IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 5, May 2019
ISSN (Online) 2348 – 7968
www.ijiset.com

Enabling Search Operations on Private Spatial Data Using Blowfish Algorithm

A. Merlin monisha
M.E Scholar Adhiyamaan College of Engineering Hosur-635109
Dr M.Lilly Florence, Prof / CSE
Professor Adhiyamaan College of Engineering Hosur-635109

Abstract-.Cloud computing consists of three distinct types of computing services delivered remotely to clients via the internet. Cloud allows data owners to take advantage of its on-demand storage and computational resources. The main challenge is maintaining data confidentiality regarding intruders. Blow fish algorithm is used to encrypt and decrypt, where encrypted queries are executed entirely by the service provider and encrypted results are returned to the user. Blowfish algorithm is applied for encryption of files to be outsourced. The user issues spatial related queries to the service provider, using the decrypt key the user can get the response. Finally our proposed method moderates the unique query communication between the authorized user and service provider. Encrypt the data using blowfish. Indexing and ranking algorithm to process KNN queries.

Index terms: Spatial Databases, Data Encryption, Security, Query Processing, Database Outsourcing.

I INTRODUCTION

The expansion of spatial information has driven associations to transfer their information onto outsider specialist organizations. Distributed computing enables information proprietors to outsource their databases, disposing of the requirement for exorbitant capacity and computational assets.

The admin was created to detail the working of a hospital record keeping system in respect to patient information from this project.

Then patient has to share their location, so that the patient nearby places are displaying. Now patient can give request to the admin. The admin has to receive the request from patient and he has to

As of late, unique areas, for example, the database and the cryptography network have investigated the issue of questioning scrambled information at the

For a little cost, associations with constrained assets can outsource their extensive volumes of information to an outsider specialist co-op and use their powerfully adaptable capacity and computational power. In any case, the reality remains that the information is controlled by an untrusted outsider and this raises basic security issues, for example, secrecy and honesty. Information privacy that untrusted specialist organization. This outsourcing of information cuts down both venture cost and operational costs for colossal partnerships. In the meantime, outsourcing involves that clients lose essential control of their information and tasks performed on the information. This thusly infers the information is helpless to security concerns, for example, information privacy.

To users and organizations with different cloud model like public cloud, private cloud and hybrid cloud. Introducing public cloud which provides data storage and query services available for more users along with low cost. Data outsourcing is a common cloud computing model provides the blowfish key for each patient. After receiving the blowfish key from admin the patient can decrypt the records and receiving the original records of patient necessitates that information isn't revealed to untrusted clients and information trustworthiness guarantees that information isn't adjusted before being prepared by the server.

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. Numerous users require LBSs on a daily basis and would like to issue spatial queries in an anonymous manner with a fast response. Also, the data owners do not want to reveal the data to the service provider in order 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.

Most existing approaches protect the outsourced data using spatial transformation schemes or conventional cryptographic techniques. However, to the best of our knowledge, with most schemes there is a trade-off between data confidentiality and efficient query processing. To overcome these limitations, we propose a two-layer encoding approach, in which the spatial data points are transformed and then an encryption technique is applied to the transformed spatial space. Encryption allows data to be securely outsourced to the untrusted service provider, while the transformation adds another layer of security to the approach by hiding the original location of the points.

In this paper, the cloud architecture model used comprises of 3 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 Hilbert space-filling curve. The DO forms a list of packets defined by the Hilbert ordering. Next, this list is encrypted using the OPE technique, which allows spatial range queries to be performed at the SP without engaging the user and reducing any additional communication overhead.

Additionally, the DO provides the Hilbert 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 ideal security desired by cloud consumers since the order of plaintext is revealed by the ciphertext. 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 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 strong and secure encryption method blowfish at the server-side . No information can be deduced from this stored encrypted data and hence no query processing can take place at 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 that provides services to multiple DOs and they could release sensitive information to competitors. Furthermore, there are malicious attackers lurking 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.

A scenario of such an exchange in a LBS application is where a data owner outsources its data to a service provider like Google. In the process, the data owner does not want to expose the sensitive information to the server. The authenticated users send queries to the service provider for information but do not want to reveal their location to the server, which is capable of handling tens of millions of user query requests.

In our approach, we try 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 Hilbert 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. Efficient query processing is a key requirement of LBSs for the user and therefore database outsourcing techniques have to achieve a low communication cost. This requires schemes that encode the spatial data and queries, and then processes spatial queries over the transformed data at the service provider. Most of the existing techniques do not utilize the computational power of the SP and thus, we plan to overcome this shortcoming by performing efficient range queries on the encrypted data at the SP. We conduct an extensive experimental analysis to show the effectiveness of our technique and comparison is done with two existing approaches on different criteria. Furthermore, since LBSs have to handle a huge amount of spatial data, we have demonstrated the capability of our approach in the Experimental Evaluation with two large static spatial datasets (from Open Street Map).

II. RELATED WORK

Cloud computing provides benefits to both the data owner and the user. Data owners can store huge 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. Hacigumus et al. were the first to propose the notion of outsourcing databases to a third-party service provider.

Symmetric Cryptography Schemes

Yiu et al 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 blowfish 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, CRT indexes are built for static data and cannot handle dynamic updates.

Similarly, Kim et al. developed a cryptographic scheme based on the Hilbert-curve transformation (HCT) to balance between data security and query efficiency. They use the Hilbert curve 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 blowfish 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 the result.

Preserving Location Data Privacy

In addition to the cryptographic techniques mentioned above, Yiu et al. 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. Another spatial transformation scheme is proposed by Hossain et al.. Their scheme offers data security by applying a shear transformation as well as the rotation transformation but is not secure against the proximity attack.

Data transformation methods provide a stronger notion of privacy despite being slightly more computationally intensive due to the encoding and decoding operations. In another solution, the data owner encodes the database prior to transmitting it to the service provider. An authorized user that possesses the secret keys, issues an encoded query to the SP. Both the database and the queries are not accessible by the SP and thus, privacy is assured. The main idea is to provide the SP with searching capabilities over the encoded data. Khoshgozaran et al. transform the points using the Hilbert mapping using parameters such as curve order, scale, orientation, etc. as the secret key. Their technique allows approximate search directly on the transformed points.

Privacy and Integrity Guarantee

On the other hand, Ku et al. proposed a technique for outsourcing databases while assuring both data privacy 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 datasets are combined and stored at SP allowing the client to examine the reliability of the query results.

III. PROPOSED SYSTEM

Cloud computing services empower 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. Only authorized users are allowed to access the data. Nobody else, including the service provider, should be able to view the data. For instance, a real-estate company that owns a large database of properties wants to allow its paying customers to query for houses according to location. On the other hand, the untrusted service provider should not be able to learn the property locations and, e.g., selling the information to a competitor.

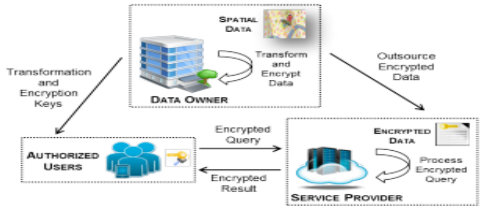
To tackle the problem, we propose to transform the location datasets before uploading them to the service provider. The application develops a spatial transformation that re-distributes the locations in space, and a cryptographic-based transformation. The data owner selects the transformation key and shares it with authorized users. Without the key, it is infeasible to reconstruct the original data points from the transformed points. The proposed transformations present distinct trade-offs between query efficiency and data confidentiality. In addition, we describe attack models for studying the security properties of the transformations. Empirical studies demonstrate that the proposed methods are efficient and applicable in practice.

Methodology

Java:

Java is a general-purpose computer-programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible.

Architectural Design



Algorithm Implement

To overcome these shortcomings of the preliminary approach, we propose to use the secure blowfish scheme. none of the well-known cryptanalysis attacks have been proven to break blowfish yet. since blowfish only allows equality comparisons on encrypted data, we enumerate the hilbert cells between fps, peg and store them in each packet. lastly, this data is encrypted using blowfish and sent to the sp. the au issues an encrypted spatial range query to the server and all query processing is done at the SP, as it should be done in a true database outsourcing application. The index search at the SP does induce a high query overhead, almost linear with respect to size(D), but with the computing power of the SP, this is not a real concern. Moreover, the order of plaintext in the encrypted packets is obscured, and this makes the new approach attractive and secure. Lastly, the AU decrypts the query results using the blowfish key with almost no overhead. In this work, we show three different variations of the highlight their advantages over one another.

The end user can give the feedback to the each and every hospital.

BLOWFISH ALGORITHM:

Blowfish is a symmetric-key block cipher. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits.[3] It is a 16-round Feistel cipher and uses large key-dependent S-boxes. The lookup results are then added and XOR ed together to produce the output. Because Blowfish is a symmetric algorithm, the same procedure is used for decryption as well as encryption. The only difference is that the input to the encryption is plaintext; for decryption, the input is cipher text.

SPACE TRANSFORMATION AND ENCRYPTION:

To preserve the privacy of spatial data, we propose to hide the original spatial data points in two-ways. First, we transform the space by converting the 2D points to 1D using the Hilbert Space Key. Next, we encode the resulting Hilbert indices and data points using an encryption scheme. Both the transformation key and the encryption key are

transmitted by the DO to the trusted AUs over a secure communication channel using SSL without the need for any costly tamper-resistant devices.

PROJECT IMPLEMENTATIONS

Modules:

Anti-Tamper Hardware

With a specific end goal to handle the security flaws posed by outsourcing databases, several prior works 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. propose a fast searchable encryption technique for the non-order preserving blowfish 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.

PRESERVING LOCATION DATA PRIVACY:

The cryptographic techniques mean, the 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. Another spatial transformation scheme. Their scheme offers data security by applying a shear transformation as well as the rotation transformation, but is not secure against the proximity attack.

PRIVACY AND INTEGRITY GUARANTEE

A technique for outsourcing databases while assuring both data privacy 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 datasets are combined and stored at SP allowing the client to examine the reliability of the query results.

PARTITIONED INDEXING METHODS:

The trade-off between security and efficiency in outsourced data, propose a scheme based on the Rˆ -tree. The Rˆ -tree follows a hierarchical encrypted index mechanism 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.

IV. RESULT ANALYSIS

DISTRIBUTION OF ENCRYPTED VALUES:

Geospatial analysis is the gathering, display, and manipulation of imagery, GPS, satellite photography and historical data, described explicitly in terms of geographic coordinates or implicitly, in terms of a street address, postal code, or forest stand identifier as they are applied to geographic models. Geospatial analysis originated in Canada for cataloguing natural resources in the 1960s, using the first geographic information systems (GIS). Geographic information systems are used to predict, manage and learn about all kinds of phenomena affecting the earth, its systems and inhabitants.

USER INTERFACE DESIGN:

1. Admin
    a. Maintain Hospitals
2. Hospital
    a. Manage Doctors, Patients, Patients Reports,etc
    b. Upload reports to the cloud, give the permission to access
3. Patients:
    a. Patients can view their reports
    b. Patients can view their report with decryption.

KEY SIZE:

The size of the encryption key K depends on the number of buckets needed for partitioning a distribution, the total size being roughly three times the number of buckets. We found that we did not need more than 200 buckets for any of our datasets (including those with 10 million values); for Uniform, the number of buckets needed was less than 10. Thus, the encryption key can be just a few KB in size.

V. CONCLUSION

Database outsourcing is a popular model 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 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 security of data and fast response time as the queries are processed on encrypted data at the cloud server. Moreover, we compare with existing approaches on large datasets and show that this approach reduces the average query communication cost between the authorized user and service. Patient records are stored in cloud storage and those records are encrypted using Blowfish algorithm which will give security of patient records (reports).Patients lost their records in somewhere and they need those records to contact the doctor, in such a case patient can able to give request to the administrator. So the admin person can share the reports in encrypted format also he is providing the blowfish algorithm. so patient can decrypt the records using the blowfish key.

VI. 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] C. Gentry et al., “Fully homomorphic encryption using ideal lattices.” In STOC, vol. 9, 2009, pp. 169–178.

[3] B. Hore, S. Mehrotra, M. Canim, and M. Kantarcioglu, “Secure multidimensional range queries over outsourced data,” The VLDB Journal The International Journal on Very Large Data Bases, vol. 21, no. 3, pp. 333– 358, 2012.

[4] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Order preserving encryption for numeric data,” in Proceedings of the 2004 ACM SIGMOD international conference on Management of data. ACM, 2004, pp. 563–574.

[5] J. K. Lawder and P. J. H. King, “Querying multi-dimensional data indexed using the hilbert space-filling curve,” ACM Sigmod Record, vol. 30, no. 1, pp. 19–24, 2001.

[6] A. Khoshgozaran and C. Shahabi, “Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy,” in Advances in Spatial and Temporal Databases. Springer, 2007, pp. 239– 257.

[7] W.-S. Ku, L. Hu, C. Shahabi, and H. Wang, “A query integrity assurance scheme for accessing outsourced spatial databases,” Geoinformatica, vol. 17, no. 1,h pp. 97–124, 2013.

[8] F. Tian, X. Gui, P. Yang, X. Zhang, and J. Yang, “Security analysis for hilbert curve based spatial data privacy-preserving method,” in 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing. IEEE, 2013, pp. 929–934.

[9] 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.

[10] H.-I. Kim, S.-T. Hong, and J.-W. Chang, “Hilbert curve based cryptographic transformation scheme for protecting data privacy on outsourced private spatial data,” in 2014 International Conference on Big Data and Smart Computing (BIGCOMP). IEEE, 2014, pp. 77–82.

[11] 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.