International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 08 | Aug 2024 www.irjet.net p-ISSN: 2395-0072

Efficient, Accurate, and Forward Secure (EAFS) Searchable encryption Supporting Range Search

Jaba Blessy W.U[1], I.Siva Prasad Manivannan., M.E., M.B.A., [2]

[1]*PG Student, Dept. of Computer Science Engineering, Rohini College of Engineering and Technology, Kanniyakumari Tamil Nadu, India*

[2]*Professor, Dept. of Computer Science Engineering, Rohini College of Engineering and Technology, Kanniyakumari, Tamil Nadu, India.*

Abstract — *In the era of cloud computing, consumers like users, businesses, and organizations prefer to subcontract massive geographical data to public clouds after encryption for privacy and security in order to achieve convenient location-based service (LBS). Be that as it may, various hurtful digital assaults occur on those public mists in an unpredicted and hourly way. In existing framework propose a lightweight and forward-secure reach question (LS-RQ) on geologically encoded information, which sufficiently balances among security and productivity. It was costly and can be satisfactory by and by since the exact outcome just included a couple of focuses ordinarily. In this task propose the meaning of the forward protection for secure reach look. Likewise, show how three broadly utilized cryptographic devices — request safeguarding encryption (OPE), pseudorandom capability, and once cushion can be utilized to plan a proficient, precise, and forward secure (EAFS) accessible encryption conspire supporting reach search in encoded mathematical data sets. In the proposed EAFS conspire, a hidden entrance just matches the last information record that fulfills the pursuit range, and different outcomes are found iteratively utilizing the past outcome. OPE's efficiency, forward privacy, and accuracy are simultaneously guaranteed by its chain-like search and embedded ciphertexts.*

Key Words: Cipher Text, Location Based Service (LBS), Cyber-attacks, Order preserving encryption.

1. INTRODUCTION

For a variety of reasons, including the ability to access our data from any location at any time with any computing device, higher service quality, and lower costs associated with data management, cloud servers (CSs) are increasingly being used to store data. Data on our laptops and mobile devices may be automatically transferred to CSs like iCloud or OneDrive in some instances. There are known security and protection issues related with the reevaluating of information, for example, the cloud specialist co-op (CSP) gaining admittance to client contents without their unequivocal authorization. This supports the significance of accessible encryption (SE), a cryptography based plot that empowers looking in the ciphertext space without releasing any data to untrusted servers. There are a wide range of SE plans, with shifting functionalities (e.g., watchword searches and likeness look). Range look are one more typical capability in data sets that spotlights on numeric correlations, for instance to find clients somewhere in the range of 20 and 40 years of age.

The data may be processed to fit a particular data structure, such as a B-tree, in which the data are stored in order, to improve range search efficiency. This is not difficult to accomplish in the plaintext space, however not the situation when data sets are encoded. First, there is insufficient semantic information in the encrypted environment to allow for numerical comparisons. In addition, in order to verify equality, it is impractical to list all possible cases for the entire range in a search request. Second, the request between various information records is likewise touchy data. All in all, the information proprietor (DO) for the most part doesn't believe the CS should be familiar with the request between various information records, and the list shouldn't uncover the request data preceding looking. As a result, range searching in the ciphertext domain is difficult.

Bijit Hore et al. [1] proposed Secure multi-faceted reach questions over reevaluated information. Questions are assessed in a rough way where the returned set of records might contain a few misleading up-sides. These records then, at that point, should be gotten rid of by the client which contains the computational above of our plan. We foster a bucketization system for noting multi-faceted reach questions on complex information. We estimate the client's computational overhead and disclosure risk for a given bucketization scheme using cost and disclosure risk metrics. Shabnam Kasra Kermanshahi et al. [2] proposed

Mathematical Reach Search on Scrambled Information. This article presents two powerful symmetric accessible encryption plans for mathematical reach search. Our developments are quick to give forward/in reverse security with regards to SSE-based plans supporting mathematical reach search. Plus, we characterize a security thought called content protection. Leaks that are crucial in the context of geometric range search but are not taken into account by forward/backward security are captured in this security concept. During both search and update, content privacy eliminates leakage of updated database points.

Cong Zuo et al. [3] proposed Forward and In reverse Confidential DSSE for Reach Questions. In this article, they first give another spillage capability for range questions, which is more muddled than the one for single catchphrase questions. Besides, we propose a substantial forward and in reverse confidential DSSE conspire by utilizing a refined double tree information structure. Xiangyu Wang et al. [4] proposed Forward/In reverse and Content Confidential DSSE for Spatial Watchword Questions. Spatial catchphrase questions are appealing strategies that have been broadly. sent, all things considered, applications as of late, for example, interpersonal organizations and area based administrations. However, the solutions that are currently available neither meet the privacy requirements of actual applications nor support dynamic update. In this article, they explore the issue of Dynamic Accessible Symmetric Encryption (DSSE) for spatial catchphrase questions. Kaiping Xue et al. [5] proposed Secure two-cloud database for numerically related SQL range queries. Businesses and people reevaluate data set to acknowledge advantageous and minimal expense applications and administrations. Numerous secure database strategies have been proposed in order to provide SQL queries with sufficient functionality. Notwithstanding, such plans are defenseless against security spillage to cloud server. Ke Cheng et al. [6] designed Emphatically Secure and Effective Reach Questions in Cloud Data sets under Various Keys. propose a safe cloud data set supporting reach questions under various keys, in which all clients could protect the privacy of their own different keys, and don't need to impart them to one another. At a more elevated level, our framework is developed on a two-cloud design and an original dispersed two-hidden entryway public key cryptosystem. Wai Kit Wong et al. [7] designed Data interoperability and secure query processing in a cloud database environment. propose and break down a safe inquiry handling framework (SDB) on social tables and a bunch of rudimentary administrators on scrambled information that permit information interoperability, which permits an extensive variety of SQL questions to be handled by the SP on encoded data. Reza Curtmola et al. [8] proposed Accessible symmetric encryption. Accessible symmetric encryption (SSE) permits a party to re-appropriate the stockpiling of its information to another party (a server) in a confidential way, while keeping up with the capacity to look through ready to be done specifically. This issue has been the focal point of dynamic examination as of late. In this paper we show two answers for SSE that at the same time partake in the accompanying properties: In comparison to all previous constant-round schemes, both solutions are more effective. Specifically, the work performed by the server per returned record is consistent rather than direct in the size of the information. Ioannis Demertzis et al. [9] proposed Deep and Practical Private Range Search In this article, they adopt an interdisciplinary strategy, which joins the meticulousness of safety details and confirmations with effective information the board methods. They develop a wide arrangement of novel plans with practical security/execution compromises, taking on the idea of Accessible Symmetric Encryption (SSE), principally proposed for watchword search. Rui Li et al. [10] proposed Range query processing that is quick and scalable. They propose the principal range inquiry handling plan that accomplishes list vagary under the lack of definition against picked watchword assault (IND-CKA). Our key thought is to sort out ordering components in a total paired tree called PBtree, which fulfills structure lack of definition.

2. METHODOLOGIES

In this article, present the proper definition for forward protection in range searches, and afterward propose a proficient, precise, and forward secure (EAFS) SE plot that fulfills this definition. To be explicit, our plan accomplishes secure reach search in a solitary CS model, and the precise outcomes can be gotten without repetitive cooperations and postprocessing tasks. There are two parts to the search phase. The first step is to locate the dataset that completely fulfills the search request, followed by the second step, which is to locate the dataset that only partially fulfills the search request and then compare the two datasets in order to return the correct results. As a result, the size of the aforementioned datasets has an impact on the level of difficulty of the search. Prior to a search, order and similarity information are hidden, and forward privacy is ensured when the data records are updated.

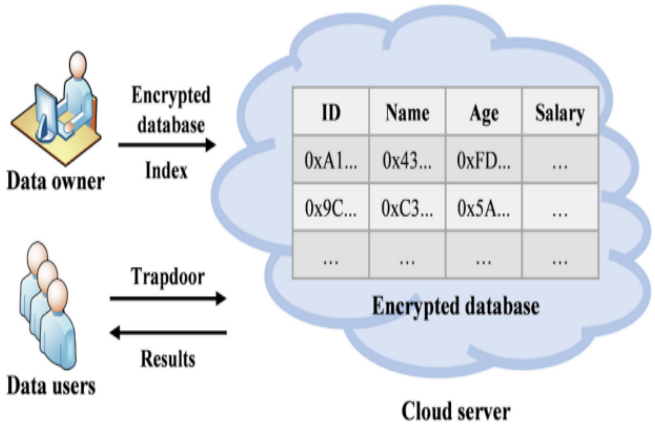


FIG 1. System Architecture

2.1 DESIGN RATIONALE

We are able to draw the conclusion that a straightforward cryptographic technology or tool cannot simultaneously guarantee the safety, effectiveness, and accuracy of range searches in encrypted databases. In this way, we expand on the onions of encryption, which is a multi-facet structure that stores numerous ciphertexts minimally. A secure range search's design can be guided by the security or functionality properties provided by each layer. Take note that the secure range search is impractical because its complexity is proportional to the size of the database—that is, the total number of data records. An index that speeds up th range search should be created by processing the original data records (bucketing). What's more, a deterministic encryption (i.e., PRF) is expected to really take a look at the correspondence and safeguard the security of the record. It is inescapable that a few bogus up-sides will exist as a tradeoff for expanding the effectiveness. To compare the ciphertexts, a functional encryption, such as OPE, is required. In any case, PRF and OPE are two more vulnerable encryption plans. The PRF uncovers which encoded values connect with the equivalent plaintext, which can be effortlessly undermined by the record infuse assault. The order of the initial data records is shown by the OPE. In this manner, a more grounded encryption (i.e., once cushion) is expected to ensure the security of the reach search. At long last, the chain-like pursuit executes the protected reach search where the intricacy just connects with the quantity of results fulfilling the inquiry solicitation and a few bogus up-sides during the whole hunt process, as well as guaranteeing the forward security.

2.2 INITIALIZATION

To accomplish a safe reach search, a few boundaries should be created in the introduction stage. We expect that the information base Dmn is to be moved to CS. To begin with, DO produces a guide capability M to preprocess the information records in Dmn. Without loss of consensus, the guide capability is characterized by similarly partitioning the scope of each property into a decent number of (e.g., f) consistent sub-ranges, which produces fm cans. Then, to achieve the protected reach search, two records should be produced. As referenced over, the state file σ is instated as {⟨B_1,0⟩,⟨B_2,0⟩,… … ,⟨B_(|B|),0⟩}, and the encoded data set EDB is introduced as ∅. By contributing the security boundary λ DO produces two mystery keys, KPRF and KOPE, which are utilized to assemble the encoded data set EDB.

2.3 UPDATE OF AN ENCRYPTED DATABASE

To refresh information, the accompanying necessities should be met. To start with, the update for an information record just rolls out little improvements on the file, which guarantees the productivity of the update. Second, forward privacy is ensured by the fact that the newly updated data record has no connection to any of the previous entities in the encrypted database. Third, the delicate data spilled from the list is limited to the degree conceivable.

2.4 GENERATION OF THE TRAPDOOR

The state index will be required as an input if DU generates a trapdoor because it contains counters representing the number of data records stored in each bucket, which is considered sensitive information about the database. The counters connected with the hunt range are required, yet the counters out of the pursuit range are uncovered. If DO produces a hidden entrance, he/she should realize the hunt range, which likewise can be viewed as touchy data about DU. As a result, you should be able to meet the following requirements. To start with, DU just acquires the counters that he/she wants, doesn't however advance anything about different ones in the state record. Second, DO has no knowledge of the DU query.

2.5 SECURE RANGE SEARCH

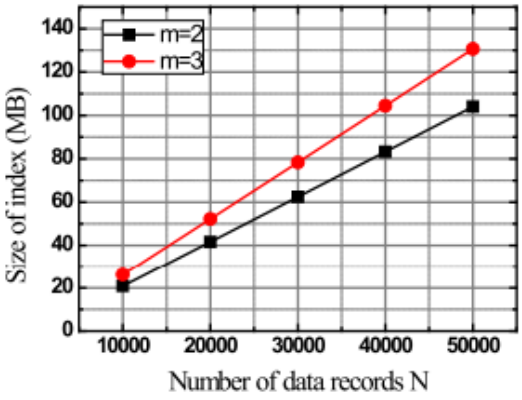
When carrying out the search procedure, it is necessary to satisfy the following requirements. To start with, the pursuit productivity connects with the size of results that fulfills the hunt demand, which empowers our plan to be utilized in enormous scope data sets. Second, the accuracy and completeness of the secure range search's output guarantees the search's quality. Thirdly, DU has a great experience because there is no additional interaction

between CS and DU or any post-process operation implemented by DU.

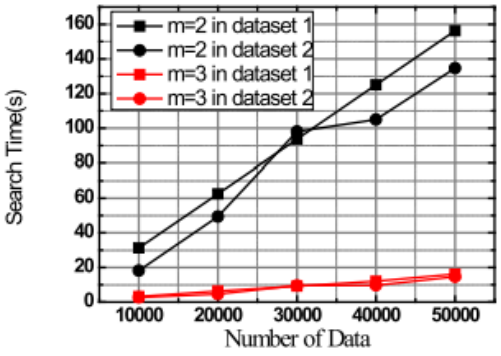
2.5 EVALUATION OF PERFORMANCE

In this section, We look at how well our plan works. We used both an artificial dataset, i.e., a manmade uniform distribution dataset known as dataset 1, and an actual dataset, i.e., the diabetes dataset1 in the UCI Machine Learning Repository known as dataset 2, because the distribution of the data has a strong correlation with the computational cost of a secure range search. The Python programming language is used to write the code for our scheme's entire procedure. Our computer simulated DO and DU. We used the real CS of Microsoft Azure to store the encrypted database and carry out the secure range search to guarantee the viability of our plan.

RESULT AND DISCUSSION

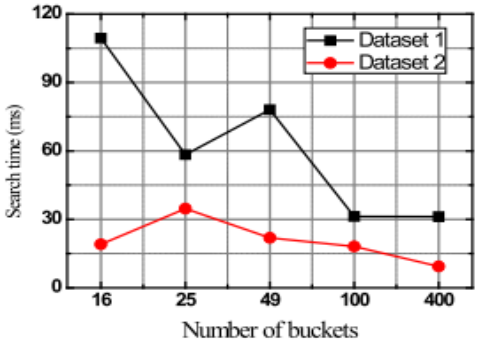


(a)

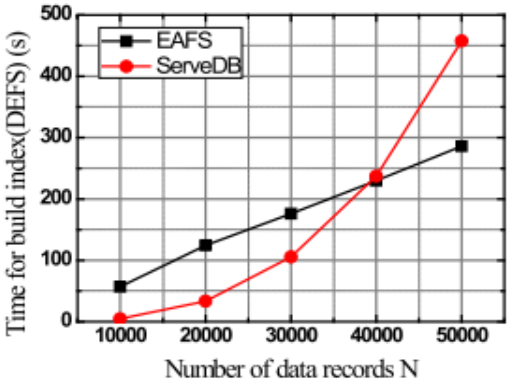


(b)

Fig -2 (a) Size of index (b) Computation cost for different number of data records



(a)



(b)

Fig -3 (a) Computation cost for different number of buckets (b) Computation cost for building index

Fig. 2(a) shows the relationship between the size of the index (aka., EDB) and the number of data records. The record put away in CS is a word reference with a key-esteem pair that is figured by the solid hash capabilities. The length of the word reference connects with the quantity of information records in the data set. As a result, as the number of data records increased, so did the size of the index. There would be more ciphertexts encrypted by OPE as the dimensions increased. The size of the record expanded straightly as the quantity of aspects expanded. Fig. 2(b) depicts the relationship between the number of data records and the amount of computation required for secure range search. The EAFS's search complexity is O(Q + F), where Q is the number of data that satisfy the query and F is the number of false positive data, as previously mentioned. When the number of attributes is taken into account, we set the number of (Q + F) to be almost 2% of the dataset's total number. Figs. 3(a) and (b) show the connection between the calculation cost of our plan and the absolute number of containers, |B|. Assuming the complete number of cans is little, and that implies that the scope of each pail is wide,

more bogus positive information records are looked for a similar inquiry token, in this way, hence, the hunt time will increment.

CONCLUSION

The proposed the definition of forward privacy in range search, as well as the creation of an EAFS SE scheme that makes it possible to perform secure range searches in encrypted databases. The computational expense for a reach search in our EAFS just connects with the quantity of results that fulfill the question and the quantity of bogus up-sides in the converging containers. Forward privacy is achieved because the chain-like search guarantees that any newly updated data entities have no connection to the previous data. We additionally assessed the security and execution of our way to deal with exhibit the utility of the EAFS.

REFERENCES

[1] Cong Zuo; Shi-Feng Sun; Joseph K. Liu et al. Forward and Backward Private DSSE for Range Queries, IEEE Transactions on Dependable and Secure Computing,2022

[2] Xiangyu Wang; Jianfeng Ma; Ximeng Liu. Forward/Backward and Content Private DSSE for Spatial Keyword Queries, IEEE Transactions on Dependable and Secure Computing, 91-48,2023

[3] K. Xue, S. Li, J. Hong et al. Two-cloud secure database for numeric-related SQL range queries with privacy preserving, IEEE Transactions on Information Forensics and Security, 2017.

[4] K. Cheng et al. Strongly secure and efficient range queries in cloud databases under multiple keys, IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, 2019.

[5] W. Wong, B. Kao, D. W. Cheung et al. Secure query processing with data interoperability in a cloud database environment, Secure query processing with data interoperability in a cloud database environment, 2014, pp. 1395–1406.

[6] R. Curtmola, J. Garay et al. Searchable symmetric encryption: Improved definitions and efficient constructions, ACM digital library, 2006.

[7] I. Demertzis et al. Practical private range search in depth, ACM Transactions on Database Systems Vol. 43, No. 1.

[8] R. Li, A. Liu et al. Fast and scalable range query processing with strong privacy protection for cloud computing, IEEE/ACM Transactions on Networking Volume: 24, Issue: 4, August 2016.

[9] B. Hore, S. Mehrotra, M. Canim, and M. Kantarcioglu et al. Secure multidimensional range queries over outsourced data. The VLDB Journal, 2012.

[10] Shabnam Kasra Kermanshahi; Shi-Feng Sun et al. Geometric Range Search on Encrypted Data With Forward/Backward Security. IEEE Transactions on Dependable and Secure Computing , Volume:19, 2022.