ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

Privacy Preserving Location Based Services Using Secure Spatial Top K Query Processing

Mukthapuram Adityakavya[1] , M.Dharani Kumar[2]

M.Tech Student, Dept. of CSE, PVKK Institute of Technology, Affiliated to JNTUA, Andhra Pradesh, India [1]

Associate Professor in Dept. of CSE, PVKK Institute of Technology, Affiliated to JNTUA, Andhra Pradesh, India[2]

ABSTRACT: Recently, Mobile devices such as Smart Phones, PDA's play a significant role among the users. A distinct pattern of resources and services are obtained from the location of the mobile users. Several applications are designed in a way, that location is the primary building of the mobile applications. Subsequently, the location should activate with enhanced protection level. Mobile Service Providers (MSP) collects and aggregates the spatial data of the mobile users. In service- end perspectives, the mobile users will concentrate on retrieving the exact locations. These geographical locations are protected with the breach of trust. This paper targets to supply a trusted communication among Mobile Users, Mobile Servers and Mobile Service Providers. We framed an authentication algorithm E2SQ-LBS (Exploring and securing the spatial queries of location based services). Firstly, the mobile server gets the user-specified queries and verifies whether the user specified location. If it's authorized, a secure communication channel is enabled between the mobile users and Mobile Service Providers. These credentials are transmitted via public channel which leads to violation of privacy, known as Intrusion. To defend from colluding attacks, spatial queries oriented clustering is formed that helps to eliminate the redundant data. Ranking schemes is employed to sum up the topmost – searched queries. This application will perfectly work with Global Positioning System or Bluetooth with lessened storage space and power cost. Performance validation will prove that information are preserved at both user and server location.

KEYWORDS: Spatial top-k query, location-based service, security.

I.INTRODUCTION

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

The University's networks and shared information systems are protected in part by login credentials (user-IDs and passwords). Access passwords are also an essential protection for personal computers in most circumstances. Offices are usually open and shared spaces, so physical access to computers cannot be completely controlled.To protect your computer, you should consider setting passwords for particularly sensitive applications resident on the computer (e.g., data analysis software), if the software provides that capability.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

II. LITERATURE SURVEY

1) Secure Top-k Query Processing via Untrusted Location-Based Service Providers

AUTHORS: R. Zhang, Y. Zhang, and C. Zhang

This paper considers a novel distributed system for collaborative location-based information generation and sharing which become increasingly popular due to the explosive growth of Internet-capable and location-aware mobile devices. The system consists of a data collector, data contributors, location-based service providers (LBSPs), and system users. The data collector gathers reviews about points-of-interest (POIs) from data contributors, while LBSPs purchase POI data sets from the data collector and allow users to perform location-based top-k queries which ask for the POIs in a certain region and with the highest k ratings for an interested POI attribute. In practice, LBSPs are untrusted and may return fake query results for various bad motives, e.g., in favor of POIs willing to pay. This paper presents two novel schemes for users to detect fake top-k query results as an effort to foster the practical deployment and use of the proposed system. The efficacy and efficiency of our schemes are thoroughly analyzed and evaluated.

2) Secure Multidimensional Range Queries over Outsourced Data

AUTHORS: B. Hore, S. Mehrotra, M. Canim, and M. Kantarcioglu

In this paper, we study the problem of supporting multidimensional range queries on encrypted data. The problem is motivated by secure data outsourcing applications where a client may store his/her data on a remote server in encrypted form and want to execute queries using server's computational capabilities. The solution approach is to compute a secure indexing tag of the data by applying bucketization (a generic form of data partitioning) which prevents the server from learning exact values but still allows it to check if a record satisfies the query predicate. Queries are evaluated in an approximate manner where the returned set of records may contain some false positives. These records then need to be weeded out by the client which comprises the computational overhead of our scheme. We develop a bucketization procedure for answering multidimensional range queries on multidimensional data.

For a given bucketization scheme, we derive cost and disclosure-risk metrics that estimate client's computational overhead and disclosure risk respectively. Given a multidimensional dataset, its bucketization is posed as an optimization problem where the goal is to minimize the risk of disclosure while keeping query cost (client's computational overhead) below a certain user-specified threshold value. We provide a tunable data bucketization algorithm that allows the data owner to control the trade-off between disclosure risk and cost. We also study the trade-off characteristics through an extensive set of experiments on real and synthetic data.

3) Secure Ranked Keyword Search over Encrypted Cloud Data

AUTHORS: N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou

As Cloud Computing becomes prevalent, sensitive information are being increasingly centralized into the cloud. For the protection of data privacy, sensitive data has to be encrypted before outsourcing, which makes effective data utilization a very challenging task. Although traditional searchable encryption schemes allow users to securely search over encrypted data through keywords, these techniques support only boolean search, without capturing any relevance of data files. This approach suffers from two main drawbacks when directly applied in the context of Cloud Computing. On the one hand, users, who do not necessarily have pre-knowledge of the encrypted cloud data, have to post process every retrieved file in order to find ones most matching their interest, On the other hand, invariably retrieving all files containing the queried keyword further incurs unnecessary network traffic, which is absolutely undesirable in today's pay-as-you-use cloud paradigm. In this paper, for the first time we define and solve the problem of effective yet secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards practical deployment of privacy-preserving data hosting services in Cloud Computing.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

We first give a straightforward yet ideal construction of ranked keyword search under the state-of-the-art searchable symmetric encryption (SSE) security definition, and demonstrate its inefficiency. To achieve more practical performance, we then propose a definition for ranked searchable symmetric encryption, and give an efficient design by properly utilizing the existing cryptographic primitive, order-preserving symmetric encryption (OPSE). Thorough analysis shows that our proposed solution enjoys ``as-strong-as-possible" security guarantee compared to previous SSE schemes, while correctly realizing the goal of ranked keyword search. Extensive experimental results demonstrate the efficiency of the proposed solution.

4) Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data

AUTHORS: N. Cao, C. Wang, M. Li, K. Ren, and W. Lou

With the advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data have to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. In this paper, for the first time, we define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). We establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multi-keyword semantics, we choose the efficient similarity measure of "coordinate matching," i.e., as many matches as possible, to capture the relevance of data documents to the search query. We further use "inner product similarity" to quantitatively evaluate such similarity measure. We first propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. To improve search experience of the data search service, we further extend these two schemes to support more search semantics. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given. Experiments on the real-world data set further show proposed schemes indeed introduce low overhead on computation and communication.

5) Achieving Secure, Scalable, and Fine-Grained Access Control in Cloud Computing

AUTHORS: S. Yu, C. Wang, K. Ren, and W. Lou

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secure under existing security models.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

III. EXISTING SYSTEM

- Our work is most related to data outsourcing, for which we can only review representative schemes due to space constraints. The framework of data outsourcing was first introduced, in which a data owner outsources its data to a third-party service provider who is responsible for answering the data queries from either the data owner or other users. In general, there are two security concerns in data outsourcing: data privacy and query integrity.
- A bucketization approach was proposed, to enable efficient range queries over encrypted data, which was recently improved.
- Shi et al. presented novel methods for multi-dimensional range queries over encrypted data.
- Some most recent proposals aim at secure ranked keyword search or fine-grained access control over encrypted data.

DISADVANTAGES OF EXISTING SYSTEM:

- We observe two essential drawbacks with current top-k query services.
- First, individual LBSPs often have very small data sets comprising POI reviews. This would largely affect the usefulness and eventually hinder the more prevalent use of spatial top-k query services. Continue with the restaurant example. The data sets at individual LBSPs may not cover all the Italian restaurants within a search radius. Additionally, the same restaurant may receive diverse ratings at different LBSPs, so users may get confused by very different query results from different LBSPs for the same query. A leading reason for limited data sets at individual LBSPs is that people tend to leave reviews for the same POI at one or at most only a few LBSPs's websites which they often visit.
- Second, LBSPs may modify their data sets by deleting some reviews or adding fake reviews and return tailored query results in favor of the restaurants that are willing to pay or against those that refuse to pay.2 Even if LBSPs are not malicious, they may return unfaithful query results under the influence of various attacks such as the Sybil attack whereby the same attacker can submit many fake reviews for the same POI.

ADVANTAGES OF PROPOSED SYSTEM:

- Our schemes support both snapshot and moving top-k queries, which enable users to verify the authenticity and correctness of any top-k query result.
- The efficacy and efficiency of our schemes are thoroughly analyzed and evaluated through detailed simulation studies.

IV. PROPOSED WORK

- In this paper, we propose three novel schemes to tackle the above challenge for fostering the practical deployment and wide use of the envisioned system. The key idea of our schemes is that the data collector pre-computes and authenticates some auxiliary information (called authenticated hints) about its data set, which will be sold along with its data set to LBSPs.
- To faithfully answer a top-k query, a LBSP need return the correct top-k POI data records as well as proper authenticity and correctness proofs constructed from authenticated hints. The authenticity proof allows the query user to confirm that the query result only consists of authentic data records from the trusted data collector's data set, and the correctness proof enables the user to verify that the returned top-k POIs are the true ones satisfying the query.
- The first two schemes both target snapshot top-k queries but differ in how authenticated hints are pre-computed and how authenticity and correctness proofs are constructed and verified as well as the related communication and computation overhead.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

- The third scheme, built upon the first scheme, realizes efficient and verifiable moving top-k queries. The efficacy and efficiency of our schemes are thoroughly analyzed and evaluated.

IMPLEMENTATION

MODULES:

- System Model
- Location Based Service Provider
- Query Processing
- Query-Result Verification

MODULES DESCRIPTION:

System Model

- ✓ In the first module we develop the System model module. In this module we develop first the data collector module. The data collector module provides you the functionality of accessing the ratings provided by the user when the search is accompanied with respect to the specific location. This will also comes with the particulars of users who are registered with the system.
- ✓ Next we develop the User Module. The User has to register initially and get the login credentials from the system. This provides the user to login to the system and search for a place. The search will provide you the result based on the interests provided by the user at the time of registration. This will show you the exact location in the google-map and the Landmark associated with the searching text.

Location Based Service Provider

- ✓ In this module, we develop the Location Based Services Provide Modules. Location-based services Provider (LBSP) are a general class of computer program-level services that use location data to control features. As such LBSP is an information service which uses information on the geographical position of the mobile device.
- ✓ LBSP are used in a variety of contexts**, such** as health, indoor object search, entertainment, work, personal life, etc. LBSP include services to identify a location of a person or object, such as discovering the nearest Shopping mall or the where about of a location. Adding location information is carried out under the LBSP using the Google-Map Latitude and Longitude. The locations will be added based on the latitude and longitude of the exact location in Google-API.

Query Processing

- ✓ The LBSP purchases the data sets of interested POI categories from the data collector. For every POI category selected by the LBSP, the data collector returns the original data set D, the signatures on Merkle root hashes, and all the intermediate results for constructing the Merkle hash tree.
- ✓ Alternatively, the data collector can just return the first two pieces of information and let the LBSP itself perform a onetime process to derive the third piece in the same way as the date collector.

Query-Result Verification

- ✓ Now we discuss how the user verifies the authenticity and correctness of the query result, which can be done via a small plug-in developed by the data collector and installed on his web browser.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

- ✓ For authenticity verification, the user checks if every piece of information in the query result can lead to the same Merkle root hash matching the data collector's signature. Specifically, the user first determines which of the above five cases belongs to based on its message format. He then derives the indexes for all related POIs.
- ✓ To perform correctness verification, the user first checks if zones I encloses the query region R. If so, he proceeds with the following verifications in accordance with the aforementioned correctness condition used in query processing

V. CONCLUSION

This paper considers a novel distributed system for collaborative location-based information generation and sharing. We have proposed three novel schemes toenable secure top-k query processing via untrusted LBSPs for fostering the practical deployment and wide use of the envisioned system. Our schemes support both snapshot and moving top-k queries, which enable users to verify the authenticity and correctness of any top-k query result. The efficacy and efficiency of our schemes are thoroughly analyzed and evaluated through detailed simulation studies.

REFERENCES

[1] R. Zhang, Y. Zhang, and C. Zhang, "Secure Top-k Query Processing via Untrusted Location-Based Service Providers," Proc. IEEE INFOCOM '12, Mar. 2012.
[2] H. Yu, M. Kaminsky, P. Gibbons, and A. Flaxman, "SybilGuard: Defending against Sybil Attacks via Social Networks," IEEE/ ACM Trans. Networking, vol. 16, no. 3, pp. 576-589, June 2008.
[3] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks," IEEE/ACM Trans. Networking, vol. 18, no. 3, pp. 885-898, June 2010.
[4] H. Hacigumus, S. Mehrotra, and B. Iyer, "Providing Database as a Service," Proc. IEEE 18th Int'l Conf. Data Eng. (ICDE), Feb. 2002.
[5] W.-S. Ku, L. Hu, C. Shahabi, and H. Wang, "Query IntegrityAssurance of Location-Based Services Accessing Outsourced Spatial Databases," Proc. Int'l Symp. Advances in Spatial and Temporal Databases, July 2009.
[6] H. Hacig€um€u¸s, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over Encrypted Data in the Database-Service-Provider Model," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD'02), pp. 216-227, 2002.
[7] B. Hore, S. Mehrotra, and G. Tsudik, "A Privacy-Preserving Index for Range Queries," Proc. 30th Int'l Conf. Very Large Data Bases (VLDB'04), pp. 720-731, Aug. 2004.
[8] B. Hore, S. Mehrotra, M. Canim, and M. Kantarcioglu, "Secure Multidimensional Range Queries over Outsourced Data," The VLDB J., vol. 21, no. 3, pp. 333-358, 2012.
[9] E. Shi, J. Bethencourt, H. Chan, D. Song, and A. Perrig, "Multi-Dimensional Range Query over Encrypted Data," Proc. IEEE Symp. Security and Privacy (S&P'07), pp. 350-364, May 2007.
[10] N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data," Proc. IEEE 30th Int'l Conf. Distributed Computing Systems (ICDCS'11), June 2011.
[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOM, Apr. 2011.
[12] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Access Control in Cloud Computing," Proc. IEEE INFOCOM'10, Mar. 2010.
[13] H. Pang and K.-L. Tan, "Verifying Completeness of Relational Query Answers from Online Servers," ACM Trans. Information and System Security, vol. 11, no. 2, pp. 1-50, Mar. 2008.
[14] M. Narasimha and G. Tsudik, "Authentication of Outsourced Databases Using Signature Aggregation and Chaining," Proc. 11th Int'l Conf. Database Systems for Advanced Applications (DASFAA'06), pp. 420-436, Apr. 2006.
[15] H. Pang, J. Zhang, and K. Mouratidis, "Scalable Verification for Outsourced Dynamic Databases," Proc. VLDB Endowment, vol. 2, no. 1, pp. 802-813, 2009.