A V Mahesh * et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.6, Issue No.1, December - January 2018, 7774-7779.

Sorting Area Securely In Graphical Track Application

A.V.MAHESH
Department of Computer Science and Engineering
M.Tech Student, Sri Venkateswara College Of Engineering And Technology

RVLSN SASTRY
Department of Computer Science and Engineering
Associate Professor, Sri Venkateswara College of Engineering And Technology

N.SAI KIRAN
Department of Computer Science And Engineering Assistant Professor, Sri Venkateswara College of Engineering And Technology

Abstract: **Using geosocial applications, such as FourSquare, millions of people interact with their surroundings through their friends and their recommendations. Without adequate privacy protection, however, these systems can be easily misused, for example, to track users or target them for home invasion. In this paper, we introduce LocX, a novel alternative that provides significantly improvedlocation privacy without adding uncertainty into query results or relying on strong assumptions about server security. Our key insight is to apply secure user-specific, distance-preserving coordinate transformations to all location data shared with the server. The friends of a user share this user's secrets so they can apply the same transformation. This allows all location queries to be evaluated correctly by the server, but our privacy mechanisms guarantee that servers are unable to see or infer the actual location data from the transformed data or from the data access. We show that LocX provides privacy even against a powerful adversary model, and we use prototype measurements to show that it provides privacy with very little performance overhead, making it suitable for today's mobile devices.**

I. INTRODUCTION

EXISTING SYSTEM

Existing systems have mainly taken three approaches to improving user privacy in geosocial systems:

- Introducing uncertainty or error into location data.
- Relying on trusted servers or intermediaries to apply anonymization to user identities and private data.
- Relying on heavy-weight cryptographic or private information retrieval (PIR) techniques.

None of them, however, have proven successful on current application platforms. Techniques using the first approach fall short because they require both users and application providers to introduce uncertainty into their data, which degrades the quality of application results returned to the user. In this approach, there is a fundamental tradeoff between the amount of error introduced into the time or location domain, and the amount of privacy granted to the user. Users dislike the loss of accuracy in results, and application providers have a natural disincentive to hide user data from themselves, which reduces their ability to monetize the data. The second approach relies on the trusted proxies or servers in the system to protect user privacy. This is a risky assumption, since private data can be exposed by either software bugs and configuration errors at the trusted servers or by malicious administrators. Finally, relying on heavy-weight cryptographic mechanisms to obtain provable privacy guarantees are too expensive to deploy on mobile devices and even on the servers in answering queries such as nearest neighbor and range queries.

DISADVANTAGES OF EXISTING SYSTEM:

- Location data privacy. The servers should not be able to view the content of data stored at a location.
- This new functionality comes with significantly increased risks to personal privacy.

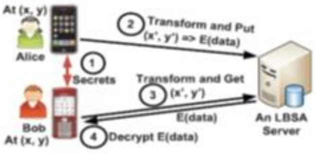
PROPOSED SYSTEM:

In this paper, we propose LocX(short for location to index mapping), a novel approach to achieving user privacy while maintaining full accuracy in location-based social applications (LBSAs from here on ward). Our insight is that many services do not need to resolve distance-based queries between arbitrary pairs of users, but only between friends interested in each other's locations and data. Thus, we can partition location data based on users' social groups, and then perform transformations on the location coordinates before storing them on untrusted servers. A user knows the transformation keys of all her friends, allowing her to transform her query into the virtual coordinate system that her friends use. Our coordinate transformations preserve distance metrics, allowing an application server to perform both point and nearest-neighbor queries correctly on transformed data. However, the transformation is secure, in that transformed values cannot be easily associated with real-world locations without a secret, which is only available to the members of the social group. Finally, transformations are efficient, in that they incur minimal overhead on the LBSAs. This makes the applications built on LocX lightweight and suitable for running on today's mobile devices.

ADVANTAGES OF PROPOSED SYSTEM:

- Our goal is to support both query types in an efficient fashion, suitable for today's mobile devices.
- Flexibility to support point, circular range, and nearest-neighbor queries on location data.
- Strong location privacy. The servers processing the data (and the administrators of these servers) should not be able to learn the history of locations that a user has visited.

SYSTEM ARCHITECTURE:



DATA FLOW DIAGRAM:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.

2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

System	:	Pentium IV 2.4 GHz.
Hard Disk	:	40 GB.
Floppy Drive	:	1.44 Mb.
Monitor	:	15 VGA Colour.
Mouse	:	Logitech.
Ram	:	512 Mb.

SOFTWARE REQUIREMENTS:

Operating system	:	Windows XP/7.
Coding Language	:	JAVA/J2EE
IDE	:	Netbeans 7.4.
Database	:	MYSQL.

II. LITERATURE REVIEW

1. Blind Evaluation of Nearest Neighbor Queries Using Space Transformation to Preserve Location Privacy

AUTHORS: A. Khoshgozaran and C. Shahabi

In this paper we propose a fundamental approach to perform the class of Nearest Neighbor (NN) queries, the core class of queries used in many of the location-based services, without revealing the origin of the query in order to preserve the privacy of this information. The idea behind our approach is to utilize one-way transformations to map the space of all static and dynamic objects to another space and resolve the query blindly in the transformed space. However, in order to become a viable approach, the transformation used should be able to resolve NN queries in the transformed space accurately and more importantly prevent malicious use of transformed data by untrusted entities. Traditional encryption based techniques incur expensive O(n) computation cost (where n is the total number of points in space) and possibly logarithmic communication cost for resolving a KNN query. This is because such approaches treat points as vectors in space and do not exploit their spatial properties. In contrast, we use Hilbert curves as efficient one-way transformations and design algorithms to evaluate a KNN query in the Hilbert transformed space. Consequently, we reduce the complexity of computing a KNN query to O(K × 22N/n) and transferring the results to the client in O(K), respectively, where N, the Hilbert curve degree, is a small constant. Our results show that we very closely approximate the result set generated from performing KNN queries in the original space while enforcing our new location privacy metrics termed u-anonymity and a-anonymity, which are stronger and more generalized privacy measures than the commonly used K-anonymity and cloaked region size measures.

COMPANY PROFILE:

Founded in 2009, JP iNFOTeCH located at Puducherry, has a rich background in developing academic student projects, especially in solving latest IEEE Papers, Software Development and continues its entire attention on achieving transcending excellence in the Development and Maintenance of Software Projects and Products in Many Areas.

ABOUT THE PEOPLE:

As a team we have the clear vision and realize it too. As a statistical evaluation, the team has more than 40,000 hours of expertise in providing real-time solutions in the fields of Android Mobile Apps Development, Networking, Web Designing, Secure Computing, Mobile Computing, Cloud Computing, Image Processing And Implementation, Networking With OMNET++ Simulator, client Server Technologies in Java,(J2EE\J2ME\EJB), ANDROID, DOTNET (ASP.NET, VB.NET, C#.NET), MATLAB, NS2, SIMULINK, EMBEDDED, POWER ELECTRONICS, VB & VC++, Oracle and operating system concepts with LINUX.

III. FEATURES OF SQL-SERVER

The OLAP Services feature available in SQL Server version 7.0 is now called SQL Server 2000 Analysis Services. The term OLAP Services has been replaced with the term Analysis Services. Analysis Services also includes a new data mining component. The Repository component available in SQL Server version 7.0 is now called Microsoft SQL Server 2000 Meta Data Services. References to the component now use the term Meta Data Services. The term repository is used only in reference to the repository engine within Meta Data Services

SQL-SERVER database consist of six type of objects,

They are,

1. TABLE

2. QUERY

3. FORM

4. REPORT

5. MACRO

TABLE:

A database is a collection of data about a specific topic.

VIEWS OF TABLE:

We can work with a table in two types,

1. Design View

2. Datasheet View

Design View

To build or modify the structure of a table we work in the table design view. We can specify what kind of data will be hold.

Datasheet View

To add, edit or analyses the data itself we work in tables datasheet view mode.

QUERY:

A query is a question that has to be asked the data. Access gathers data that answers the question from one or more table. The data that make up the answer is either dynaset (if you edit it) or a snapshot (it cannot be edited).Each time we run query, we get latest information in the dynaset. Access either displays the dynaset or snapshot for us to view or perform an action on it, such as deleting or updating.The OLAP Services feature available in SQL Server version 7.0 is now called SQL Server 2000 Analysis Services. The term OLAP Services has been replaced with the term Analysis Services. Analysis Services also includes a new data mining component. The Repository component available in SQL Server version 7.0 is now called Microsoft SQL Server 2000 Meta Data Services. References to the component now use the term Meta Data Services. The term repository is used only in reference to the repository engine within Meta Data Services

SYSTEM STUDY

FEASIBILITY STUDY: The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the

Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

IV. CONCLUSION

This paper describes the design, prototype implementation, and evaluation of LocX, a system for building location based social applications (LBSAs) while preserving user location privacy. LocX provides location privacy for users without injecting uncertainty or errors into the system, and does not rely on any trusted servers or components. LocX takes a novel approach to provide location privacy while maintaining overall system efficiency, by leveraging the social data-sharing property of the target applications. In LocX, users efficiently transform all their locations shared with the server and encrypt all location data stored on the server using inexpensive symmetric keys. Only friends with the right keys can query and decrypt a user's data. We introduce several mechanisms to achieve both privacy and efficiency in this process, and analyze their privacy properties.

Using evaluation based on both synthetic and real-world LBSA traces, we find that LocX adds little computational and communication overhead to existing systems. Our LocX prototype runs efficiently even on resource constrained mobile phones. Overall, we believe that LocX takes a big step toward making location privacy practical for a large class of emerging geosocial applications.

V. REFERENCES

[1] M. Motani, V. Srinivasan, and P.S. Nuggehalli, "PeopleNet: Engineering a Wireless Virtual Social Network," Proc. ACM MobiCom, 2005.

[2] M. Hendrickson, "The State of Location-Based Social Networking on the iPhone," http://techcrunch.com/2008/09/28/the-state-oflocation-based-social-networking-on-the-iphone, 2008.

[3] P. Mohan, V.N. Padmanabhan, and R. Ramjee, "Nericell: Rich Monitoring of Road and Traffic Conditions Using Mobile Smartphones," Proc. Sixth ACM Conf. Embedded Network Sensor Systems, 2008.

[4] G. Ananthanarayanan, V.N. Padmanabhan, L. Ravindranath, and C.A. Thekkath, "Combine: Leveraging the Power of Wireless Peers through Collaborative Downloading," Proc. Fifth Int'l Conf. Mobile Systems, Applications Services, 2007.

[5] M. Siegler, "Foodspotting is a Location-Based Game that Will Make Your Mouth Water," http://techcrunch.com/2010/03/04/foodspotting, 2013.

[6] "SCVNGR," http://www.scvngr.com, 2013.

[7] B. Schilit, J. Hong, and M. Gruteser, "Wireless Location Privacy Protection," Computer, vol. 36, no. 12, pp. 135-137, Dec. 2003.

[8] F. Grace, "Stalker Victims Should Check for GPS," http://www.cbsnews. com, Feb. 2003.

[9] A. Gendar and A. Lisberg, "How Cell Phone Helped Cops Nail Key Murder Suspect. Secret 'Pings' that Gave Bouncer Away," New York Daily News, Mar. 2006.

[10] "Police: Thieves Robbed Homes Based on Facebook, Social Media Sites," WMUR News, http://www.wmur.com/r/24943582/detail.html, Sept. 2010.

[11] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking," Proc. First Int'l Conf. Mobile Systems, Applications Services, 2003.

[12] M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The New Casper: A Privacy-Aware Location-Based Database Server," Proc. IEEE 23rd Int'l Conf. Data Eng., 2007.

[13] B. Gedik and L. Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model," Proc. IEEE 25th Int'l Conf. Distributed Computing Systems, 2005.

[14] T. Jiang, H.J. Wang, and Y.-C. Hu, "Preserving Location Privacy in Wireless Lans," Proc. Fifth Int'l Conf. Mobile Systems, Applications Services, 2007.

[15] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing Location-Based Identity Inference in Anonymous Spatial Queries," IEEE Trans. Knowledge Data Eng., vol. 19, no. 12, pp. 1719-1733, Dec. 2007.

[16] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private Queries in

Location Based Services: Anonymizers Are Not Necessary," Proc. ACM SIGMOD Int'l Conf. Management Data, 2008.

[17] S. Papadopoulos, S. Bakiras, and D. Papadias, "Nearest Neighbor Search with Strong Location Privacy," Proc. VLDB Endowment, vol. 3, nos. 1/2, pp. 619-629, Sept. 2010.

[18] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location Privacy via Private Proximity Testing," Proc. Network Distributed System Security Conf., 2011.

[19] G. Zhong, I. Goldberg, and U. Hengartner, "Louis Lester and Pierre: Three Protocols for Location Privacy," Proc. Seventh Int'l Conf. Privacy Enhancing Technologies, 2007.

[20] N. Daswani and D. Boneh, "Experimenting with Electronic Commerce on the Palmpilot," Proc. Third Int'l Conf. Financial Cryptography, 1999.

[21] A. Khoshgozaran and C. Shahabi, "Blind Evaluation of Nearest Neighbor Queries Using Space Transformation to Preserve Location Privacy," Proc. 10th Int'l Conf. Advances Spatial Temporal Databases, 2007.

[22] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIVE: Anonymous Location-Based Queries in Distributed Mobile Systems," Proc. 16th Int'l Conf. World Wide Web, 2007.

[23] P. Golle and K. Partridge, "On the Anonymity of Home/Work Location Pairs," Proc. Pervasive Computing, 2009.

[24] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing Security and Privacy in Traffic-Monitoring Systems," IEEE Pervasive Computing Magazine, vol. 5, no. 4, pp. 38-46, Oct. 2006.

[25] B. Hoh et al., "Preserving Privacy in GPS Traces via Uncertainty-Aware Path Cloaking," Proc. 14th ACM Conf. Computer Comm. Security, 2007.

[26] J. Krumm, "Inference Attacks on Location Tracks," Proc. Fifth Int'l Conf. Pervasive Computing, 2007.

[27] A. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing Comm. Workshop, 2004.

[28] M.L. Yiu, C.S. Jensen, X. Huang, and H. Lu, "Spacetwist: Managing the Trade-Offs among Location Privacy Query Performance and Query Accuracy in Mobile Services," Proc. IEEE 24th Int'l Conf. Data Eng., 2008.

[29] D. Lin, E. Bertino, R. Cheng, and S. Prabhakar, "Position Transformation: A Location Privacy Protection Method for Moving Objects," Proc. Int'l Workshop Security Privacy GIS LBS, 2008.

[30] C.-Y. Chow and M.F. Mokbel, "Enabling Private Continuous Queries for Revealed User Locations," Proc. 10th Int'l Conf. Advances Spatial Temporal Databases, pp. 258-275, 2007.

[31] E.O. Turgay, T.B. Pedersen, Y. Saygin, E. Savas, and A. Levi, "Disclosure Risks of Distance Preserving Data Transformations," Proc. 20th Int'l Conf. Scientific Statistical Database Management, 2008.

[32] S. Mascetti, C. Bettini, and D. Freni, "Longitude: Centralized Privacy-Preserving Computation of Users' Proximity," Proc. Sixth VLDB Workshop Secure Data Management, 2009.

[33] S. Mascetti, C. Bettini, D. Freni, X.S. Wang, and S. Jajodia, "Privacy-Aware Proximity Based Services," Proc. Tenth Int'l Conf. Mobile Data Management: Systems, Services Middleware (MDM '09), 2009.

[34] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second- Generation Onion Router," Proc. 13th Conf. USENIX Security Symp., 2004.

[35] H. Hu, J. Xu, C. Ren, and B. Choi, "Processing Private Queries over Untrusted Data Cloud through Privacy Homomorphism," Proc. IEEE 27th Int'l Conf. Data Eng. (ICDE), 2011.

[36] W.K. Wong, D.W.-L. Cheung, B. Kao, and N. Mamoulis, "Secure kNN Computation on Encrypted Databases," Proc. SIGMOD Int'l Conf. Management (SIGMOD '09), 2009.

[37] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: An Online Social Network with User Defined Privacy," Proc. ACM SIGCOMM Conf. Data Comm., 2009.

[38] T. Ristenpart, G. Maganis, A. Krishnamurthy, and T. Kohno, "Privacy-Preserving Location Tracking of Lost or Stolen Devices: Cryptographic Techniques and Replacing Trusted Third Parties with

DHTs," Proc. 17th Conf. Security Symp. (SS '08), 2008.

[39] A. Mislove, K. Gummadi, and P. Druschel, "Exploiting Social Networks for Internet Search," Proc. Fifth Workshop Hot Topics Networks (HotNets '06), 2006.

[40] A. Mislove, A. Post, P. Druschel, and K. Gummadi, "Ostra: Leveraging Trust to Thwart Unwanted Communication," Proc. Fifth USENIX Symp. Networked Systems Design Implementation (NSDI '08), pp. 15-30, 2008.

[41] T. Isdal, M. Piatek, A. Krishnamurthy, and T. Anderson, "Privacy-Preserving P2P Data Sharing with Oneswarm," Proc. ACM SIGCOMM, 2010.

[42] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," Proc. 16th Ann. Int'l Cryptology Conf. Advances Cryptology, 1996.

AUTHOR's PROFILE

A.V.MAHESH, Department of Computer Science and Engineering M.Tech Student, Sri Venkateswara College Of Engineering And Technology

RVLSN SASTRY, Department of Computer Science and Engineering Associate Professor, Sri Venkateswara College of Engineering And Technology

N.SAI KIRAN, Department of Computer Science And Engineering Assistant Professor, Sri Venkateswara College of Engineering And Technology