International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

Spatial Data With Range Search With Encryption

Bandi Harish & A.Ramesh Babu
1 Pg Scholar, Department Of Cnis, Vaagdevi College Of Engineering
2 Asst.Professor, Department Of Cse, Vaagdevi College Of Engineering

ABSTRACT

Geometric range search is a fundamental primitive for spatial data analysis in SQL and NoSQL databases. It has extensive applications in location-based services, computer aided design, and computational geometry. Due to the dramatic increase in data size, it is necessary for companies and organizations to outsource their spatial data sets to third-party cloud services (e.g., Amazon) in order to reduce storage and query processing costs, but, meanwhile, with the promise of no privacy leakage to the third party. Searchable encryption is a technique to perform meaningful queries on encrypted data without revealing privacy. However, geometric range search on spatial data has not been fully investigated nor supported by existing searchable encryption schemes. In this paper, we design a symmetric-key searchable encryption scheme that can support geometric range queries on encrypted spatial data. One of our major contributions is that our design is a general approach, which can support different types of geometric range queries. In other words, our design on encrypted data is independent from the shapes of geometric range queries. Moreover, we further extend our scheme with the additional use of tree structures to achieve search complexity that is faster than linear. We formally define and prove the security of our scheme with indistinguish ability under selective chosen-plaintext attacks, and demonstrate the performance of our scheme with experiments in a real cloud platform (Amazon EC2).

1. INTRODUCTION

With advancements in the cloud computing, greater demands arise for the storage and security analysis. The origin of the cloud computing is from the development of parallel computing, distributed computing, grid computing with the evolution of virtualization and utility computing. Generally, the services of cloud computing is segmented into Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Services (PaaS) [1]. It works on the basis of 'Pay-per-use-on' model which can conveniently access the shared IT resources via web modules. The cloud technology offers unlimited resources and services to manage the outsourced data. With further improvements, the support of dynamic

data is initialized. These features attracted the cloud users to store massive amount of information to this system [2]. Searchable encryption [3] is the stereotype of encryption technique which most recently studied by research community. It executes search operations on the encrypted databases. By doing that, the privacy of the data should be obtained from semi-trusted third party service providers. The cloud users are unaware about their data location. Thus, the client performs search operation over the server and obtains its results. Prior work depicts that the server's execution from the result set of encrypted documents and its security parameters like data dimension and documents. Better the privacy design, better the search operation. Reachability is one of the parameters that depict the available of the resources over given time e.g. social behavior analysis, recommendations model, public services etc. The location of the user is dynamic one. The user's location can notified from Location Based Services (LBS) [4] such as Google Maps, Foursquare etc. This scenario motivates to study about the reachability analysis of cloud data. Since, the data volume increases, the need for LBS companies are increased. In order to provide better information retrieval process, the security and privacy issues should be devised properly [5]. Though the concept of searchable encryption is examined previously, the security and privacy challenges are not yet accomplished. Some additional security index was used for the data search process. In this paper, we suggest a geometric range search process over the encrypted data, so as to enhance the data privacy. Geometric queries are the queries that deal with spatial data. The data is denoted as 'points' and queries are portrayed as geometric objects like triangle, spheres and rectangles.

2. RELATED WORK This section describes the prior work carried out by researchers. Previously, data utilization method is performed over the plaintext search. Due to increase of the cloud users, search operation is given importance. Usually, Boolean search operation [6] was performed over the server to yield better results. This search fails to give better security to the cloud data. The data is being stored to cloud using 'innerproduct similarity'. Search over encrypted data is still in its infancy. Initially, multi-keyword ranked search was introduced by finding the association. Further, k-NN classification technique is used for generating the security index. secure index was obtained from mini-hash include cryptography, image processing and information retrieval [7]. The schema contains hash functions and inverted visual words. It yields slow performance in inverted visual words. The theme of cryptographic provide secure systems.

The method incurs higher storage overhead and not guarantees the security. The author in [8] studied about the issue of CSP towards search operations. Similarly, authentication model was also suggested the data access. Their technique purely works as Public key encryption. The computational cost of decrypting the data was wisely reduced. The author in [9] authorized data privacy systems. They defined t algorithms which depicts searching efficiency and privacy of the query. It was executed on personal health records of healthcare applications. It fails to support synonyms or morphological variants are used. In [10], the author suggested an alternate scheme to handle synonyms variants. Cong method drastically lessened the processing cost and network traffic. It eliminates the search barriers in the information retrieval systems proposed other methods named, 'Ranked Searchable Symmetric Encryption', 'Order persevering symmetric encryption' and 'One many order preserving mapping Their method solved irrelevant data and traffic issues. It didn't cooperate for the query matching. The author in [11] framed search method based on Identity based Encryption. Their method supported a single query as well as multi queries. Any cloud users can access the data but only authorized users permit to edit the data. The author in [12] suggested predictive based encryption technique that supports hierarchical functioning systems. It is computationally expensive. Confidentiality is one of the security parameters the encrypted data in cloud. It wisely makes order system. Depending on encrypted queries it ranks the documents and document having most rank will be pushed up using ranked method. The given method is well suited for large documents and also it provides higher accuracy and security. But for this method computational cost is high and protecting communication link is bit difficult task. the author studied about the attribute based encryption model. The attribute based model is merged with the predictive encryption scheme. In order to makes the faster, a highly secured retrieval system was framed. Keyword plays an important role in both attribute and predictive based encryption. By doing so, privacy of the data is assured. Still, the challenges like keywords refreshment, channel elimination and multi-keyword processing. Though it maintains the secret data but fails to support integrity and privacy design. The study was further enhanced and introduced locality based searching technique. It is highly effective than the hashing techniques. Since, it's a one process, the resultset doesn't meet the user's requirements. The author in [14] framed a privacy preserving model search operation is carried out in two phases, namely, Ranked over keyword search, search over structured data. NN classification

urity index. The hash sketches that cryptography, image processing and information hash functions and inverted visual words. It yields slow performance in inverted The theme of cryptographic model is to method incurs higher storage The author in [8] ied about the issue of CSP towards search operations. n model was also suggested the data access. Their technique purely works as Public key The computational cost of decrypting the data [9] suggested an They defined two algorithms which depicts searching efficiency and privacy It was executed on personal health records of It fails to support synonyms or suggested an alternate scheme to handle method drastically lessened the processing cost and network traffic. It eliminates the search barriers in the information retrieval systems. And they also proposed other methods named, 'Ranked Searchable Order persevering symmetric One many order preserving mapping'. irrelevant data and traffic issues. It The author in [11] framed search method based on Identity based Encryption. Their method supported a single query as well as multiAny cloud users can access the data but only The author in [12] based encryption technique that supports hierarchical functioning systems. It is Confidentiality is one of the security parameters used over makes use of ranking ystem. Depending on encrypted queries it ranks the documents and document having most rank will be pushed up using ranked method. The given method is well suited for large documents and also it provides higher accuracy and putational cost is high and protecting communication link is bit difficult task. In [13], studied about the attribute based encryption The attribute based model is merged with the makes the system faster, a highly secured retrieval system was framed. in both attribute and By doing so, privacy of the data the challenges like keywords refreshment, keyword processing. Though it maintains the secret data but fails to support integrity and The study was further enhanced and based searching technique. It is highly Since, it's a one-way , the resultset doesn't meet the user's requirements. framed a privacy preserving model. The two phases, namely, Ranked over keyword search, search over structured data. Though confidentiality parameter is achieved, over encrypted data was unsuccessful. studied about the confidentiality, verifiability and security of their proposed algorithm. The parameter verifiability was achieved by performing cross encrypted data. They also studied about the system to provide privacy.

3. PROPOSED WORK The proposed work is purely based on Symmetric Key Encryption scheme. The system model consists of three

entities, namely, data owner, data user and cloud server. The task of data owner is to preserve the data at cloud server, eventually focus on reducing the local cost. searched by the data user. The task of cloud server is to provide services to the data owner and data users. Since, the cloud server is semi-trusted, the cloud service is reliable. The learning of range queries over the private a challenging task. The data owner stores the data in encrypted form, to preserve The different geometric data is and then preceded in the ciphertext data. algorithm eliminates the multiple rounds of communication between server and client. Firstly, the points are denoted for data records and then range queries are determined from the set of geometric points. The proposed algorithm is explained as follows: i) Each record is symbolized as geometric points. ii) Given the input 1λ , the data owner generates the secret keys. SSW. Setup (1λ⇓SK) iii) Along the secret key, bloom filters are generated and outputs as {m, h1….hk} where length and h is the hash functions. filter contains all possible combination of ciphertext, which is further used as search token. The author in [15] confidentiality, verifiability and security of The parameter verifiability was achieved by performing cross-check condition over encrypted data. They also studied about the fuzzy logic is purely based on Symmetric Key The system model of our scheme is The system model consists of three entities, namely, data owner, data user and cloud server. The task of preserve the data at cloud server, eventually focus on reducing the local cost. The outsourced data will be searched by the data user. The task of cloud server is to provide services to the data owner and data users. Since, the trusted, the cloud service is reliable. range queries over the private information is a challenging task. The data owner stores the data in encrypted form, to preserve the spatial dataset. System Architecture Our proposed algorithm supports different and continuous The different geometric data is preprocessed and then preceded in the ciphertext data. The proposed algorithm eliminates the multiple rounds of communication Firstly, the points are denoted for and then range queries are determined from the The proposed algorithm is explained Each record is symbolized as geometric points. , the data owner generates the secret (1) Along the secret key, bloom filters are generated and } where m is the bloom filter length and h is the hash functions. In fact, the bloom filter contains all possible combination of ciphertext, which is further used as search token.

IV Encryption phase:

Afforded with secret key SK and dataset D, the data owner encrypts the data as follows: BFDi: =BF. Init (m) BFDi :=BF. Add (Di, BFDi) The

eqn. (2) and (3) will processed for all data points and the ciphertext Ci will estimated as: SSW. Enc (SK, Ui)⇓Ci Then, the encrypted dataset is C= (C1… C v) Token Generation phase (S): The search token is generated from secret key SK and geometric query Q, the data owner calculates S= {S1…St}:= EnumerateInsidePoints (Q) BFQ :=BF. Init (m) BFQ: = BF. Add (Si, BFQ), for 1≤i≤t, t points of Q. The search token, TK computes as SSW.GenToken (SK, ﺏ (⇓TK vi) Search phase: Afforded with TK and C, the cloud server returns the search results, IQ SSW. Query (TK, Ci) for 1 ≤ i≤ n.⇓Flag i For each flag, the identifier Ii is added to the The proposed algorithm works in tree structure in order to improve the search complexity. By analyzing pattern, search pattern and access pattern leakage is reduced in tree structure.

V CONCLUSION

We study a general approach to securely search encrypted spatial data with geometric range queries. Specifically, our solution is independent with the shape of a geometric range query.With the additional use of R-trees, our scheme is able to achieve faster-than-linear search complexity regarding to the number of points in a dataset. The security of our scheme is formally defined and analyzed with indistinguishability under Selective Chosen-Plaintext Attacks. Our design has great potential to be used and implemented in wide applications, such as Location-Based Services and spatial databases, where the use of sensitive spatial data with a requirement of strong privacy guarantee is needed.

REFERENCES

[1] B. Chazelle, "Filtering search: A new approach to query-answering," *SIAM J. Comput.*, vol. 15, no. 3, pp. 703–724, 1986.

[2] P. K. Agarwal and J. Erickson, "Geometric range searching and its relatives," *Discrete Comput. Geometry*, vol. 223, pp. 1–56, 1999.

[3] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location privacy via private proximity testing," in *Proc. NDSS*, 2011.

[4] H. Shirani-Mehr, F. Banaei-Kashani, and C. Shahabi, "Efficient reachability query evaluation in large spatiotemporal contact datasets," *Proc. VLDB Endowment*, vol. 5, no. 9, pp. 848–859, 2012.

[5] M. de Berg, O. Cheong, M. van Kreveld, and M. Overmars, *Computational Geometry: Algorithms and Applications*. Berlin, Germany: Springer-Verlag, 2008.

[6] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Proc. Theory Cryptogr. (TCC)*, 2007, pp. 535–554.

[7] E. Shi, J. Bethencourt, T.-H. H. Chan, D. Song, and A. Perrig, "Multidimensional range query over encrypted data," in *Proc. IEEE SP*, May 2007, pp. 350–364.

[8] Y. Lu, "Privacy-preserving logarithmic-time search on encrypted data in cloud," in *Proc. NDSS*, 2012, pp. 1–17.

[9] B. Wang, Y. Hou, M. Li, H. Wang, and H. Li, "Maple: Scalable multidimensional range search over encrypted cloud data with tree-based index," in *Proc. ACM ASIA CCS*, 2014, pp. 111–122.

[10] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in *Proc. ACM SIGMOD*, 2004, pp. 563–574.

[11] R. A. Popa, F. H. Li, and N. Zeldovich, "An ideal-security protocol for order-preserving encoding," in *Proc. IEEE SP*, May 2013, pp. 463–477.

[12] F. Kerschbaum and A. Schropfer, "Optimal average-complexity idealsecurity order-preserving encryption," in *Proc. ACM CCS*, 2014, pp. 275–286.

[13] B. Wang, Y. Hou, M. Li, H. Wang, H. Li, and F. Li, "Tree-based multidimensional range search on encrypted data with enhanced privacy," in *Proc. SECURECOMM*, 2014, pp. 1–25.

[14] E.-O. Blass, T. Mayberry, and G. Noubir, "Practical forward-secure range and sort queries with update-oblivious linked lists," in *Proc. PETS*, 2015, pp. 81–98.

[15] B. Wang, M. Li, H. Wang, and H. Li, "Circular range search on encrypted spatial data," in *Proc. IEEE ICDCS*, Jun./Jul. 2015, pp. 794–795.

[16] [Online]. Available: http://aws.amazon.com/solutions/case-studies/

[17] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE SP*, May 2000,pp. 44–55.

AUTHOR'S DETAILS:

BANDI HARISH, PG SCHOLAR, DEPARTMENT OF CNIS, VAAGDEVI COLLEGE OF ENGINEERING

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

A.RAMESH BABU, ASST.PROFESSOR,

DEPARTMENT OF CSE, VAAGDEVI

COLLEGE OF ENGINEERING