RESEARCH ARTICLE OPEN ACCESS

# Privacy Preserving in Distributed verifiable Data Control in cloud Storage

R.Pavithra[1],Gayathri[2], K.Sangeetha, .S.Vijaykumar[3]
[1,2] (Information Technology),[3](Assistant Professor –CSE)

## Abstract:

Cloud computing economically enables the paradigm of data service outsourcing. However, to protect data privacy, sensitive cloud data have to be encrypted before outsourced to the commercial public cloud, which makes effective data utilization service a very challenging task. Although traditional searchable encryption techniques allow users to securely search over encrypted data through keywords. In this paper, we define and solve the problem ofsecure ranked keyword search over encrypted cloud data.

## I. INTRODUCTION

The content-aware search scheme,which can make semantic search more smart. The Conceptual Graphs (CGs) as a knowledge representation tool. In order to conduct numerical calculation, transfer original CGs into their linear form with some modification and map them to numerical vectors. Next, employ the technology of muti-keyword ranked search over encrypted cloud data as the basis against two threat models and raise PRSCG and PRSCG-TF to resolve the problem of privacy-preserving smart semantic search based on conceptual graphs

Specifically, we explore the statistical measure approach, i.e., relevance score, from information retrieval to build a secure searchable index, and develop a one-to-many order-preserving mapping technique to properly protect those sensitive score information. Thorough analysis when compared to previous searchable encryption schemes, while correctly realizing the goal of ranked keyword search.

## FEASIBILITY STUDY

## TECHNICAL FEASIBILITY:

Evaluating the technical feasibility is the trickiest part of a feasibility study. This is because , at this point in time, not too many detailed design of the system, making it difficult to access issues like performance, costs on ( account of the kind of technology to be deployed) etc. A number of issues have to be considered while doing a technical analysis.

i) Understand the different technologies involved in the proposed system :

Before commencing the project, we have to be very clear about what are the technologies that are to be required for the development of the new system.

ii) Find out whether the organization currently possesses the required technologies:

Is the required technology available with the organization?

If so is the capacity sufficient?

For instance – “Will the current printer be able to handle the new reports and forms required for the new system?”

## ECONOMIC FEASIBILITY:

Economic feasibility attempts 2 weigh the costs of developing and implementing a new system, against the benefits that would accrue from having the new system in place. This feasibility study gives the top management the economic justification for the new system.

A simple economic analysis which gives the actual comparison of costs and benefits are much more meaningful in this case. In addition, this proves to be a useful point of reference to compare actual costs as the project progresses. There could be various types of intangible benefits on account of automation. These could include increased customer satisfaction, improvement in product quality better decision making timeliness of information, expediting activities, improved accuracy of operations, better documentation and record keeping, faster retrieval of information, better employee morale.

**OPERATIONAL FEASIBILITY:**

Proposed projects are beneficial only if they can be turned into information systems that will meet theorganizationsoperating requirements. Simply stated, this test of feasibility asks if the system will work when it is developed and installed. Are there major barriers to Implementation? Here are questions that will help test the operational feasibility of a project:

- Is there sufficient support for the project from management from users? If the current system is well liked and used to the extent that persons will notbe able to see reasons for change, there may be resistance.
- Are the current business methods acceptable to the user? If they are not, Users may welcome a change that will bring about a more operational and useful systems.
- Have the user been involved in the planning and development of the project?
- Early involvement reduces thechances of resistance to the system and in
- General and increases thelikelihood of successful project.

Since the proposed system was to help reduce the hardships encountered. In the existing manual system, the new system was considered to be operational feasible.

**EXISTING SYSTEM**

We show that existing proposals to achieve *anonymity* in search logs are insufficient in the light of attackers who can actively influence the search log. However, we show that it is impossible to achieve good utility with differential privacy.

**DISADVANTAGES**

Existing work on publishing frequent item sets often only tries to achieve anonymity or makes strong assumptions about the background knowledge of an attacker.

**PROPOSED SYSTEM**

The main focus of this paper is search logs, our results apply to other scenarios as well. For example, consider a retailer who collects customer transactions. Each transaction consists of a basket of products together with their prices, and a time-stamp. In this case can be applied to publish frequently purchased products or sets of products. This information can also be used in a recommender system or in a market basket analysis to decide on the goods and promotions in a store.

**ADVANTAGES**

Our results show that yields comparable utility to OPSE while at the same time achieving much stronger privacy guarantees.

**CONCLUSION**

In this paper,compared with the previous study.we propose two more secure and efficient schemes to solve the problem of privacy preserving smart semantic search based on conceptual graph over encrypted outsourced data.Considering various semantic representation tools,we select conceptual graphs as our semantic carrier because of its excellent ability of expression and extension.To improve the accuracy of retrieval.we use tregex simplify the key sentence and make it more generalizable. We transfer CG into its linear form with some modification creatively which makes quantitative calculation on CG and fuzzy retrieval in semantic level possible.We use different methods to generate indexes and construct two different schemes with two enhanced schemes respectively against two threat models by introducing the frame of MRSE.e implement our scheme on the real data set to prove its effectiveness and efficiency.

For the further work,we will explore the possibility of semantic search over encrypted cloud data with nature language processing technology.

## REFERENCES

[1] S. Miranda-Jimnez, A. Gelbukh, and G. Sidorov, ”Summarizingconceptual graphs for automatic summarization task,” ConceptualStructures for STEM Research and Education,Springer Berlin Heidelberg, pp.245-253,2013.

[2] R. Ferreira, L. de Souza Cabral, and R. D. Lins, ”Assessing sentence scoringtechniques for extractive text summarization,Expertsystems with applications,vol.40,no.14,pp.5755-5764, 2013.

[3] M. Liu, R. Calvo, and A. Aditomo, ”Using wikipedia and conceptual graph structures to generate questions for academic writing support,” Learning Technologies,IEEE Transactions on, vol.5,no.3, pp.251-263,2012.

[4] M. Heilman, and N. A. Smith, ”Extracting simplified statementsfor factual question generation ,” Proceedings of QG2010: The ThirdWorkshop on Question Generation, pp.11-20,2010.

[5] D. X. Song, D. Wagner, and A. Perrig, ”Practical techniques forsearches on encrypted data,” Proceedings of Security and Privacy,2000IEEE Symposium on, pp.44-55,2000.

[6] Y. -C. Chang and M. Mitzenmacher, ”Privacy preserving keywordsearches on remote encrypted data,” Proceedings of ACNS, pp.391-421,2005.

[7] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, ”Searchablesymmetric encryption: improved definitions and efficient constructions,” Proceedings of ACM CCS, pp.79-88,2006.

[8] C. Wang, N. Cao, and J. Li, ”Secure ranked keyword search overencrypted cloud data,” Proceedings of Distributed Computing Systems(ICDCS),2010 IEEE 30th International Conference on, pp.253-262,2010.

[9] N. Cao, C. Wang, and M. Li, ”Privacy-preserving multi-keywordranked search over encrypted cloud data,”Parallel and Distributed Systems,IEEE Transactions on, vol.25,no.1, pp.222-233,2014.

[10] W. Sun, B. Wang, and N. Cao, ”Privacy-preserving multi-keywordtext search in the cloud supporting similarity-based ranking,” Proceedings of the 8th ACM SIGSAC symposium on Information,computerandcommunicatio nsecurity, pp.71-82,2013.

[11] R. Li, Z. Xu, and W. Kang, ”Efficient multi-keyword rankedquery over encrypted data in cloud computing,” Future GenerationComputer Systems, vol.30, pp.179-190,2014.

[12] Z. Fu, X. Sun, and Q. Liu, ” Achieving Efficient Cloud SearchServices: Multi-keyword Ranked Search over Encrypted CloudData Supporting Parallel Computing,” IEICE Transactions on Communications, vol.E98-B,no.1, pp.190-200,2015.

[13] Z. Xia, X. Wang, and X. Sun, ”A Secure and Dynamic Multikeyword Ranked Search Scheme over Encrypted Cloud Data,”Parallel and Distributed Systems,IEEE Transactions on, vol.27,no.2,pp.340-352,2015.

[14] Z. Fu, J. Shu, and X. Sun, ”Semantic keyword search based on trie over encrypted cloud data,” Proceedings of the 2nd internationalworkshop on Security in cloud computing, ACM, pp.59-62,2014.

[15] J. F. Sowa, ”Conceptual structures: information processing in mind andmachine,” 1983.

[16] J. F. Sowa, Conceptual Graphs. In: Handbook of Knowledge Representation, pp.213-237,2008.

[17] J. Zhong, H. Zhu, and J. Li, Conceptual graph matching for semantic search. Conceptual structures: Integration and interfaces, SpringerBerlin Heidelberg, pp.92-106,2002.

[18] G. S. Poh, M. S. Mohamad, and M. R. Zaba, Structured encryption for conceptual graphs. Advances in Information and Computer Security, Springer Berlin Heidelberg, pp.105-122,2012.

[19] S. Hensman, and J. Dunnion, ”Automatically building conceptualgraphs using VerbNet and WordNet,” Proceedings of the 2004 international symposium on Information and communication technologies,Trinity College Dublin, pp.115-120,2004.

[20] W. K. Wong, D. W. Cheung, and B. Kao, ”Secure KNN computation on encrypted databases,” Proceedings of the 2009 ACM SIGMODInternational Conference on Management of data, pp.139-152,2009.

[21] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, ”Enabling Personalized Search over Encrypted Outsourced Data with EfficiencyImprovement,” Parallel and Distributed Systems,IEEE Transactions on,vol.27,no.9, pp.2546-2559,2016.

[22] Z. Fu, X. Sun, S. Ji, and G. Xie, ”Towards Efficient Contentaware Search over Encrypted Outsourced Data in Cloud,” The 35thAnnual IEEE International Conference on Computer Communications(IEEE INFOCOM), San Francisco,CA,2016, DOI: 10.1109/INFOCOM.2016.7524606.

[23] S. Zerr, E. Demidova, D. Olmedilla, W. Nejdl, M. Winslett, andS. Mitra, ”Zerber: r-Confidential Indexing for Distributed Documents,” Proc. 11th Int’l Conf. Extending Database Technology (EDBT’08), pp.287-298,2008.

[24] J. Zobel and A. Moffat, ”Exploring the Similarity Space,” ACMSIGIR Forum, vol.32, pp.18-34,1998.

[25] C. Chen, X. Zhu, P. S, J. Hu, S. Guo, Z. tari, and A. Y. Zomaya, ”Anefficient privacy-Preserving Ranked Keyword Search Method,” Parallel and Distributed Systems,IEEE Transactions on, 2015.

[26] Z. Fu, F. Huang, X. Sun, A. V. Vasilakos, and C. Yang, ”EnablingSemantic Search based on Conceptual Graphs over EncryptedOutsourced Data,” Services Computing,IEEE Transactions on, 2016.DOI:10.1109/TSC.2016.2622697.

[27] S. Kamara, C. Papamanthou, and T. Roeder, ”Dynamic searchablesymmetric encryption,” Proceedings of the 2012 ACM conference onComputer and communications security, pp.965-976,2012.

[28] R. Curtmola, J. Garay, and S. Kamara, ”Searchable symmetricencryption: improved definitions and efficient constructions,” Proceedings of the 13th ACM conference on Computer and communicationssecurity, pp.79-88,2006.

[29] M. Chase, and S. Kamara, ”Structured encryption and controlleddisclosure,” In Advances in Cryptology-ASIACRYPy 2010,SpringerBerlin Heidelberg, pp.577-594,2010.

[30] R. D. Lins, and S. J. Simske, ”A multi-tool scheme for summarizingtextual documents,” Proceedings of 11st IADIS international conferenceWWW/INTERNET, pp.1-8,2012.
[31] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, ”Towards Effi-cient Multi-keyword Fuzzy Search over Encrypted Outsourced
Data with Accuracy Improvement”, IEEE Transactions on Information Forensics and Security, vol.11,no.12, pp.2706-2716,2016. DOI:10.1109/TIFS.2016.2596138.

[32] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, ”APrivacypreserving and Copy-deterrence Content-based Image Retrieval Scheme in Cloud Computing,” IEEE Transactions on Information Forensics and Security, 2016. DOI:10.1109/TIFS.2016.2590944.

[33] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, ”Mutual VerifiableProvable Data Auditing in Public Cloud Storage,” Journal of InternetTechnology, vol.16,no.2, pp.317-323,2015.

[34] B. Gu, and V. S. Sheng, ”A Robust RegularizationPath Algorithm for -Support Vector Classification,” IEEETransactions on Neural Networks andLearning Systems,2016;DOI:10.1109/TNNLS.2016.2527796.

[35] G. Sankareeswari, S. Selvi, and R. Vidhyalakshmi, ”Enabling secure outsourced cloud data,” Information Communication and Embedded Systems (ICICES), 2014 International Conference on, IEEE, pp.1-6,2014.

[36] J.Wang, X. Chen, and X. Huang, ”Verifiable auditing for outsourced database in cloud computing,” IEEE Transactions on Computers, vol.64,no.11, pp.3293-3303,2015.

[37] F. Cheng, Q. Wang, and Q. Zhang, ”Highly Efficient Indexing forPrivacy-Preserving Multi-keyword Query over Encrypted CloudData,” International Conference on Web-Age Information Management,pp.348-359,2014