Facilitating Secure and Efficient Spatial Query Processing on the Cloud

B.Narendra[1], Dr M.Sreedevi[2]
[1]*Dept of Computer Science, Sri Venkateswara University*
[2]*Assistant Professor, Dept. of Computer Science, Sri Venkateswara University*

***Abstract*- Database outsourcing is a common cloud computing paradigm that allows data owners to take advantage of its on-demand storage and computational resources. The main challenge is maintaining data confidentiality with respect to untrusted parties i.e., cloud service provider, as well as providing relevant query results in real-time to authenticated users. Existing approaches either compromise confidentiality of the data or suffer from high communication cost between the server and the user. To overcome this problem, we propose a dual transformation and encryption scheme for spatial data, where encrypted queries are executed entirely at 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 uses the encryption key to decrypt the query response returned. This allows a balance between the security of data and efficient query response 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 provider, as only a single round of communication is required by the proposed approach.**

INTRODUCTION

The increase of spatial data has led organizations to upload their data onto third-party service providers. Cloud computing allows data owners to outsource their databases, eliminating the need for costly storage and computational resources [1]. For a small cost, organizations with limited resources can outsource their large volumes 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 data is not disclosed 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 explored 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 toan increase in spatial data which has to be managed and maintained effectively. Spatial data in a 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 issues patial 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. Thus, one has to consider the following requirements when outsourcing spatial databases in the cloud environment. First, the database content should be kept hidden from the service provider and malicious attackers. Naturally, there exists a na¨ıve 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

EXISTING SYSTEM

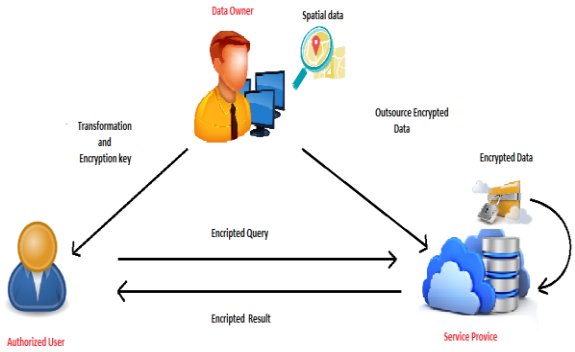
Secure cloud computing is key for business success and end-user adoption of federated and decentralized cloud services and thus essential to stimulate the growth of the European Digital Single Market. RestAssured will provide solutions to specific technical concerns of data protection in the cloud (such as geo-location restrictions on personal data), which are imposed by the dynamic, multi-stakeholder and decentralized nature of federated cloud systems. These concerns mean that privacy and security by design approaches will no longer be sufficient, due to uncertainty at design time of how the cloud and privacy requirements may dynamically evolve and change at run time. To this end, RestAssured provides novel mechanisms and cloud architectures for the runtime detection, prediction and prevention of data protection violations.Rest Assured will assure the protection of sensitive business and citizen data in the cloud by combining four pillars of innovation: (1) combination of fully homomorphic encryption to process data without decryption with cloud enablement of SGX hardware for protected data processing, (2) sticky policies for decentralized data lifecy-cle management, (3) models@runtime for data protection assurance, and (4) automated risk management for run-time data protection. The applicability and usefulness of the RestAssured solutions will be demonstrated through three use cases driven by project partners and involving other stakeholders from outside the consortium; High Performance Computing for commercial enterprises; Pay As You Drive usage based insurance.

PROPOSED SYSTEM

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.

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. 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. 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. Cloud computing offers on-demand delivery of various computing resources by outsourcing data to untrusted cloud servers and allowing access only to authorized users.

ARCHITECTURE DIAGRAM



Modules:
1.Data Owner.
2.Authorized user.
3.ServiceProvider.

DATA OWNER

Database outsourcing is a common cloud computing paradigm that allows data owners to take advantage of its on-demand storage and computational resources.
Cloud computing allows data owners to outsource their databases, eliminating the need for costly storage and computational resources. , the data owners do not want to reveal the data to the service provider in order to maintain the confidentiality of the data.
The data owner encrypts all spatial data and sends only encrypted data objects to the service provider without revealing the encryption key. 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. 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.

AUTHORIZED USER

The 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.

The aim is to have minimal processing done by the authorized user so that the user is not engaged This project extends the preliminary approach in to provide better data confidentiality by using the conventional and secure AES instead of the OPE. An authorized user that possesses the secret keys, issues an encoded query to the Service provider.

SERVICE PROVIDER

cloud service provider providing relevant query results in real-time to authenticated users. Also The small cost, organizations with limited resources can outsource their large volumes of data to a third-party service provider and utilize their dynamically-scalable storage as well as computational power.
This permits range queries on the encrypted data directly at the untrusted service provider without having to decrypt confidential data. 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.
we build on the dual encoding approach proposed in to make it more secure by allowing search on encrypted data . 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.
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.

Algorithm 1: Hilbert Packet List Construction
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, called the Hilbert Packet List (HPL), in which the spatial data points are transformed and then an encryption technique is applied to the transformed spatial space.

Algorithm 1: Spatial Range Query

A spatial query is a special type of database query supported by geodatabases and spatial databases. The queries differ from non-spatial SQL queries in several important ways. Two of the most important are that they allow for the use of geometry data types such as points, lines and polygons and that these queries consider the spatial relationship between these geometries.

CONCLUSION

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 Hilbertcurve. 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 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 provider, as only a single round of communication is required by the proposed approach. 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] 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. Srikanth, 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 spacez 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 © October 2017| IJIRT | Volume 4 Issue 5 | ISSN: 2349-6002 outsourced spatial databases," Geoinformatica, vol. 17, no. 1, 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.

[12] 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.

[13] N. F. Pub, "197: Advanced encryption standard," Federal Information Processing Standards Publication, vol. 197, pp. 441–0311, 2001.

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

[15] 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.

[16] 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 .

[17] 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 (Cloud Com). IEEE, 2010, pp. 97–103.

[18] "Open street map," http://www.openstreetmap.org/.

[19] H. Hacig¨um¨us, B. Iyer, and S. Mehrotra, "Providing database as a service," in 18thInternational Conference on Data Engineering, 2002 .Proceedings .IEEE, 2002, pp. 29–38.

[20] 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.

[21] A.A.Hossain, S.-J. Lee, and E.-N. Huh, "Shear-based spatial transformation to protect proximity attack in outsourced database," in 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (Trust Com).IEEE, 2013, pp.1633– 1638.

[22] 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.

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

[24] A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill, "Order-preserving symmetric encryption," in Advances in Cryptology-EUROCRYPT 2009. Springer, 2009, pp. 224–241.

[25] A. Boldyreva, N. Chenette, and A. ONeill, "Order-preserving encryption revisited: Improved security analysis and alternative solutions," in Advances in Cryptology–CRYPTO 2011. Springer, 2011, pp. 578–595.