International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A Novel Approach for Protecting Location Information in Geosocial Applications

*SYEDA SOBIA FAREES **M.SURESH KUMAR

*M.TECH student , Dept of CSE, VAAGDEVI COLLEGE OF ENGINEERING
**Assistant Professor, Dept of CSE , VAAGDEVI COLLEGE OF ENGINEERING

Abstract:

With geo-social applications, like FourSquare, Gowalla millions of people communicate with their surroundings through their friends and their recommendations and comments. Without privacy protection, these applications can be easily misused, e.g., to track or target users for home invasion. In this paper, we introduce a novel alternative Locx that provides significantly-improved location privacy without providing uncertainty into query results or relying on strong assumptions on server security. Our key in sight is to apply secure user-specific, coordinate transformations to all location data shared in the server. The friends of a user share this user's secrets so they can apply the same transformation We show that LocX provides location privacy even against a powerful adversary, and making it suitable for today's mobile device applications .Also Locx provides location privacy with very little performance overhead, and location transformation function is used to hide the location data from others.

Keywords: LBSAs, Locx, L2I, I2D

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

1. Introduction

Nowadays, smartphone applications offered by Apple iTunes and Android are quickly becoming the dominant computing platform for today's user mobile applications with billions in downloads and annual revenue. Examples of popular social applications include social rendezvous [1], local friend recommendations for dining and shopping [2]. The wide popularity of mobile social networks such as SCVNGR and Four Square indicate that social recommendations will be our primary source of information about our surroundings in the future. But, this new functionality comes with significantly increased risks to users privacy. Geo-social applications operate on time-stamped location information. For current systems with less privacy mechanisms, this data can be used to infer or track user's detailed activities, and predict the user's daily movements. That is, mobile social networks of future require stronger privacy properties than the open to-all policies available today. In this paper, we propose LocX (short for location to index mapping), a novel approach for achieving user privacy while maintaining full accuracy in location-based social mobile applications .Our key insight is that based on users' social groups, and then perform transformations on the location coordinates before storing them on untrusted servers or proxies. A user knows the transformation keys of all her friends, allowing her to transform her query into the 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, transformation incur minimal overhead on the LBSAs. Locx has a main drawback when an untrusted person tries to access the users location data.So to resolve this problem,a transformation index(latitude, longitude) is maintained by every user. Thus untrusted person retrieves only fake location values according to the transformation indices. It makes the applications built on LocX lightweight and suitable for running on today's mobile device applications.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

2. Related Works

Existing systems have mainly taken many approaches for improving personal privacy in geo-social applications [5]. But none of them, have proven successful on current application platforms. Techniques using the approach require both users and application providers to introduce uncertainty into their data, which degrades the quality of results returned to the user. The next approach relies on the servers in the system to protect user privacy. This is a risky assumption, because personal data can be exposed by either software bugs and configuration errors. Finally, relying on heavy-weight cryptographic mechanisms to obtain provable privacy guarantees are too expensive to deploy on mobile devices [6] .

3. Implementation

To clarify the need for each component of Locx, we start with basic design description. The server should support different types of queries such as point, circular range and nearest-neighbor queries on location data. For the server to be able to support this, we need to reveal the location coordinates in plain text. But doing so would permit the malicious server to destruct a user's location privacy.

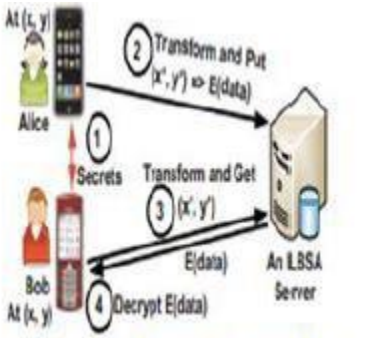

Figure 1: A Basic Design of Locx

We propose the idea of coordinate transformation. Each user u in the system uses a set of secrets that they reveal only to their friends. These secrets include a rotation angle θu, a shift bu, and a symmetric key symmu. The users exchange their secrets via interactions when friends meet in person, or via a trusted channel, like email, phone etc. The secret angle and shift are used by the users to transform all the location coordinates they share with the servers. Similarly, the secret symmetric key is used to encrypt all the location details they store on the servers. These secrets are known only to the friends, and hence only the friends can retrieve and decrypt the location data. Figure 1 depicts this basic design. A limitation: This basic design has one limitation: the server can uniquely detect client devices (for

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

e.g. using the IP address). Using this, the server can associate different transformed coordinates to the same user. Sufficient number of such associations can break the transformations. Somaintaining unlinkability between different queries is very critical. So one approach to resolve this limitation is to route all the queries through an anonymous routing system like Tor. But simply routing the data through Tor all the time willn't be Locx build on the top of the basic design,and here introduces two mechanisms to overcome basic design limitations. First, in LocX, we divide the mapping between the location and its data into two sets:a mapping from the transformed location to an encrypted index(L2I), and a mapping from the index tothe encrypted location data(I2D). This division helps in making our system more efficient. Second, users saveand retrieve the L2Is via untrusted proxies. This redirection of data via proxies, with division, significantly improves privacy in LocX. For efficiency,I2Ds are not proxied, but privacy is preserved. Save their L2Is on the index server through untrusted proxies. These proxies can be of any of the following: PlanetLab nodes, corporate NATs and email servers in a user's work places, a user's home and office desktops or laptops. We only require a one-hop indirection the proxies are non-malicious and do not collude with the index server. In Locx if any malicious user tries to access the application, then server will provide fake location details and pretending like a trusted user. Figure 2 depicts the design of Locx.

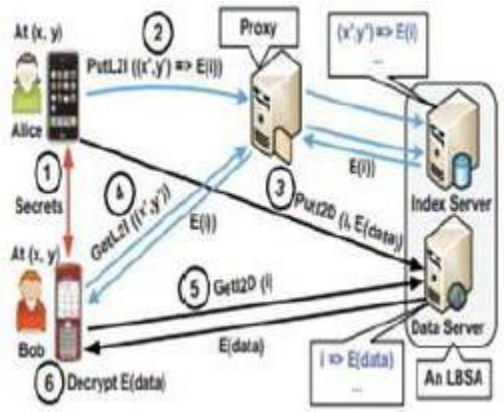

Figure 2: Design of LocX.1) Alice and Bob exchange their secrets via trusted channels, 2)Alice generates an L2I and I2D from her review of the restaurant (at(x,y)), and stores the L2I on the index server via a proxy. 3)She then saves the I2D on the data server directly, 4)Bob later visits the restaurant and fetches for L2Is from his friends by sending the transformed coordinates via a proxy, 5)he decrypts the L2I obtained and then

queries for the correspondingI2D, 6)finally Bob decrypts Alice's review.

4. Conclusion

This paper describes the design, implementation ,and evaluation of LocX.A system for developing location-based social applications(LBSAs) while maintaining user location privacy. LocX provides location privacy for users without injecting uncertainty in to the system. LocX uses a novel approach to provide location privacy while preserving overall system efficiency. In LocX, users efficiently transform all their location data shared with the server and encrypt all location data stored on the server. Only friends with the right keys can decrypt a user's data. **References**

[1] M. Motani, V. Srinivasan, and P. S. Nuggehalli, "Peoplenet: engineering a wireless virtual social network," in Proc. of MobiCom, 2005.

[2] M. Hendrickson, "The state of location-based social networking," 2008.

[3] M. Gruteser and D.Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in Proc. of Mobisys, 2003.

[4] T. Jiang, H. J. Wang, and Y.-C. Hu, "Preserving location privacy in wireless lans," in Proc. of MobiSys, 2007.

[5] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: anonymizers are not necessary," in SIGMOD Conference.2008.

[6] N. Daswani and D. Boneh, "Experimenting with electronic commerce on the palmpilot," in Financial Cryptography. Springer, 1999 .

AUTHOR 1 :-

*Syeda Sobia Farees completed her B tech in Jaya Institute of Technology and Science for Women in 2014 and pursuing M-Tech in Vaagdevi College of Engineering

AUTHOR 2:-

**M.Suresh Kumar is working as Assistant Professor in Dept of CSE, Vaagdevi College of Engineering