INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 6 (2016) PAGES 1281 - 1285
RECEIVED : 25/10/2016. PUBLISHED: 01/11/2016 November 1, 2016

AN EFFECTIVE ACCESSING IN SOCIAL MEDIA APPLICATION USING FEEDBACK RELAVENCE

[1]M.Maragathamani, [2]R.Vijay Kumar,
[1]PG Scholar, Dept of CSE, AVS Engineering College,
[2]Asst prof, of CSE, AVS Engineering College.

Abstract:

Using geosocial applications, such as Four Square, 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 improved location 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.

Keyword:LocX, Keyword search (KWS), Geosocial,LBSA.

1. INTRODUCTION

Mobile computing is human computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications. Mobile Computing is taking a computer and all necessary files and software out into the field. Mobile computing: being able to use a computing device even when being mobile and therefore changing location. Portability is one aspect of mobile computing. Mobile computing is the ability to use computing capability without a pre-defined location and/or connection to a network to publish and/or subscribe to information.

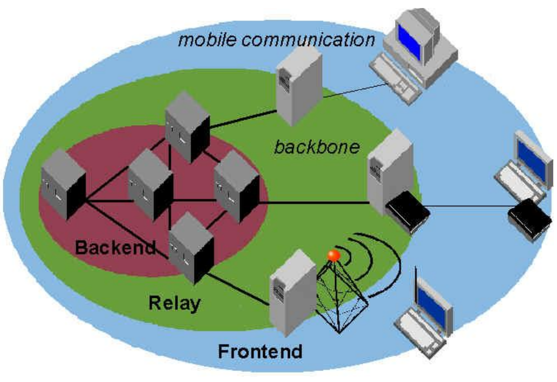

Fig.1.Mobile computing

Smart phone applications offered by Apple iTunes and Android are quickly becoming the dominant computing platform for today's user applications. Within these markets, a new wave of geosocial applications is fully exploiting GPS location services to provide a "social" interface to the physical world. Examples of popular social applications include social, local friend recommendations for dining and shopping, as well as collaborative network services and game. The explosive popularity of mobile social networks such as SCVNGR indicate that in the future, social recommendations will be our primary source of information about our surroundings. Unfortunately, this new functionality comes with significantly increased risks to personal privacy. Geosocial applications operate on fine-grain, time-stamped location information. For current services with minimal privacy mechanisms, these data can be used to infer a user's detailed activities, or to track and predict the user's daily movements. In fact, there are numerous real-world examples where the unauthorized use of location information has been misused for economic gain, physical stalking and to gather legal evidence. Even more disturbing, it seems that less than a week after Facebook turned on their popular "Places" feature for tracking users' locations, such location data were already used by thieves to plan home invasions. Clearly, mobile social networks of tomorrow require stronger privacy properties than the open-to-all policies available today.

2. RELATED WORK

In this paper[1]"DBXPLORER: a system for keyword-based search over relational databases" Keyword search (KWS) over relational databases has recently received significant attention. Many solutions and many prototypes have been developed. This task requires addressing many issues, including robustness, accuracy, reliability, and privacy. An emerging issue, however, appears to be performance related: current KWS systems have unpredictable running times. In particular, for certain queries it takes too long to produce answers, and for others the system may even fail to return (e.g., after exhausting memory). Today's users have been "spoiled" by the performance of Internet search engines, KWS systems should return whatever answers they can produce quickly and then provide users with options for exploring any portion of the answer space not covered by these answers. The basic idea is to produce answers that can be generated quickly as in today's KWS systems, then to show users query forms that characterize the unexplored portion of the answer space. Combining KWS systems with forms allows us to bypass the performance problems inherent to KWS without compromising query coverage. We provide a proof of concept for this proposed approach, and discuss the challenges encountered in building this hybrid system. In this paper[2]" Protecting User Identity in Geo-Social ApplicationsUsing Coordinate Transformations" Now a days people mostly depend on the geo-social applications which is a location based service which serves the user by providing recommendations about the neighbor places from their vicinity. Using such applications, the user interacts with their surroundings to know about their search locations and to share their reviews. Due to the lack of protection to their location identity the user's location information is misused by the hackers and other unwanted users to get access to the personal information such economic gain physical stalking etc. Location to index mapping is a technique that provides the security to user identity by preserving coordinate transformation to the location data that shared with the servers. It is made suitable to implement in the mobile devices.

In this paper[3]" Anonymous usage of location-based services through spatial and temporal cloaking "The tremendous growth of the Internet has significantly reduced the cost of obtaining and sharing information about individuals, raising many concerns about user privacy. Spatial queries pose an additional threat to privacy because the location of a query may be sufficient to reveal sensitive information about the queries. In this paper we focus on k nearest neighbor (kNN) queries and define the notion of strong location privacy, which renders a query indistinguishable from any location in the data space. The previous work fails to support this property for arbitrary kNN search. Towards these methods that offer strong location privacy, by integrating private information retrieval (PIR) functionality. Specifically, secure hardware-aided PIR, which has been proven very efficient and is currently considered as a practical mechanism for PIR. By analyzing the drawbacks AHG is proposed to tackle them.

3. PROBLEM FORMULATION

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 itemization to user identities and private data and relying on heavy-weight cryptographic or private information retrieval (PIR) techniques. None of them, however, have proven successful on current application platforms. There are mainly three categories of proposals on providing location privacy in general LBSs that do not specifically target social applications. First is spatial and temporal cloaking wherein approximate location and time is sent to the server instead of the exact values. The second category is location transformation, which uses transformed location coordinates to preserve user location privacy. The third category of work relies on PIR to provide strong location privacy. Its performance, although improved by using special hardware.

4. PROPOSED SYSTEM

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 wards). Many services do not need to resolve distance-based queries between arbitrary pairs of users, but only between friends interested in each others locations and data. Thus, we can partition location data based on user social groups, and then perform transformations on the location coordinates before storing them on encrusted 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.

5. SYSTEM MODEL

The following modules are present in the project.

1. LBS MODULE
2. LONGITUTDE AND LATITIUDE
3. LOCATION TO INDEX MAPPING
4. LOCATION TRANSFORMATION
5. SCALABILITY IN PRIVACY PRESERVING

1. LBS MODULE

Location-based services are emerging as the next killer app in personal wireless devices, but there are few safeguards on location privacy . In fact, the demand for improved public safety is pushing regulation in the opposite direction. The challenge with wireless location privacy is making it easy to share the right information with the right people or service at the right time and, conversely. In addition, the corporate world can discover and match a person's location trail to create unwelcome spam. Disclosure of location information may cause embarrassment or humiliation.

2. LONGITUDE & LATITUDE

Longitude is a work which adopts this technique. Longitude transforms locations coordinates to prevent disclosure to the servers. In Longitude, the secrets for transformation are maintained between every pair of friends in order to allow users to selectively disclose locations to friends. Longitude eases privacy concerns by making it possible to share a user's location data blindly and allowing the user to control who can access her location, when and to what degree of precision. This is with the help of cryptographer algorithms and this can be adapted to mobile phones also. Here in the system model it consists of a location-sharing service provider and the set of users registered with the provider. The provider store location along with some data.

The user can determine which other users should view their data. The security model assumes that the server is honest but curious about user's detailed location and information. The Longitude protocol is based on proxy encryption. Here the user registers with the service provider, the service Provider provide them with some cryptographer elements. This can be saved safely in the user devices.

3. LOCATION TO INDEX MAPPING

Location to index mapping is another approach towards location privacy of users here in this system the data and location are partitioned into two components and are stored in separate servers. The authorized person with the necessary credentials can only access the location information of the users. The location is stored in a server called as index server via another encrusted server called as proxy server. Proxy server is used in order for preventing the index server from uniquely identifying the client devices. Here the location information is transferred to another coordinate system and this is known as transformed location. Each user will be provided with an element which consists of a shift, a rotation angle, and an encryption key. Here in this system this element will be shared with trusted friends circle.

4. LOCATION TRANSFORMATION

The location is transformed using the shift and rotation in the secret element of the particular user. This transformed location will be encrypted by the encryption key of the particular user and will be stored in the index server via the proxy server in a unique index. The data is encrypted and stored into the data server directly in previously defined unique index. A person who has the decryption key, rotation and shift only can retrieve the data from the index and data servers. If user B want to know about the location information and corresponding data that A has put on the server, then user B with the right elements need to transform the specific location to be known to the transformed coordinate of user A and this need to be send to the proxy server and from proxy this request will be redirected to the

Index server and the corresponding index for the data will be retrieved to the user B. With this index user B can request for data corresponding to the index in the data server and the encrypted data will be retrieved to the user. Using the decryption key user can decrypt the information related to the particular location.

5. SCALABILITY IN PRIVACY PRESERVING

When two users decide to make a connection, they should be assured that messages indeed originate from each other. As such, the infrastructure to exchange encounter information should be accessible most of the time. The unavailability of individual users should not affect the availability of other users. Since the time at which encounter parties check for potential encounters associated with their activities could be arbitrary, the encounter-based social network is more sensitive to availability than conventional social networks.With typical social networks being large in size, any potential social network design, including those based on encounters, should scale to support a large number of simultaneous users. This requires minimizing dependence on a centralized entity.

CONCLUSION

LocX is a method which provides the privacy protection for user information in location based applications with affecting the quality of the services given to the user. This method efficiently transforms all the location identities that is accessed by the servers and also encrypt the data associated with it. This technique is analyzed in both the synthetic data and the real-world LBSA traces. LocX uses light weighted cryptographic technique that makes it to run efficiently in the mobile devices. However the LocX technique have little computational and communication overhead this can be enhanced in the future considerations.

REFERENCE

[1] 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.

[2] N. Daswani and D. Boneh, “Experimenting with Electronic Commerce on the Palmpilot,” Proc. Third Int’l Conf. Financial Cryptography, 1999.

[3] 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.

[4] 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.

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

[6] 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.

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

[8] J. Krumm, “Inference Attacks on Location Tracks,” Proc. Fifth Int’l Conf. Pervasive Computing, 2007.

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

[10] 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.