Impact Factor Value: 4.029 ISSN: 2349-7084
International Journal of Computer Engineering In Research Trends
Volume 4, Issue 7, July-2017, pp. 301-307 www.ijcert.org

Enabling Secure and Effective Spatial Query Processing on the Cloud using Forward Spatial Transformation

V. Swathi[1], D. Saidulu[2], B. Chandrakala[3]

[1,3]*Assistant Professor, Department of Computer Science and Engineering, Guru Nanak Institutions Technical Campus-Hyderabad, India.*
[2] *Associate Professor, Department of Computer Science and Engineering, Guru Nanak Institutions Technical Campus-Hyderabad, India.*
Email ID: swathivelugoti@gmail.com[1], fly2.sai@gmail.com[2], chandrakala.beerelly@gmail.com[3]

Abstract:- Data outsourcing is a common cloud computing model that allows data owners to takings advantage of its on-demand storage and computational resources. The main challenge is maintaining data confidentiality regarding intruders. Presented methodologies either conciliation the undisclosed of the data or undergo from high communication cost between the server and the user. To overcome this problem, we suggest a dual transformation and encryption scheme for spatial data, where encrypted queries are executed entirely by the service provider on the encrypted database, and encrypted results are returned to the user.The user issues encrypted spatial range queries to the service provider and then use the encryption key to decrypt the query response returned which establishments a balance between the security of data and efficient query response as the queries be processed on encrypted data at the cloud server finally our proposed method moderates the unique query communication cost between the authorized user and service provider.

Index Terms:- Data Encryption, Forward Spatial Transformation, Security, Query Processing, Database Outsourcing, Spatial Databases.

---

1. Introduction

The intensification of spatial data has managed organizations to upload their data onto third-party service providers. Cloud Computing permits data owners to outsource their databases, eliminating the requisite for expensive storage and computational resources [1]. For a trivial cost, organizations with limited resources can outsource their enormous sizes of data to a third-party service provider and utilize their dynamically-scalable storage as well as computational power. However, the fact remains that the data is controlled by an untrusted third-party and this raises critical security issues such as confidentiality and integrity. Data confidentiality requires that information is not revealed to untrusted users and data integrity assures that data is not altered before being processed by the server. In recent years, different domains such as the database and the cryptography community have discovered the problem of querying encrypted data at the untrusted service provider. This outsourcing of data brings down both investment cost and operational expenses for huge corporations. At the same time, outsourcing entails that customers lose primary control of their data and operations performed on the data. This in turn implies

that the data is susceptible to security concerns such as data confidentiality. Recently, mobile devices and navigational systems have become exceedingly common, and this has created the need for Location-Based Services (LBSs), which is a motivating application for database outsourcing.

This in turn has led to an increase in spatial data which has to be managed and maintained effectively. Spatial data in LBS includes the location information (i.e., latitude and longitude) besides other descriptive components which require huge storage capacity. Many users require LBSs on a daily basis and would like to issue spatial queries anonymously with a fast response. Also, the data owners do not want to reveal the data to the service provider to maintain the confidentiality of the data. With a cloud computing platform, it is possible to enhance query processing without burdening the user and manage the storage efficiently. Therefore, in this work, the aim is to effectively utilize the cloud environment to provide high throughput processing with low latency by performing queries at the service provider. Thus, one has to consider the following requirements when outsourcing spatial databases in the cloud environment.

1. The database content should be kept secreted from the service provider and malicious attackers. Naturally, there exists a native solution to protect the data owners: The data owner encrypts all spatial data and sends only encrypted data objects to the service provider without revealing the encryption key. However, the drawback of using off-the-shelf encryption is that the service provider cannot gain any underlying information from the encrypted data, nor can it perform any computations on cryptographic data. Thus, during the query phase, an authorized user retrieves all the encrypted data from the server, decrypts it using the key and searches for the required data objects. This would provide perfect security in a theoretical sense, but clearly, it cannot be used in real-time applications as the resulting communication cost will be extremely high. This is particularly the case for regular queries on huge datasets where only a small portion of the data is required to be returned.

Additional important issue to resolve is the development of efficient query processing techniques that can be executed on encrypted data at the service provider, such that user queries are handled entirely by the service provider without requiring multiple rounds of communication with the authenticated users. Several specialized encryption techniques have been proposed for this purpose. A relatively new encryption scheme is the Fully Homomorphic Encryption [2] technique suggested by Gentry et al., which enables direct computation on encrypted data which is stored in the service providers in the cloud. Different types of queries can be processed without decrypting the data.

In this paper, the cloud architecture model used comprises of three main entities, namely the Data Owner (DO), Service Provider (SP) and Authenticated User (AU). The DO guarantees security by transforming and encrypting the spatial database before outsourcing to the SP. To transform the 2D spatial data points, the DO employs the forward spatial transformation. The DO forms a list of packets defined by the forward spatial transformation. Next, this list is encrypted using the OPE (Order preserving Encryption) technique, which allows spatial range query to be performed at the SP without engaging the user and reducing any additional communication overhead. Additionally, the DO provides the forward spatial transformation key as well as the encryption key to the AUs. The keys are used by the AU to issue encoded range queries to the SP. The query is processed on the encrypted database at the SP, and the results are returned to the AU. Lastly, the AU decrypts the query response using the encryption key to obtain the actual result.

The main issue with OPE is that it cannot provide the ciphertext reveals ideal security desired by cloud consumers since the order of plaintext. Moreover, with the basic OPE scheme construction; client-side decryption time is much higher than traditional encryption techniques. Thus, in this work, we build on the dual encoding approach proposed in [4] to make it more secure by allowing search on encrypted data at the service provider without using OPE. The simple solution would be to store the encrypted spatial database using a vigorous and secure encryption method (such as Advanced Encryption Standard (AES) [4]) at the server-side as in [3]. No information can be deduced from this stored encrypted data, and

hence no query processing can take place on the server. The only way is to send the whole encrypted database to the user, where the user can decrypt and extract the required result.

In spatial database outsourcing applications, the attackers have to be prevented from gaining illegal access to the data. To analyze the security provided by the proposed schemes, it is assumed that the users are trusted by the data owners and, the transformation and encryption key is only provided to the authenticated users. However, the cloud service provider cannot be trusted with confidential data, as the SP is an untrusted third-party [5], [6], [7], [8] that provides services to multiple DOs and they could release sensitive information to competitors. Furthermore, malicious attackers are waiting around, waiting to eavesdrop and compromise the data confidentiality and query privacy required by the data owner using the cloud server. Outsourced data and user queries can be kept confidential by using cryptography to encrypt the data and prevent attackers and eavesdroppers from prying private information. Thus, in our approach, confidentiality is guaranteed by the dual encoding technique. We show that using both keys for spatial data provides security against known attacks defined in the literature.

In our approach, we attempt and achieve a balance between efficient query processing and obscuring data at the server. We achieve efficiency by performing query search at the service provider on the forward spatial transformation Packet List and thus, reduce the time taken to communicate the query response between the user and server, i.e., a single round of communication. Data is kept confidential at the server by encrypting the forward spatial transformation and the spatial data using the secure AES, and query processing at the SP is achieved by conducting equality comparisons on the encrypted data directly. One previously existing work by Yiu et al. [2] inherits the security of AES in a cryptographic-based transformation scheme (CRT). They cannot provide range query processing exclusively at the server. Thus, answering user queries requires multiple rounds of data communication between the server and the user. The R∗ - tree structure is used to index the database where each node is then encrypted using AES. The number of rounds is based on the depth of the tree. This protocol increases the communication cost entailed significantly and requires processing at the user end during query processing as well. Similarly, Kim et al. [3] designed a transformation scheme based on the forward spatial transformation (FST). The data is encrypted using the standard AES and stored at the server. The user then requests for required data, hence requiring multiple rounds of communication

A summary of our contributions is as follows:

- The aim is to have minimal processing done by the authorized user so that the user is not engaged. This paper extends the preliminary approach in [4] to provide better data confidentiality by using the conventional and secure AES instead of the OPE.
- Given encrypted queries, all of the range query processing can be performed at the service provider without any need to involve the user. The AU only has to decrypt the results encrypted using AES, which is fast.
- Moreover, the proposed cryptographic scheme requires only one round-trip between the user and server which is a significant improvement over the method in [2], [3]. As a result, the communication cost reduces drastically for larger query sizes.
- To balance the trade-off between confidentiality and efficiency, we have proposed three variations of the HPL approach.

2. Related Works

Cloud Computing profits to both the data owner and the user. Data owners can store enormous amounts of data on the cloud for a low cost. Users can enjoy on-demand provision of services, hence saving time. However, the cloud environment poses data security and privacy challenges. With the excessive use of mobile devices and navigational systems with GPS, location-based services have become widely popular in this domain. Database outsourcing has become common in recent times due to the large amount of spatial data available.

2.1 Anti-Tamper Hardware

In order to handle the security imperfections pretended by outsourcing databases, several prior works [9],[10] resolved the issue by adding a middleware or tamper-proof device at the SP to ensure security. This device assists in query processing by encrypting and decrypting the transmitted messages. Assuming a trusted device exists at the server, Damiani et al. [10] propose a fast searchable encryption technique for the non-order preserving AES [4] encryption. The database owners start by building a B-tree over 1-D values and encrypt each record at the node level to protect the data from the untrusted SP. However, with numerous users, it is not practical to have an individual device for every AU at the SP. To overcome this, other techniques have to be explored[14].

2.2 Symmetric Cryptography Schemes

Yiu et al. [2] present a cryptographic-based transformation scheme for two-dimensional data to enhance the security of spatial data. The DO uses the R+-tree structure to index the database and encrypts each node using the AES encryption. Query processing requires multiple rounds based on the depth of the R+ -tree between the user and server, thus increasing the communication cost. The SP sends the encrypted root node to the AU and the AU decrypts the node using the key. The AU then requests the child node overlapping with the query region till a leaf node with the data points is reached. However, both the HPL and CRT indexes are built for static data and cannot handle dynamic updates. Similarly, Kim et al. [3] developed a cryptographic scheme based on the forward spatial transformation (FST) to balance between data security and query efficiency. They use the forward spatial transformation to locally cluster the data by transforming two-dimensional data to a single dimension and thus hiding the coordinates of the original points. Then a straightforward approach is followed, and the conventional AES encryption is applied to the transformed data. The encrypted file is securely stored at the SP. For query processing, the entire encrypted file has to be sent to the AU, decrypted and then searched for the records relevant to the query. Since this requires multiple communication rounds, this proves to be highly time-consuming and data-intensive for usual range queries that require only a portion of the database as a result[15].

2.3 Preserving Location Data Privacy

In addition to the cryptographic techniques mentioned above, Yiu et al. [2] also present three different spatial transformation methods that are based on partitioning and redistributing the locations in the space. Namely: 1) Hierarchical Space Division (HSD), 2) Error-Based Transformation (ERB) and 3) a hybrid of HSD and ERB. However, these techniques preserve the coordinates of the original points and assuming that an attacker can gain background knowledge of the original points and coordinates of these points in the transformed space, information about close by data points can be exposed.

2.4 Privacy and Integrity Guarantee.

On the other hand, Ku et al. [11] proposed a technique for outsourcing databases while assuring both data confidentiality and query integrity. To preserve data privacy, the data points are encrypted with a symmetric key and indexed by the Hilbert value. Whereas, to ensure query integrity, a probabilistically replication method is applied to a portion of the data which is encrypted with a different space key. Then the two encrypted data sets are combined and stored at SP allowing the client to examine the reliability of the query results. Based on the current research in the field [7], the Hilbert-curve does not take the distribution of spatial points into consideration when transforming the original space. In fact, it divides the space using the same granularity and generates Hilbert values to construct the Hilbert index.

2.5 Partitioned Indexing Methods

To balance the trade-off between security and efficiency in outsourced data, Wang et al. [3] propose a scheme based on the R- ˆ tree. The R-tree follows a hierarchical encrypted index mechanism ˆ where an asymmetric scalar-product preserving encryption is used. Moreover, the method uses the leaf Minimum Bounding Rectangle (MBR) to hide ordering and hence, protects the data from being disclosed. However, the authors do not provide any substantial

definition of security guaranteed by the scheme. Khoshgozaran et al. [12] propose a system to maintain an encrypted index on the server and efficiently update it. The system supports encrypted spatial queries. Hence it is used to offer proximity based services. However, the system requires users to be organized in groups, with each cluster sharing a secret key, and all the users in a group must trust each other. Moreover, the queries are processed at the user-side, and thus, the AUs require secure communication with the untrusted SP

3. Problem Statements

In this section, we briefly assessment the cloud computing model applicable to our solution and provide a formal introduction to the proposed spatial database outsourcing approach.

3.1 System Architecture

Cloud computing offers on-demand delivery of various computing resources by outsourcing data to untrusted cloud servers and allowing access only to authorized users. The data owners have to be aware of security concerns while achieving higher scalability and lower cost by outsourcing databases to the cloud. The cloud architecture model (cf. Figure 1) comprises of 3 main entities, namely the Data Owner, Service Provider and Authenticated User. The data owners have the two-dimensional spatial data points that have to be outsourced to a server that cannot be trusted. They deploy the required cloud service and guarantee security by transforming and encrypting the database before outsourcing to the service provider. Moreover, the authenticated users are provided with the transformation key as well as the decryption key. The AU utilizes the conversion key to issue encrypted range queries to the SP. The query is processed on the encrypted database at the SP, and the results are returned to the user. The AU decrypts the query response using the key to obtain the actual data points.

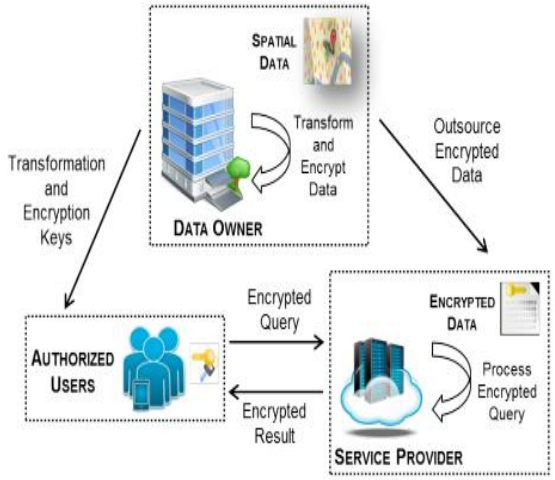

Figure 1: Spatial Architecture for Spatial outsourced cloud data

4. Adversary Model

The key requirements of a secure database outsourcing scheme demand that: 1) data confidentiality is maintained on the cloud server and, 2) queries are efficiently processed by the SP and results are returned to the user without any alteration. As mentioned previously, the AUs are trusted by the DO and hence have been provided with both the HSK and encryption keys. Thus, we focus on the curious intruder model [13], also known as the passive adversary model for the SP. Since our approach provides a dual layer of security, we analyze the security of the forward spatial transformation based on the brute-force attack and the location approximation attack. Lastly, the popular known-plaintext attack along with a statistical attack based on order is presented for order-preserving encryption.

4.1 Brute-Force Attack

If an attacker is aware of the space-transformation technique used (i.e., Hilbert curve in our method), as well as a subset of the original spatial data points along with their transformed forward spatial transformation cell values, the attacker can determine the key of the transformation technique. The study by [6] suggests that it is infeasible for a malicious adversary to infer the exact transformation key being used.

4.2 Location Approximation Attack

The spatial data points are stored along with their indices in the forward spatial transformation. Each packet in the forward spatial transformation

4.3 Known-Plaintext Attack

The attacker is required to obtain the plaintexts for the encrypted data. Order-preserving encryption schemes are deterministic such that they ensure that the numerical ordering of plaintext data is preserved in the ciphertext domain

5. Spatial Range Query

The proposed forward spatial transformation approach deals with two-dimensional spatial range queries due to their popularity. When a query request is initiated by the AU, the range query is converted to a set of 1-D Hilbert cell values and this includes cells that partially or wholly overlap with the query region. Since some of these cells only partially overlap with the query, the set of indices might retrieve irrelevant data points (i.e., false positives) in the query response. The SP is responsible for processing the query request. Figure 4 shows the range query process on the example given in Figure 3. Given the coordinates of opposite corner points of a range query, the AU converts the query into a set of Hilbert cell values that belong to the region. The mapping of a query is made possible using the HSK provided by the DO, without any knowledge of the original space distribution. Next, the AU encrypts the query request using the OPE key and then sends it to the SP

6. Conclusions

Database outsourcing is a popular paradigm of cloud computing. In this work, we are trying to achieve a balance between data confidentiality at the server and efficient query processing. We propose to transform the spatial database by applying the forward spatial transformation. Next, we make it more secure by applying encryption to the transformed data. We define several attack models and show that our scheme provides strong security against them. This allows a balance between the safety of data and fast response time as the queries are processed on encrypted data at the cloud server. Thus, the dual transformation method not only protects the data but also enables the authenticated users to retrieve spatial range query responses efficiently.

References.

[1] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Communications Surveys & Tutorials,, vol. 15, no. 2, pp. 843–859, 2013.

[2] M. L. Yiu, G. Ghinita, C. S. Jensen, and P. Kalnis, "Enabling search services on outsourced private spatial data," The VLDB Journal, vol. 19, no. 3, pp. 363–384, 2010.

[3] P. Wang and C. V. Ravishankar, "Secure and efficient range queries on outsourced databases using r-trees," in 2013 IEEE 29th International Conference on Data Engineering (ICDE). IEEE, 2013, pp. 314–325.

[4] A. M. Talha, I. Kamel, and Z. A. Aghbari, "Enhancing confidentiality and privacy of outsourced spatial data," in 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud). IEEE, 2015, pp. 13–18.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE Infocom, 2010 proceedings. IEEE, 2010, pp. 1–9.

[6] H. Xu, S. Guo, and K. Chen, "Building confidential and efficient query services in the cloud with rasp data perturbation," IEEE transactions on knowledge and data engineering, vol. 26, no. 2, pp. 322–335, 2014.

[7] H. Hu, J. Xu, C. Ren, and B. Choi, "Processing private queries over untrusted data cloud through privacy homomorphism," in IEEE 27th International Conference on Data Engineering. IEEE, 2011, pp. 601– 612.

[8] G. Zhao, C. Rong, J. Li, F. Zhang, and Y. Tang, "Trusted data sharing over untrusted cloud storage providers," in IEEE Second International Conference

on Cloud Computing Technology and Science (CloudCom). IEEE, 2010, pp. 97–103.

[9] H. Hacigum¨ us, B. Iyer, and S. Mehrotra, "Providing database as a ¨ service," in 18th International Conference on Data Engineering, 2002. Proceedings. IEEE, 2002, pp. 29–38. [10] E. Damiani, S. Vimercati, S. Jajodia, S. Paraboschi, and P. Samarati, "Balancing confidentiality and efficiency in untrusted relational dbmss," in Proceedings of the 10th ACM conference on Computer and Communications Security. ACM, 2003, pp. 93–102.

[11] W.-S. Ku, L. Hu, C. Shahabi, and H. Wang, "Query integrity assurance of location-based services accessing outsourced spatial databases," in Advances in Spatial and Temporal Databases. Springer, 2009, pp. 80– 97.

[12] A. Khoshgozaran and C. Shahabi, "Private buddy search: Enabling private spatial queries in social networks," in International Conference on Computational Science and Engineering, 2009 (CSE'09)., vol. 4. IEEE, 2009, pp. 166–173.

[13] Anil Kumar Uppula , Srinivasulu Tadisetty ," Achieving better Authentication and Copyright protection Using DWT and SVD Based Watermarking Scheme,"International Journal of Computer Engineering In Research Trends.,vol.3,no.9,pp.487-491,September 2016.

[14] Venkata Srinivasu Veesam, Bandaru Satish Babu," Evaluation of Captcha Technologies towards Graphical Password Scheme," International Journal of Computer Engineering In Research Trends.,vol.2,no.1,pp.98-106,February 2015.

[15] D.J. Ashpin Pabi, N.Puviarasan, P.Aruna," Fast Singular value decomposition based image compression using butterfly particle swarm optimization technique (SVD-BPSO)," International Journal of Computer Engineering In Research Trends.,vol.4,no.4,pp.128-135,April 2017.

