is represented by matrix of encrypted 0s and 1s. The ElGamal cryptosystem is semantically secure, and the cipher text of every 1 or 0 is different from other 1s or 0s. So it preserves the search privacy. The cloud cannot know that what the user is searching for. Data owner uploads data on cloud for sharing, for security purpose data is encrypted before uploading on cloud using PBEWithMD5AndDES i.e. password based encryption with MD5 and Data Encryption Standard algorithm. In proposed system user uses keyword to retrieve files so dictionary attack can be possible in this case. So MD5 algorithm helps to prevent dictionary attack.

5.Mathematical Model

R -> Rank
Q -> Query
M -> Mask Matrix
K -> Keyword
B -> Buffer
S -> System
S={User, Q, R, M, ADL, Cloud}

- Input: Users send query to ADL Qi={Ki,Ri}
- Process: ADL aggregates different queries, Q={Q1,Q2..,Qn}ADL generates mask matrix Epk {M} which Encrypted with ADLs public key pk, it sends to Cloud. Cloud sends result to ADL B= {File, K}
- Output: ADL distributes results to users {File1, File2.,Filen}

6.Modules

- Cloud Service Provider

It stores all files uploaded by the authorized data owner, and allow accessing the data only to the authorized User. It accepts the query from ADL and sends the result according to the query send by ADL.

- Data Owner

The data owner is person who uploads the data. Data owner should login first to store their data on cloud. Only authorized owner can store their data on cloud and new data owner should register first.

- Cloud User

In this module, the cloud user should be authenticated so the user should register and login for cloud usage. The vendor which verifies that whether the user is authenticated or not, If he/she is unauthorized user then CSP cannot continue further processing. Once login successfully then he/she can obtain the basic information from cloud storage for data integration. Here the user can request the data to cloud using certain keywords.

- Query Search based on ranking

In this module, each user set the rank to their query and cloud searches the results on the basis of the rank. Cloud returns certain percentage of matched file to the ADL. The basic idea of this module is to protect the privacy and rank the user queries. In this module, Cloud sends the file along with the keywords.

- File Distribution

The aggregation and distribution layer (ADL), is an intermediate layer between the user and cloud. It aggregates the queries and sends combined query to the cloud. cloud sends result to the ADL, Finally the file distribution will be performed to deliver the requested files to the corresponding users.

- Performance Evaluation

Here we compare the performance of existing scheme with proposed flexible ranking mechanisms. It represents the performance analysis of the work in the form of a graph to show the variance occurred in between them.

7.Results and Discussion

Figure 3: Ranked Keyword Serching

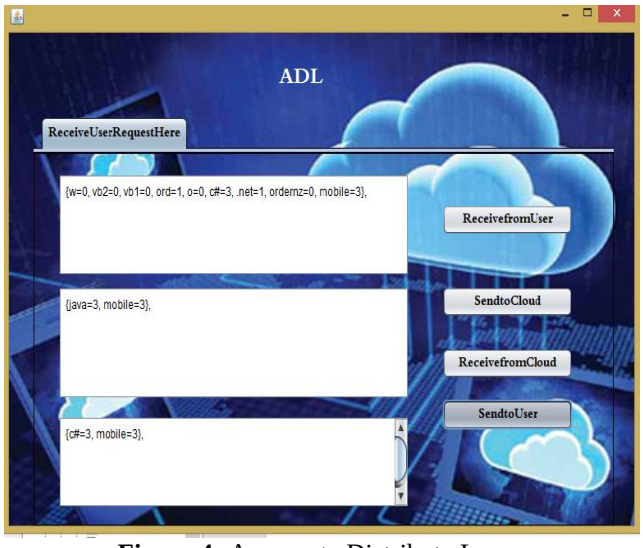

Figure 4: Aggregate Distribute Layer

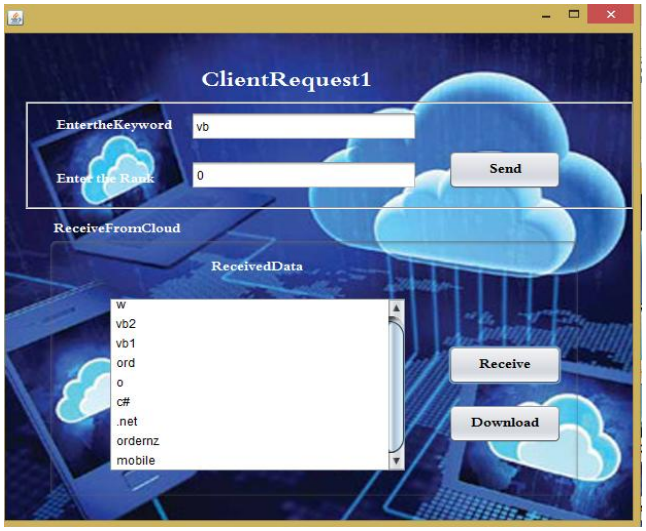

Figure 5: Client Request

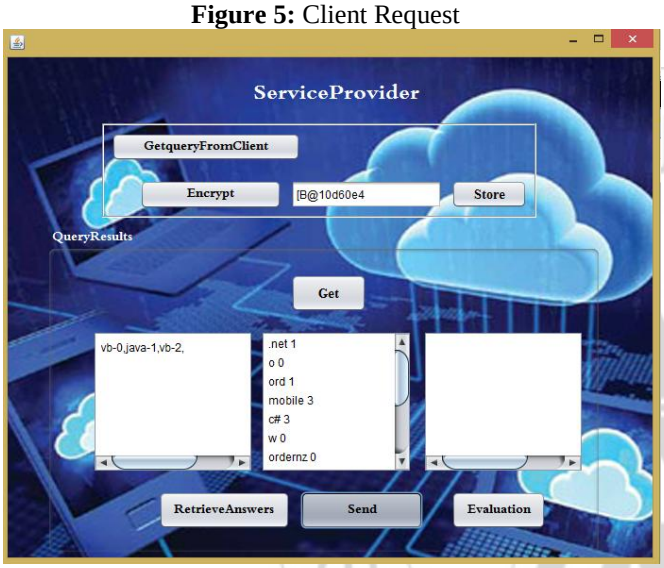

Figure 6: Cloud Service Provider

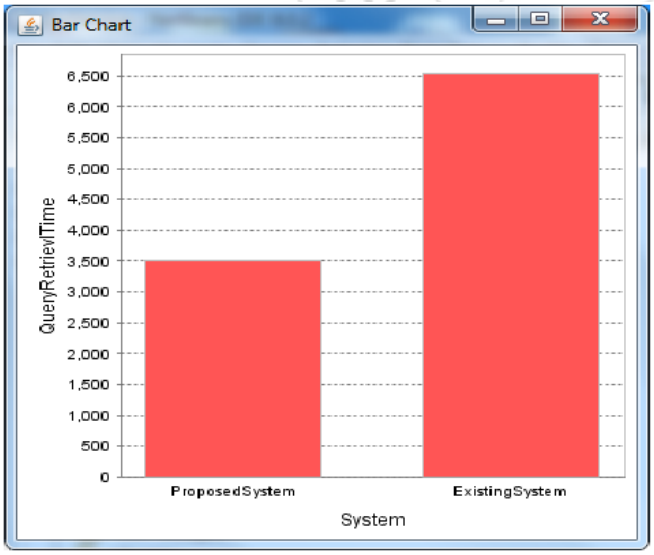

Figure 7: Performance Evaluation

8.Conclusion

The proposed flexible ranking model helps to improve the performance and security in cloud computing. In this scheme user can retrieve different percentages of matched files by specifying queries of different ranks. This technique is useful when there are a large number of matched files, but the users are interested in certain percentage of matched files. Aggregate Distribute Layer introduced between user and cloud ,aggregates the query and distributes the results to different user this helps to reduce the communication and computation cost during information retrieval in cloud computing environment. Proposed system provides security to user and data during secure searching. In future work we can use MD5 algorithm to provide more security to data. This technique helps to check the integrity of data stored on cloud.

References

[1] Qin Liu, Chiu C. Tan, Jie Wu and Fellow ,Towards Differential Query Services in Cost-Efficient Clouds IEEE Transactions On Parallel and
[2] Distributed Systems, VOL. 25, NO. 6, JUNE 2014.
[3] Ostrovsky and W. Skeith III, Private searching on streaming data, in Proc. of ACM CRYPTO, 2005.
[4] Q. Liu, C. Tan, J. Wu, and G. Wang, Cooperative Private Searching in Clouds,J. Parallel Distrib. Comput. , vol. 72, no. 8, pp. 1019-1031, Aug.2012.
[5] Q. Liu, C. C. Tan, J. Wu, and G. Wang,Efficient information retrieval for ranked queries in cost-effective cloud environments, in Proc. of IEEE INFOCOM, 2012.
[6] G. Danezis and C. Diaz, Improving the decoding efficiency of private search,in IACR Eprint archive number 024, 2006.
[7] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, Secure ranked keyword search over encrypted cloud data, in Proc. of IEEE ICDCS, 2010
[8] Boldyreva, N. Chenette, Y. Lee, and A. Oneill,Order-preserving symmetric encryption, Advances in Cryptology-EUROCRYPT, 2009.
[9] Ning Cao, Cong Wang , Li, Ming , Kui Ren, Wenjing Lou, Privacy- Preserving Multi-keyword Ranked Search over Encrypted Cloud Data,
[10] INFOCOM, 2011 Proceedings IEEE April 2011.
[11] P. Paillier,Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, in Proc. EUROCRYPT, 1999, pp. 223-238. V. Hristidis and Y. Papakonstantinou, DISCOVER: Keyword Search in Relational Databases,in Proceedings of the 29th International Conference on Very Large Data Bases, VLDB Endowment, August 2002, pp. 670681.
[12] Cong Wang, Ning Cao, Kui Ren, and Wenjing Lou,Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data, IEEE Transactions On Parallel And Distributed Systems, Systems, VOL. 23, NO. 8.