user of same group their private key compulsory update and recomputed.
2. user search files using Multi keyword search system.
3.

GROUP MANAGER:

Group Manager is created the Groups. And Manager decided space of group and Dynamical efficiently used space.

Algorithms:

1. TFIDF Algorithm:

Terminology:

1. t — term (word)
2. d — document (set of words)
3. N — count of corpus
4. corpus — the total document set

• TF: Term Frequency, which measures how frequently a term occurs in a document. Since every document is different in length, it is possible that a term would appear much more times in long documents than shorter ones. Thus, the term frequency is often divided by the document length (aka. the total number of terms in the document) as a way of normalization:

tf (t, d) = count of tind/numberofwordsind

• IDF: Inverse Document Frequency, which measures how important a term is. While computing TF, all terms are considered equally important. However it is known that certain terms, such as ‖is‖, ‖of‖, and ‖that‖, may appear a lot of times but have little importance. Thus we need to weigh down the frequent terms while scale up the rare ones, by computing the following:

$$idf\,(t) = log(N/(df + 1))$$

$$tf - idf(I^j) log(tf(I^j, d_j) + 1) * log(D/1 + df(I^j, D))$$

2.ECC ALGORITHM:

The equation of an elliptic curve is given as,

$$y^2 = x^3 + ax + b$$

Few terms that will be used, E -¿ Elliptic Curve

P -¿ Point on the curve

n -¿ Maximum limit (This should be a prime number)

KEY GENERATION

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver‘s public key and the receiver will decrypt its private key.Now, we have to select a number _d‘ within the range of _n‘. Using the following equation we can generate the public key

$$Q = d * p$$

d = the random number that we have selected within the range of (1 to n-1). P is the point on the curve. _Q‘ is the public key and _d‘ is the private key.

Encryption

Let _m‘ be the message that we are sending. We have to represent this message on the curve. This have in-depth implementation details.

Consider _m‘ has the point _M‘ on the curve _E‘. Randomly select _k‘ from [1 – (n-1)]. Two cipher texts will be generated let it be C1 and C2.

$$C1 = M + k * Qp \quad C_2$$

C1 and C2 will be send.

DECRYPTION

We have to get back the message _m‘ that was send to us,

$$M = C_2 - d * C_1$$

M is the original message that we have send. How does we get back the message?

$$M = C_2 - d * C_1$$

M can be represented as

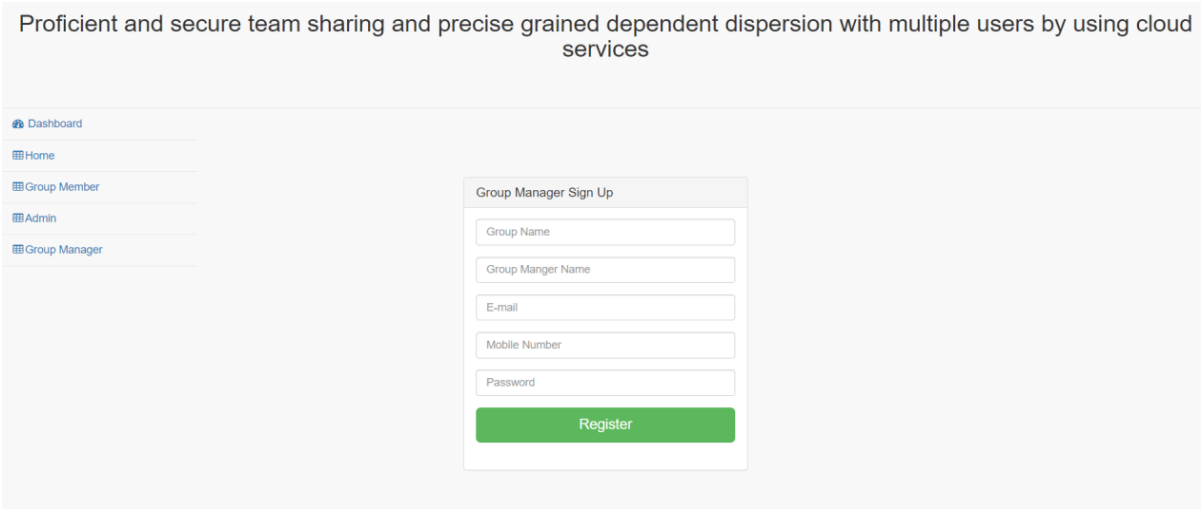
$$\_C2 - D * C1$$

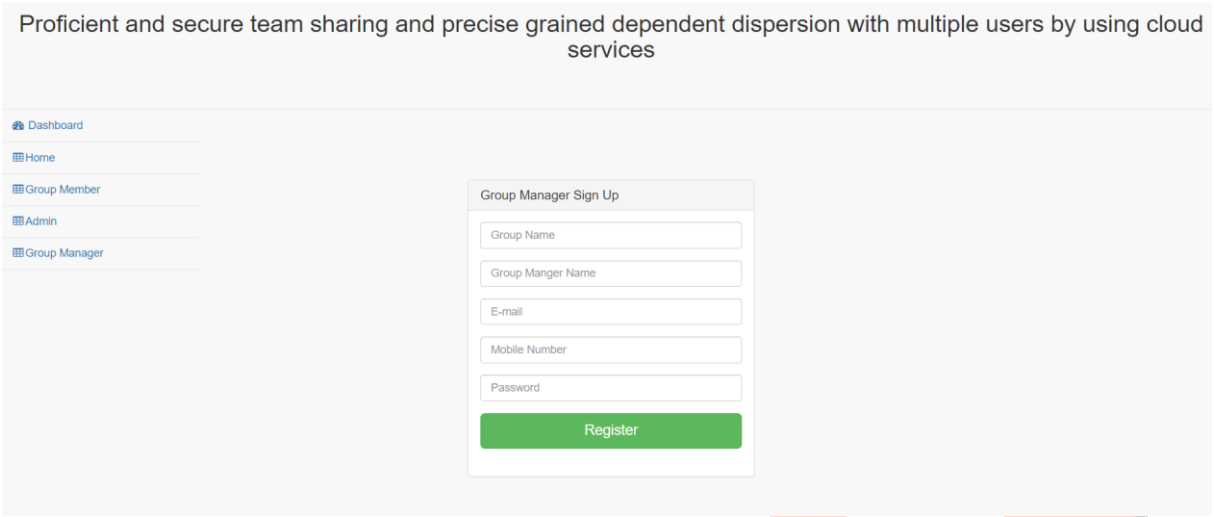
$$C - D * C = (M + K * Q) - D * (K * P) (C = M + K * Q \text{ AND } C = K * P)$$

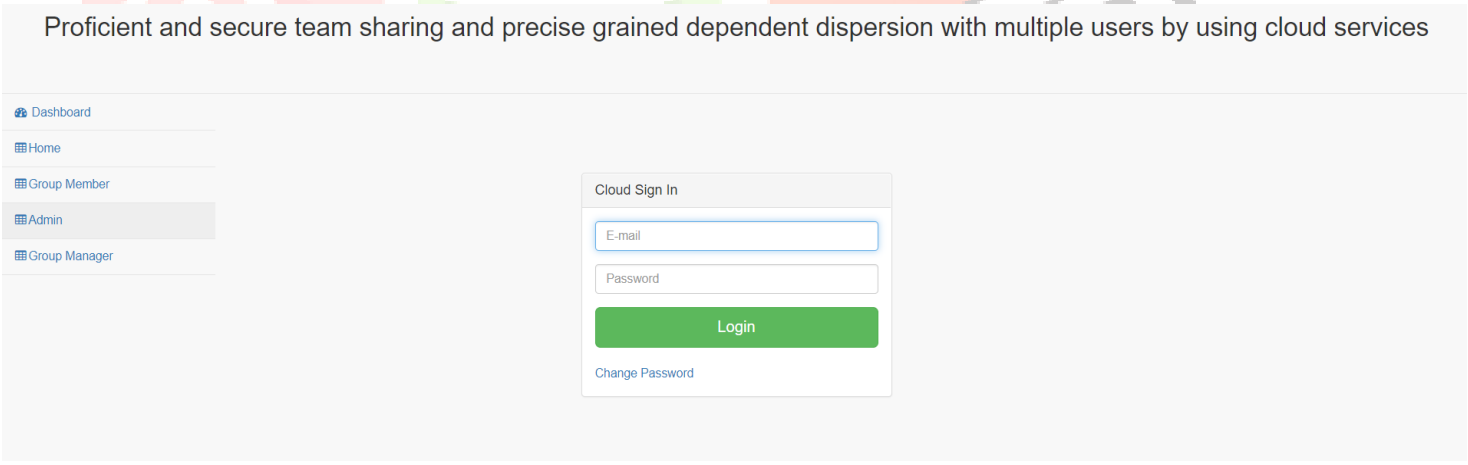
$$= M + k * d * P - d * k * P$$

$$= M \ (Original\ Message)$$

III. RESULTS AND DISCUSSION


Proficient and secure team sharing and precise grained dependent dispersion with multiple users by using cloud services
Dashboard
Home
Group Member
Admin
Group Manager
Group Manager Sign Up
Group Name
Group Manger Name
E-mail
Mobile Number
Password
Register


Proficient and secure team sharing and precise grained dependent dispersion with multiple users by using cloud services
Dashboard
Home
Group Member
Admin
Group Manager
Group Manager Sign Up
Group Name
Group Manger Name
E-mail
Mobile Number
Password
Register


Proficient and secure team sharing and precise grained dependent dispersion with multiple users by using cloud services
Dashboard
Home
Group Member
Admin
Group Manager
Cloud Sign In
E-mail
Password
Login
Change Password

Proficient and secure team sharing and precise grained dependent dispersion with multiple users by using cloud services

Dashboard
Home
Upload File
Members in Group
All Files
Logout

Group Manager Home

Proficient and secure team sharing and precise grained dependent dispersion with multiple users by using cloud servic

Dashboard
Home
Upload File
Members in Group
All Files
Logout

Upload File

Choose File No file chosen

Upload

Proficient and secure team sharing and precise grained dependent dispersion with multiple users by using cloud services

Dashboard
Home
Members in Group
All Files
Logout

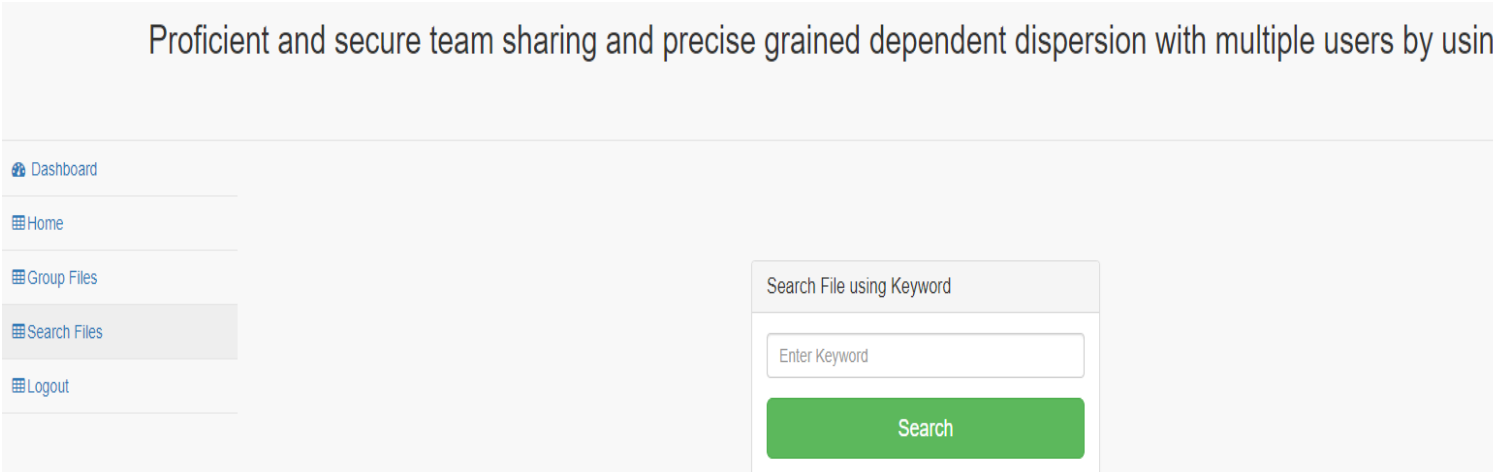
User Details Table

Name	Address	Email	Mobile No	DOB	Group Name	Status
sonali	pune	sonalimitkari05@gmail.com	9890234512	2021-06-14	cat	Active
Akshay	xyz	akshay44@gmail.com	8888099874	2001-02-04	dog	Active
Pallavi	sangamner	pallavi34@gmail.com	9145652488	1998-12-07	cat	Active
Nisha	nasik	nisha29@gmail.com	9865342665	2000-04-29	dog	Active
supriya	Mumbai	supriya12@gmail.com	9865322356	2002-07-12	cat	Active
Saksham	Sangamner	saksham13@gmail.com	9785462456	2022-01-13	cat	Active
Swaraj	Pune	swaraj12@gmail.com	9586245621	2022-05-06	cat	Active
Aarush	Nagpur	aarush12@gmail.com	8545623145	2017-11-01	dog	Active
Krushna	Kopargaon	krushna12@gmail.com	9585642413	2011-04-23	dog	Active
Pari	Pune	pari@gmail.com	9856231425	2021-02-21	school	Inactive
ram	sangamner	ram12@gmail.com	9874561231	1993-02-04	akshay	Inactive

Proficient and secure team sharing and precise grained dependent dispersion with multiple users by using cloud services

Dashboard
Home
Group Files
Search Files
Logout

User Home



IV. 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 multi-keyword search in 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 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 access control mechanism on encrypted text, which allows the co-owners of the data add their access policies to Encrypted text. In addition, provide three aggregation criteria strategies that include full authorization, owner priority and majority help solve the problem of privacy conflicts.

V. REFERENCES

[1]Q in long Huang, Member, IEEE, Yixian Yang, Wei Yue and Yue He" Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing", IEEE TRANSACTIONS ON CLOUD 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, "Providing user security guarantees in public infrastructure clouds," IEEE Transactions on CFu, "Secure data group sharing and dissemination with attribute and time conditions in Public Clouds," IEEE Transactions on Services Computing, 2018.

[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. 199-210, 2017

[8]Fang, L. Yin, Y. Guo, Z. Wang, and Fenzhua Li, "Resolving access conflicts: an auction-based incentive approach," Proc. IEEE Military Communications Conference (MILCOM), pp. 1-6, 2018.

[9]Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing," IEEE Access, vol. 6, pp. 36584–36594, 2018.

[10]S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu, and W. Xie, "Attribute based data sharing scheme revisited in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1661–1673, 2016.

[11]K. Seol, Y. Kim, E. Lee, Y. Seo, and D. Baik, "Privacy-preserving attribute- based access control model for XML-based electronic health record system," IEEE Access, vol. 6, pp. 9114-9128, 2018.

[12]H. Hu, G. Ahn, and J. Jorgensen, "Multiparty access control for online social networks: Model and mechanisms," IEEE Trans. on Knowledge and Data Engine, vol. 25, no. 7, pp. 1614-1627, 2013.

[13]Q. Huang, Y. Yang, and M. Shen, "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing," Future Generation Computer Systems, vol. 72, pp. 239-249, 2017.

[14]J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Trans. on Knowledge and Data Eng., vol. 25, no. 10, pp. 2271-2282, 2013.