# SURVEY ON SECURITY ENHANCEMENT ON QUERY TRANSFORMATION WITH RANDOM SPACE PERTURBATION

NIVEDHITHA S

***Abstract*— Cloud computing provides a reliable, customized, and guaranteed computing and a dynamic environment for end users. For online data analytics,the range query is one that is used as a most frequently used queries.The Providers Providing such a query service could be expensive for the data owner to host their data. Now with the development of services and cloud computing, it has become possible to data owners for hosting their data in large outsource databases to database service providers and let the range query service are maintained by the service providers. The random space perturbation (RASP) and data perturbation method is used to provide a secure and efficient range query and kNN query services for protected data in the cloud. The RASP data perturbation method has a combination of some features such as: encryption of order preserving, expansion of dimensionalities, random noise injection, and random projection. These features are used to provide strong resilience to attacks on the perturbed data and queries. On the other hand, a secure outsourced service should still provide efficient query processing and significantly reduce the in house workload to fully realize the benefits of outsourcing Efficient query processing.To enhance the security in query transformation a kd tree with RAndom Space Perturbation (RASP) approach is proposed.**

***Index Terms*— Query services in the cloud, privacy, range query, kNN query, RASP Method, kd tree**

## I.INTRODUCTION

Today's modern life is totally based on Internet. Now a day's people cannot imagine life without Internet. Also, the people do not want internet without security. They need the privacy for their data on the internet without confidentiality the data owner does not want to move their data to cloud. Hosting data-intensive query services in the cloud is increasingly popular because of the unique advantages in scalability and cost-saving by means of the cloud infrastructures the service owners can expediently scale up or down the service and only pay for the hours of using the servers. This is a smart feature because the workloads of query services are highly dynamic and it will be expensive and inefficient to serve such dynamic workloads with in-house infrastructures. The data in the cloud lose the control because of service providers. Data confidentiality and query privacy have become the major concerns. Adversary such as curious service providers can possibly make a copy of the database or eavesdrop users' queries which will be difficult to detect and prevent in the cloud infrastructures. as new approach are needed to protect data confidentiality and query privacy the efficiency of query services and the benefits of using the clouds should also be preserved. It will not be significant.[1]. Cloud computing is the long dreamed vision of computing. Its great flexibility and economic savings are motivating both individuals and enterprises to outsource their local complex data management system into the cloud, especially when the data produced by them that need to be stored and utilized is rapidly increasing. To protect data privacy and combat unsolicited accesses in cloud and beyond, sensitive data, e.g., emails, personal health records, photo albums, tax documents, financial transactions, etc., may have to be encrypted by data owners before outsourcing to commercial public cloud . "Coordinate matching" i.e., as many matches as possible, is an efficient principle among such multi-keyword semantics to refine the result relevance, and has been widely used in the plaintext information retrieval (IR) community. However, how to apply it in the encrypted cloud data search system remains a very challenging task because of inherent security and privacy obstacles, including various strict requirements like data privacy, index privacy, keyword privacy, and many others[2]. Range query is the most frequently used query in online data analytics (OLAP) that requires the service provider to quickly respond to concurrent user queries. To efficiently process range queries, indexing is a necessary step. However, most existing encryption approaches require linear scan over the entire database, thus, impractical for OLAP. Fully homomorphic encryption in theory allows any operation on encrypted data that can be traced back to an equivalent operation on the corresponding plaintexts. However, as the author of mentioned, this is still too expensive to be practical

***Manuscript received March, 2015***.

*Ms.S.**Nivedhitha.**, Information Technology IFET College of Engineering., Villupuram, India,*



ISSN: 2278 – 7798 

even for a simple application like encrypted keyword search Several methods that consider different tradeoffs between data security and efficiency of query processing were proposed in the recent years. Both Crypto-index and order-preserving encryption (OPE) assume the attacker does not have sufficient prior knowledge about the data; thus powerful attacks cannot be conducted. Specifically, they assume the attacker knows only the ciphertext. However, we have found that if the attacker has some prior knowledge, such as the attribute domains (maximum and minimum values), the attribute distributions, and even a few pairs of plaintext and ciphertext, these encryption methods will be vulnerable to attacks.[3]. Symmetric searchable encryption can be achieved in its full generality and with optimal security using the work of Ostrovsky and Goldreich on oblivious RAMs More precisely, using these techniques any type of search query can be achieved (e.g., conjunctions or disjunctions of keywords) without leaking any information to the server,(i.e., which documents contain the keyword).

## II.LITERATURE SURVEY

In this section, we are focus on the different methods for enhancing the security to the query services.[1] "Exploiting RASP Data Perturbation for Building Confidential and Query Services in the Cloud", Describes the Exploitation of RASP Data Perturbation for Building Confidential and Query Services in the Cloud. Thus the RASP provides exclusive security features. It aims to protect the topology of the query range in the disturbed space and allows using indices for efficient range query processing. With the topology conserve features we are able to build up efficient range query services to achieve sub linear time complexity of processing queries. We can develop the kNN query service based on the range query service. Cloud computing services enable organizations and individuals to outsource the management of their data to a service provider in order to save on hardware investments and reduce maintenance costs. The safety of both the troubled data and the protected queries is carefully analyzed under a precisely defined danger model. We also do some sets of experiment to show the efficiency of query processing and the low cost of inhouse processing.[2] "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Describes,The Defining and Solving the challenging problem of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE) were made, and establishing a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. Among various multi-keyword semantics,we choose the efficient principle of "coordinate matching", i.e., as many matches as possible, to capture the similarity between search query and data documents, and further use "inner product similarity" to quantitatively formalize such principle for similarity measurement. The first proposal is based on a basic MRSE scheme using secure inner product computation, and then significantly improve it to meet different privacy requirements in two levels of threat models. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given, and experiments on the real-world dataset further show proposed schemes indeed introduce low overhead on computation and communication.Thus the advantage of this system is Multi-keyword ranked search over encrypted cloud data (MRSE) and the "Coordinate matching" by inner product similarity.The main draw back is the searchable encryption focuses on single keyword search or Boolean keyword search, and rarely differentiates the search results.[3] "RASP: Efficient Multidimensional Range Query on Attack- Resilient Encrypted Databases," Describes about the Most existing encryption based approaches require linear scan over the entire database, which is inappropriate for online data analytics on large databases. While a few encryption solutions are more focused on efficiency side, they are vulnerable to attackers equipped with certain prior knowledge. Thus the proposed work consists of the Random Space Encryption (RASP) approach that allows efficient range search with stronger attack resilience than existing efficiency focused approaches. Thus the use of RASP to generate indexable auxiliary data that is resilient to prior knowledge enhanced attacks. Range queries are securely transformed to the encrypted data space and then efficiently processed with a two stage processing algorithm.Thus, the potential attacks on the encrypted data and queries at three different levels of prior knowledge available to an attacker. [4] "Searchable Symmetric Encryption: Improved Definitions



ISSN: 2278 – 7798 

and Efficient Constructions," Describes that the Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. The area of searchable encryption has been identified by DARPA as one of the technical advances that can be used to balance the need for both privacy and national security in information aggregation systems .

## III.CONCLUSION

In this paper our proposed system apply, a kd tree with RAndom Space Perturbation (RASP) approach. *k*-d trees are a useful data structure for several applications, such as searches involving a multidimensional search key.The RASP perturbation is designed to securely transform the ranged queries into polyhedra in the RASP-perturbed data space.Finally we are able to identify the authorized and unauthorized users,if any third party user tries to hack the data it simply block and drop their request. So,the utility for processing range queries is preserved.Thus, we are able to minimize the in-house processing workload because of the low perturbation cost and high precision query results.

## IV.FUTURE WORK

The security of both the perturbed data and the protected queries is carefully analyzed under a precisely defined threat model. And the efficiency of query processing and the low cost of in-house processing is achieved. The Future Enhancement is based on three aspects: 1) further improve the performance of query processing for range queries, 2) formally analyze the access patterns and the possible effect on both data and query confidentiality and 3)Allow the trusted user to view the file for their usage.Moreover,it is just a beginning further the system may be utilized in various other types of storage systems viz.Cloud storage system or similar process applications.

## REFERENCES

[1] S.Priyanga, Mrs. S.Lalitha, "Exploiting RASP Data Perturbation for Building Confidential and Query Services in the Cloud", International Journal of Research for Science Technologies & Engineering (IJRSTE) Vol-1, Issue-2, Nov-2014, ISSN 2393-8714

[2] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOMM, 2011

[3]. K. Chen, R. Kavuluru, and S. Guo, "RASP: Efficient Multidimensional Range Query on Attack- Resilient Encrypted Databases," Proc. ACM Conf. Data and Application Security and Privacy, pp. 249-260, 2011

[4] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," Proc. 13th ACM Conf. Computer and Comm. Security, pp. 79-88, 2006.

[5] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order Preserving Encryption for Numeric Data," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD), 2004.

[6] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.K. Andy Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," technical report, Univ. of Berkerley, 2009.

[7] J. Bau and J.C. Mitchell, "Security Modeling and Analysis," IEEE Security and Privacy, vol. 9, no.3, pp. 18-25, May/June 2011.

[8] S. Boyd and L. Vandenberghe, Convex Optimization. Cambridge Univ. Press, 2004.

[9] K. Chen and L. Liu, "Geometric Data Perturbation for Outsourced Data Mining," Knowledge and Information Systems, vol. 29, pp. 657-695, 2011.

[10] K. Chen, L. Liu, and G. Sun, "Towards Attack-Resilient Geometric Data Perturbation," Proc. SIAM Int'l Conf. Data Mining, 2007.

## AUTHOR BIOGRAPHY

**Ms.S.Nivedhitha** Currently pursuing B.Tech,Information Technology at IFET College of Engineering, Villupuram,India. Her area of interests includes Computer Networks,Web Technology,Object Oriented Analysis and Design.



ISSN: 2278 – 7798 