d)The position of the first appearance of the word

$$\#(Word)/\sum Word_i$$

A. Experimental Setup:

The system is built using Java framework (version jdk 1.8) on Windows platform, MySQL 5.0 and SqlYog 5.0 for database .Net beans (8.0.2) is use as development tool. The current system doesn't require any specific hardware to run. Any standard machine is capable of running the application.

5. Performance Evaluation

The fig. A shows the time comparison between document search using Euclidean Distance, cosine similarity and document search using CRF &cosine similarity.

Table 1: Comparative readings for document search

	Euclidean Distance	Cosine Similarity	CRF & Cosine Similarity
Time (in ns)	990000000	700000000	60000000

The document search using CRF &co-sine similarity take less time than document search using Euclidean Distance and document search using cosine similarity, in-crease the performance.

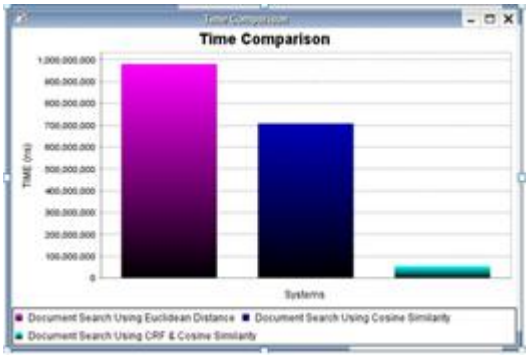

Figure a: Time Comparison Graph

Table 2: Comparative readings for document search

	Existing system	Proposed System
Memory Space (in bytes)	340	145

The figure B shows the data storage comparison between existing system (Traditional Trapdoor) and proposed system (Trapdoor using CRF). The data storage in proposed system (Trapdoor using CRF) in low.

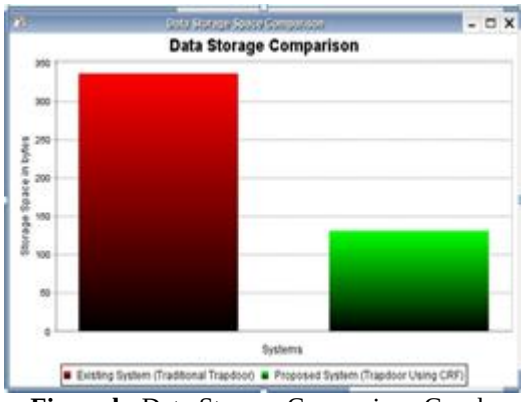

Figure b: Data Storage Comparison Graph

Table 3: Comparative document search for 4 keywords

	Number of Keywords (Dictionary Words)			
	500	750	1000	1500
Euclidean Distance (Time in Ms)	1512	2020	2143	2527
Cosine Similarity (Time in Ms)	1469	1999	2096	2502
CRF and Cosine Similarity (Time in Ms)	1306	1529	1590	1738

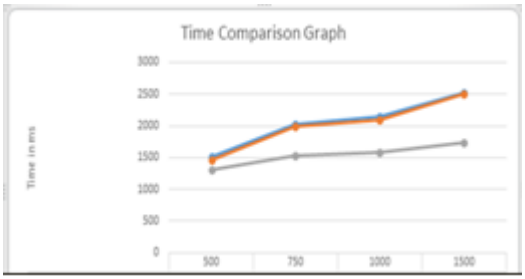

Figure c: Time Comparison Graph

The above fig C graph shows time required to search same number (w = 4) of keywords from different size of keyword dictionary with the same number of documents, In Fig.1 X-axis shows Number of Keywords while Y-axis shows time required to search the keywords in ms.

Table 4: Time comparison Graph (different keywords)

	Number of Keywords (Dictionary Words)			
	5	10	15	20
Euclidean Distance (Time in Ms)	2527	2540	2596	2602
Cosine Similarity (Time in Ms)	2462	2512	2569	2588
CRF and Cosine Similarity (Time in Ms)	1412	1521	1591	1602

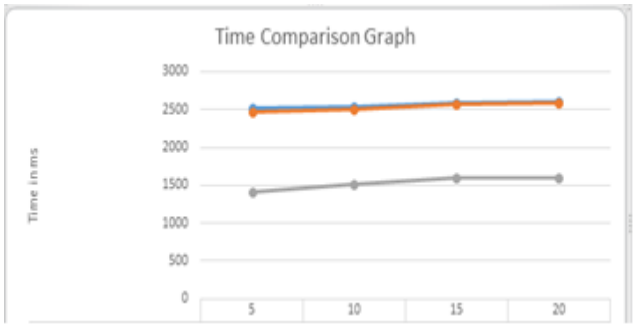

Figure d: Time Comparison Graph having same number of Dictionary Words

The above graph, figure D shows time required to search different number of keywords from same size of keyword dictionary (1500 keywords) with the same number of documents, In Fig.2 X-axis shows Number of Keywords while Y-axis shows time required to search the keywords in ms.

6. Related Work

In paper [1] for achieving effective retrieval of remotely stored encrypted data for mobile cloud computing, authors designed and implemented new ranked fuzzy keyword search method. A test on a real database set (RFC) is performed and demonstrated the proficiency of their suggestion and a correlation with the latest searchable encryption algorithm given a critical upgrade of the index development speed of plan.

Authors proposes [2] the 1st choas based searchable encryption approach which additionally permits both ranked and fuzzy keyword searches on the encoded information put away in the cloud. Given methodology ensures the security and secrecy of the client. This plan is executed and assessed utilizing two databases: RFCs and the Enron database. Tests have been performed to demonstrate the proficiency of the proposition.

Author developed a Searchable Encryption CP-ABE (SE-CP-ABE) access control method by mixing of both security holomorphic encryption algorithm with traditional CP-ABE algorithm and provided security observation as well as examined observation for the method. Outcomes of technique demonstrate that SE-CP-ABE method is assures security of CP-ABE as well as deploys ciphertext retaining and mitigates time of retaining [3].In paper [4] author presented cryptographic method to overcome the issue of searching over encrypted data as well as given evidences of security. This method gives confidentiality for encryption in case of unreliable server which is unknown related with the plaintext if just ciphertext is provided.

Author proposed [5] an effective index to enhance the search performance and accept the blind storage method to hide access pattern of the searching user. Observations of method show that method is able to gain secrecy of documents as well as dex, trapdoor confidentiality, trapdoor unlinkability and hiding access pattern of user.

In [7], [8] authors proposed search authority in SPE using attribute-based encryption technique.

7. Conclusion

The proposed system is used a multi-keyword ranked search scheme for accurate, efficient and secure search on encrypted mobile cloud data. Proposed scheme can effectively achieve user's confidentiality of documents as well as index, trapdoor unlink-ability, trapdoor privacy, and concealing access pattern of the search on the basis of security analysis. Proposed scheme can achieve better efficiency on the basis of extensive performance evaluations shown in terms of the functionality and computation overhead as compared with existing ones.

By using CRF algorithm, there is reduction in the time consumption and Cosine similarity algorithm is used to increase the accuracy of proposed system.

References

[1] Abir Awad, Adrian Matthews, Brian Lee," Secure Cloud Storage and Search Scheme for Mobile Devices", 17th IEEE Mediterranean Electro technical Conference, Beirut, Lebanon, 13-16 April 2014.
[2] Abir Awad, Adrian Matthews, Yuansong Qiao, Brian Lee," Chaotic Searchable Encryption for Mobile Cloud Storage", IEEE Transactions on Cloud Computing,, no. 1, pp. 1, July2015.
[3] An-Ping Xiong, Qi-Xian Gan, Xin-Xin He, Quan Zhao, "A searchable encryption of CP-ABE scheme in cloud storage", Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2013 10th International Computer Conference on Dec. 2013.
[4] Dawn Xiaodong Song David Wagner Adrian Perrig, ''Practical Techniques for Searches on Encrypted Data,'' Defense Advanced Research Projects Agency under DARPA contract N6601-99- 28913
[5] B. Zhang and F. Zhang, ''An efficient public key encryption with conjunctive-subset keywords search,'' J. Netw. Comput. Appl., vol. 34, no. 1, pp. 262–267, Jan. 2011.
[6] Q. Liu, C. C. Tan, J. Wu, and G. Wang, ''Efficient information retrieval for ranked queries in cost-effective cloud environments,'' in Proc. IEEE INFOCOM, Mar. 2012, pp. 2581–2585
[7] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, ''Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud,'' in Proc. IEEE INFOCOM, Apr./May 2014, pp. 226–234.
[8] Q. Zheng, S. Xu, and G. Ateniese, ''VABKS: Verifiable attribute based keyword search over outsourced encrypted data,'' in Proc. IEEE INFOCOM, Apr. 2014, pp. 522–530.
[9] Song DX, Wagner D, Perrig A (2000), "Practical techniques for searches on encrypted data." In: Proceedings of the IEEE Symposium on Security and Privacy, IEEE, pp 44–55.
[10] Korkmaz, T. Tek, S. "Analyzing Response Time of Batch Signing." Journal of Internet Services and Information Security, Vol. 1, 2011, No. 1, pp. 70-85.
[11] Fukushima, K. Kiyomoto, S. Miyake, Y. "Towards Secure Cloud Computing Architecture - A Solution Based on Software protection Mechanism". Journal of Internet Services and Information Security, Vol. 1, 2011, pp. 4-17