Data and User Confidentiality Privacy Preservation in Distributed Servers

[1]Dr.D.Suresh, [2]Dr.N..Dhanalakshmi, [3]Dr.A.Thomas Paul Roy

Abstract**—***Advances in sensing and tracking technology enable location-based applications but they also create significant privacy risks. Anonymity can provide a high degree of privacy, save service users from dealing with service providers' privacy policies, and reduce the service providers' requirements for safeguarding private information. However, guaranteeing anonymous usage of location-based services requires that the precise location information transmitted by a user cannot be easily used to re-identify the subject. This paper presents a middleware architecture and algorithms that can be used by a centralized location broker service. The adaptive algorithms adjust the resolution of location information along spatial or temporal dimensions to meet specified anonymity constraints based on the entities who may be using location services within a given area. Using a model based on automotive traffic counts and cartographic material, we estimate the realistically expected spatial resolution for different anonymity constraints. The median resolution generated by our algorithms is 125 meters. Thus, anonymous location-based requests for urban areas would have the same accuracy currently needed for E-911 services; this would provide sufficient resolution for wayfinding, automated bus routing services and similar location-dependent services.*

Keywords —

I. INTRODUCTION

As an emerging computing paradigm, cloud computing attracts increasing attention from both research and industry communities. Outsourcing data and computation to cloud server provides a cost effective way to support large scale data storage and query processing. However, due to security and privacy concerns, sensitive data need to be protected from the cloud server as well as other unauthorized users. A common approach to protect the confidentiality of outsourced data is to encrypt the data.

[1]*Professor, Department of CSE., PSNA College of Engineering and Technology, sureshdgll@gmail.com*
[2]*Professor, Department of CSE., PSNA College of Engineering and Technology, ndmugi@gmail.com*
[3]*Professor, Department of CSE., PSNA College of Engineering and Technology, pauli.dgl@gmail.com*

To protect the confidentiality of the query from cloud server, authorized clients also send encrypted queries to the cloud server. It illustrates our problem scenario of secure query processing over encrypted data in the cloud. The data owner outsources encrypted data to the cloud server. The cloud server processes encrypted queries from the client on the encrypted data and returns the query result to the client. During the query processing, the cloud server should not gain any knowledge about the data, data patterns, query, and query result. Fully homomorphic encryption schemes ensure strong security while enabling arbitrary computations on the encrypted data. However, the computation cost is prohibitive in practice. Trusted hardware such as Intel's Software Guard Extensions (SGX) brings a promising alternative, but still has limitations in its security guarantees. Many techniques have been proposed to support specific queries or computations on encrypted data with varying degrees of security guarantee and efficiency (e.g., by weaker encryptions). Focusing on similarity search, secure k-nearest neighbor (KNN) queries, which return k most similar (closest) records given a query record, have been extensively studied.

II.LITERATURESURVEY

[1]Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking

Authors:B. Rogers, S.Chhabra,Y.Solihin,and M. Prvulovic

Advances in sensing and tracking technology enable location-based applications but they also create significant privacy risks. *Anonymity* can provide a high degree of privacy, save service users from dealing with service providers' privacy policies, and reduce the service providers' requirements for safeguarding private information. However, guaranteeing anonymous usage of location-based services requires that the precise location information transmitted by a user cannot be easily used to re-identify the subject. This paper presents a middleware architecture and algorithms that can be used by a centralized location broker service. The adaptive algorithms adjust the resolution of location information along spatial or temporal dimensions to meet specified anonymity constraints based on the entities who *may* be using location services within a given area. Using a model based on automotive traffic counts and cartographic material, we estimate the realistically expected spatial resolution for different anonymity constraints. The median resolution generated by our algorithms is 125 meters. Thus, anonymous location-based requests for urban areas would have the same accuracy currently needed for E-911 services; this would provide sufficient resolution for wayfinding, automated bus routing services and similar location-dependent services.

[2]2Dummy Based Privacy Preservation in Continuous Querying Road Network Services.

Authors:Fincy Francis1, Aparna M.S, Anitta Vincent

Dummies are useful for improving success rate because they can be always available, however, using dummies have two main challenges. The first is how to generate a dummy that is indistinguishable from a real user especially on road networks which have varied movement trends. Secondly, dummies can be used to launch attacks on the location based server by malicious clients which affects the business of the service providers. In this paper, we propose a novel client orientated privacy preserving scheme for continuously querying road network service that is also capable of protecting location based servers from attacks. We employed an offline trajectory clustering algorithm that clustered users' trajectory and used the derived parameters to generate a cost effective reusable realistic dummies on road network. To overcome malicious clients using dummies to launch attacks on location based servers, we developed a privacy preserving verification protocol capable of checking the activities of all clients in privacy preserving manner to curb such attacks. We tested the efficiency of our algorithm with some defined evaluation metrics, and it provided an effective privacy protection, satisfied clients at all times within an excellent processing time at a reasonable dummy processing cost when continuously querying road network services.

[3]Location Privacy via Differential Private Perturbation of Cloaking Area

Authors:C. Gentry, S. Halevi, and N. P. Smart

The increasing use of mobile devices has triggered the development of location based services (LBS). By providing location information to LBS, mobile users can enjoy variety of useful applications utilizing location information, but might suffer the troubles of private information leakage. Location information of mobile users needs to be kept secret while maintaining utility to achieve desirable service quality. Existing location privacy enhancing techniques based on K-anonymity and Hilbertcurve cloaking area generation showed advantages in privacy protection and service quality but disadvantages due to the generation of large cloaking areas that makes query processing and communication less effective. In this paper we propose a novel location privacy preserving scheme that leverages some differential privacy based notions and mechanisms to publish the optimal size cloaking areas from multiple rotated and shifted versions of Hilbert curve. With experimental results, we show that our scheme significantly reduces the average size of cloaking areas compared to previous Hilbert curve method. We also show how to quantify adversary's ability to perform an inference attack on user location data and how to limit adversary's success rate under a designed threshold.

[4]Achieving k-anonymity in Privacy-Aware Location-Based Services

Authors : E. Aktas, F. Afram, and K. Ghose

Location-Based Service (LBS) has become a vital part of our daily life. While enjoying the convenience provided by LBS, users may lose privacy since the untrusted LBS server has all the information about users in LBS and it may track them in various ways or release their personal data to third parties. To address the privacy issue, we propose a Dummy- Location Selection (*DLS*) algorithm to achieve k-anonymity for users in LBS. Different from existing approaches, the *DLS* algorithm carefully selects dummy locations considering that side information may be exploited by adversaries. We first choose these dummy locations based on the entropy metric, and then propose an *enhanced-DLS* algorithm, to make sure that the selected dummy locations are spread as far as possible. Evaluation results show that the proposed *DLS* algorithm can significantly improve the privacy level in terms of entropy. The *enhanced-DLS* algorithm can enlarge the cloaking region while keeping similar privacy level as the *DLS* algorithm.

III.PROPOSED SYSTEM

A Skyline

A **skyline query** returns the objects that cannot be dominated by any other objects. In the case of a dataset consisting of multidimensional objects, an object dominates another object if it is as good in all dimensions, and better in at least one dimension.

Skyline queries received great attention in the database community during the past decades. The skyline computation became crucial to many multi-criteria decision making applications. A significant number of algorithms were proposed and studied extensively.

B Stegnography Data

Steganography is the art of hiding data in a seemingly innocuous cover medium. For example – any sensitive data can be hidden inside a digital image. Steganography provides better security than cryptography because cryptography hides the contents of the message but not the existence of the message.

Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. In this paper we will discuss how digital images can be used as a carrier to hide messages. This paper also analyses the performance of some of the steganography tools. Steganography is a useful tool that allows covert transmission of information over an over the communications channel. Combining secret image with the carrier image gives the hidden image. The hidden image is difficult to detect without retrieval. This paper will take an in-depth look at this technology by introducing the reader to various concepts of Steganography, a brief history of Steganography and a look at some of the Steganography technique

C Blockchain Privacy

A **blockchain**, originally **block chain**, is a growing list of records, called *blocks*, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree).

By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, block chains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.

D SecureMulti-party Computation (SMC)

Secure multi-party computation (also known as secure computation, multi-party computation (MPC), or privacy-preserving computation) is a subfield of cryptography with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private. Unlike traditional cryptographic tasks, where cryptography assures security and integrity of communication or storage and the adversary is outside the system of participants (an eavesdropper on the sender and receiver), the cryptography in this model protects participants' privacy from each other.

The foundation for secure multi-party computation started in the late 1970s with the work on mental poker, cryptographic work that simulates game playing/computational tasks over distances without requiring a trusted third party. Note that traditionally, cryptography was about concealing content, while this new type of computation and protocol is about concealing partial information about data while computing with the data from many sources, and correctly producing outputs.

E Secure Query Processing On Encrypted Data

Fully homomorphic encryption schemes enable arbitrary computations on encrypted data. Even though it is shown that we build encryption schemes, to provide better security the data has to be encrypted. Many techniques are proposed to support computations on encrypted data with security guarantee and efficiency. We are aware of intruder in any formal work on secure skyline queries over encrypted data with semantic security.

An important research has been made to answer the problem that users may be interested for skyline queries in subspaces of the data. In a framework is proposed which uses skyline groups and decisive subspaces, to compute the skyline in any required subspace. Upon this framework an efficient algorithm is proposed, named SKYEY, which applies a top-down approach to recursively compute the skyline in subspaces. Pre-sorting strategies and multidimensional roll-up and drill-down analysis reduce the set of objects to be searched. A similar approach, the SKYCUBE, is proposed in, which is the union of the skylines of all possible non-empty subsets of a given set of dimensions. Several computation sharing strategies are used, based on effectively identifying the computation dependencies among multiple related skyline queries. Bottom-Up and Top-Down algorithms are proposed to compute the SKYCUBE efficiently

IV.REFERENCES

1. K. Fawaz and K. G. Shin, “Location privacy protection for smartphone users,” in Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 2014, pp. 239–250.

2. K. Fawaz, H. Feng, and K. G. Shin, “Anatomization and protection of mobile apps’ location privacy threats,” in fUSENIXg Security Symposium, 2015, pp. 753–768.

3. B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, “Achieving k-anonymity in privacy-aware location-based services,” in IEEE INFOCOM, 2014, pp. 754–762.

4. P.-R. Lei, W.-C. Peng, I.-J. Su, C.-P. Chang et al., “Dummy-based schemes for protecting movement trajectories,” Journal of Information Science and Engineering, vol. 28, no. 2, pp. 335–350, 2012.

5. T. Hara, A. Suzuki, M. Iwata, Y. Arase, and X. Xie, “Dummy-based user location anonymization under real-world constraints,” IEEE Access, vol. 4, pp. 673–687, 2016.

6. T. Wang, J. Zeng, M. Z. A. Bhuiyan, H. Tian, Y. Cai, Y. Chen, and B. Zhong, "Trajectory privacy preservation based on a fog structure for cloud location services," IEEE Access, vol. 5, pp. 7692–7701, 2017.

V . RESULT

As for future work, we plan to optimize the communication time complexity to further improve the performance of the protocol. Additional features like encryption and decryption using cryptography as well as images and videos can also be implemented in case of illusion data. Stegnography techniques can also be implemented for better future enhancement.

VI . CONCLUSION

In this paper, we proposed a fully secure skyline protocol on encrypted data using two non-colluding cloud servers under the semi-honest model. It ensures semantic security in that the cloud servers knows nothing about the data including indirect data patterns, query, as well as the query result. In addition, the client and data owner do not need to participate in the computation. We also presented a secure dominance protocol which can be used by skyline queries as well as other queries. Furthermore, we demonstrated twooptimizations, data partitioning and lazy merging, to further reduce the computation load. Finally, we presented our implementation of the protocol and demonstrated the feasibility and efficiency of the solution. Along with this we introduce more newtechniques like intruder breach, illusion data occurrencesand the encrypted data as well as the encrypted data and database.So that the data that has been saved in the server are with quiet better privacy and security.