**International Journal of Web Services Research**
Volume 21 • Issue 1

# A Secure and Fast Range Query Scheme for Encrypted Multi-Dimensional Data

Zhuolin Mei, Jiujiang University, China
Huilai Zou, Zhejiang Institute of Mechanical and Electrical Engineering, China*
Jinzhou Huang, Hubei University of Arts and Science, China
Caicai Zhang, Zhejiang Institute of Mechanical and Electrical Engineering, China
Bin Wu, Jiujiang University, China
Jiaoli Shi, Jiujiang Key Laboratory of Cyberspace and Information Security, China
Zhengxiang Cheng, Jiujiang University, China

## ABSTRACT

In recent years, more and more data has been stored on the cloud to provide various services. These data often contain users' private information, which inevitably raises concerns about data security. Encryption before outsourcing is a direct solution to mitigate these concerns. However, traditional encryption schemes such as block encryption make basic data services hard to support. Therefore, this paper proposes a secure and fast range query scheme for encrypted multi-dimensional data, called SFRQ. The scheme constructs a secure index over the ciphertexts of multi-dimensional data, utilizing the R-tree index, Bloom filter, and 0-1 encoding techniques. This secure index enables the cloud to provide fast range query services over the ciphertexts of multi-dimensional data. The authors have evaluated SFRQ through extensive experiments, which demonstrate its high efficiency. Additionally, the security analysis shows that no external entity, including the cloud, can obtain additional information during the entire query process.

## KEYWORDS

Ciphertext Multi-Dimensional Data, Cloud Computing, Encryption, Range Search Service, Secure Index

## INTRODUCTION

Cloud computing has been widely adopted by individuals, organizations, and businesses (Zeng et al., 2020; Mei et al., 2024). Many applications (Wang et al., 2022) have the capacity to leverage cloud servers for outsourcing their data and services, thereby improving the quality of the services they offer. Thus, the cloud often contains a substantial volume of data, which frequently encompasses sensitive information. Therefore, data security in the cloud becomes a popular research area in both academic and business communities (Zeng et al. 2017; Wu et al., 2020; Wu et al., 2021). To tackle these security concerns, one of the most straightforward approaches is to employ data encryption prior to outsourcing. Nevertheless, traditional encryption methods are difficult to support in some

DOI: 10.4018/IJWSR.340391

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

basic data operations, such as data retrieval. Although some new encryption schemes can be used to address the problem of ciphertext search, there exist some constraints.

Agrawal et al. (2004) proposed the first order-preserving encryption (OPE), which aims to incorporate order information of plaintexts into the corresponding ciphertexts. As a result, an OPE scheme is very suitable to solve the problem of ciphertext search. However, many OPE schemes (Agrawal et al., 2004; Peng et al., 2017; Popa et al., 2011; Quan et al., 2018) mainly consider ciphertext search for single-dimensional data (Zhan et al., 2022). Moreover, due to the disclosure of order information caused by OPE schemes, this can be used to accurately deduce the plaintexts (David et al., 2004). Therefore, OPE schemes pose potential data security risks.

Bucketization schemes (Wang et al., 2013; Hore et al., 2004; Hore et al., 2012) can protect order information of ciphertexts and enable ciphertext querying. In a bucketization scheme, all the data is partitioned and placed into different buckets. The data in each bucket are treated as a unit and encrypted. Thus, the order information of ciphertexts in the same bucket can be protected well. Suppose $B$ is a bucket and $Q$ is a queried range. If $B \cap Q \neq \varnothing$, all the ciphertexts in $B$ are as the results for $Q$ and finally returned to the data user. To enhance the efficiency of bucketization schemes, researchers have proposed bucketization-based index schemes (Wang et al., 2013; Mei et al., 2018). Nevertheless, the scheme devised by Wang et al. (2013) involves many matrix operations, resulting in low efficiency. The scheme of Mei et al. (2018) exhibits suboptimal performance when dealing with datasets that have non-uniform distributions.

In this paper, we propose a secure and fast range query scheme for encrypted multi-dimensional data, namely SFRQ. In our scheme, a normal R-tree, 0-1 encoding (Gupta et al., 2001), and Bloom filter (Bloom et al., 1970) are used to construct a secure R-tree index. 0-1 encoding and a Bloom filter are used to process the minimum bounding rectangle (MBR) corresponding to each node in the R-tree. This allows each processed MBR to be securely and effectively determined whether the query range intersects with it. The data in each bucket are treated as a unit and encrypted. We conducted a large number of simulation experiments, and the results show that the proposed scheme SFRQ exhibits a high search efficiency. The contributions of this paper are as follows.

1. We have developed a secure R-tree index by leveraging a conventional R-tree, 0-1 encoding, and Bloom filter.
2. We propose a secure and fast range query scheme for encrypted multi-dimensional data, namely SFRQ, by using the proposed secure R-tree index.
3. We carry out extensive experiments to evaluate the efficiency and provide a thorough analysis of correctness and security.

## RELATED WORK

An OPE scheme was first proposed by Agrawal et al. (2004). As the order information of plaintexts is preserved in the corresponding ciphertexts, i.e., larger plaintexts correspond to larger ciphertexts, OPE enables ciphertext search without decryption. A strict definition for the security of OPE was proposed by Boldyreva et al. (2009), but unfortunately, there is no OPE that satisfies the strict definition. Therefore, they propose a weaker definition, i.e., ciphertexts are indistinguishable from the values calculated by a random increment function, and then construct an instance of OPE that meets the weaker definition. Since then, many researchers have conducted extensive studies (Boldyreva et al., 2011; Dyer et al., 2017; Krendelev et al., 2014; Teranishi et al., 2014; Xiao et al., 2012) based on the work of Boldyreva et al. (2009). However, most of these OPE schemes only study the single-dimensional data. In recent years, Zhan et al. (2022) proposed a scheme that organizes all the data in a network data structure and uses prefix encoding and a Bloom filter to process the values stored in the structure, enabling the execution of range searches on encrypted multi-dimensional data (MDD). Unfortunately, the leakage of order information in OPE is likely inevitable.

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/a-secure-and-fast-range-query-scheme-for-encrypted-multi-dimensional-data/340391

## Related Content

Knowledge Representation Technologies Using Semantic Web

Vudattu Kiran Kumar (2019). *Web Services: Concepts, Methodologies, Tools, and Applications  (pp. 1068-1076).*

www.irma-international.org/chapter/knowledge-representation-technologies-using-semantic-web/217876

Automatic Metadata Generation for Geospatial Resource Discovery

Miguel-Angel Manso-Callejoand Arturo Beltran Fonollosa (2012). *Discovery of Geospatial Resources: Methodologies, Technologies, and Emergent Applications (pp. 78-110).*

www.irma-international.org/chapter/automatic-metadata-generation-geospatial-resource/65110

Improve Distributed Client Lifecycle Control in ShadowStream

Junhua Yan, Chen Tian, Jingdong Sunand Hanzi Mao (2014). *International Journal of Web Services Research (pp. 62-78).*

www.irma-international.org/article/improve-distributed-client-lifecycle-control-in-shadowstream/124986

Exploring the Usage of Big Data Analytical Tools in Telecommunication Industry in Oman

Himyar Ali Al Jabri, Ali H. Al-Badiand Oualid Ali (2019). *Web Services: Concepts, Methodologies, Tools, and Applications  (pp. 459-472).*

www.irma-international.org/chapter/exploring-the-usage-of-big-data-analytical-tools-in-telecommunication-industry-in-oman/217845

User Cold Start Recommendation System Based on Hofstede Cultural Theory

Yunfei Liand Shichao Yin (2023). *International Journal of Web Services Research (pp. 1-17).*

www.irma-international.org/article/user-cold-start-recommendation-system-based-on-hofstede-cultural-theory/321199