

A New Methodology to Preserve User Profile and Functionality In Geosocial Networks

P. Dinakaran, L. Mogana Priya

Computer Science and Engineering, IFET College of Engineering, Villupuram, Tamil Nadu, India

ABSTRACT

Social networking services have become an important source to store individual information. Geolocation on web based social network can be IP-based or used hotspot trilateration. A recent addition to this space, social networking such as Yelp or Foursquare, collects some user locations, through check-ins performed by users at visited venues. Overtly, individual information allows social networking providers to offer a different type of applications, including individual recommendations and targeted advertising, and venue owners to promote their business through the spatio-temporal incentives. Without individual people may be reluctant to use social networking; without user information the provider not able to use applications and have no incentive to associate in social networking services.

Keywords : PROFILER, Homomorphic Cryptosystem, Location centric profiles (LCP), Anonymizer, Identity fake news, and Benaloh's Cryptosystem.

I. INTRODUCTION

In this paper, we have introduced the PROFILER, a framework for building location centric profiles (LCP), combined built over the profiles of users that have visited through the different locations (i.e., venues) and a set of co-located users. User submitted location data or geo-location technique that can allow social network to connect and coordinate user with local people. PROFILER endows users with powerful information about themselves guarantees and providers with correctness assurances. In addition to a venue centric approach, we propose a distributed solution for computing real time location centric profiles snapshots over the profiles.

II. METHODS AND MATERIAL

1. System Analysis

Existing System

- In Existing system, a recent addition to this space, geo-social networks (GSNs) such as Yelp and Foursquare further collect fine grained location

information, through check-ins performed by users at visited venues.

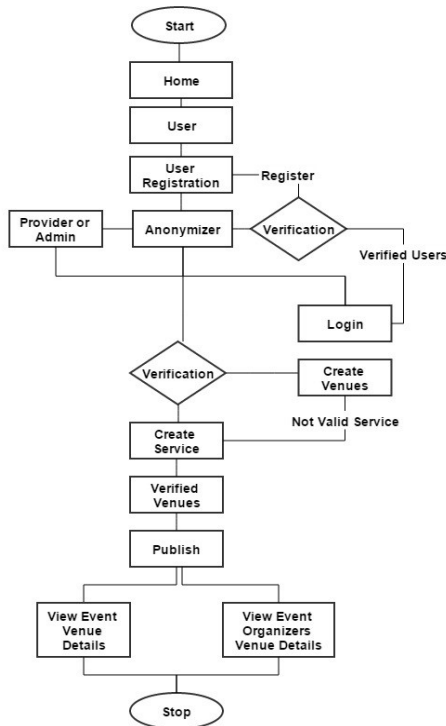
- The personal information allows GSN providers to offer a variety of applications, including personalized recommendations.
- There is no significant to provide privacy of users when reporting information (e.g., age, gender, location).
- Targeted advertising, and venue owners to promote their businesses through spatio-temporal incentives, e.g., rewarding frequent customers through accumulated badges.

Proposed System

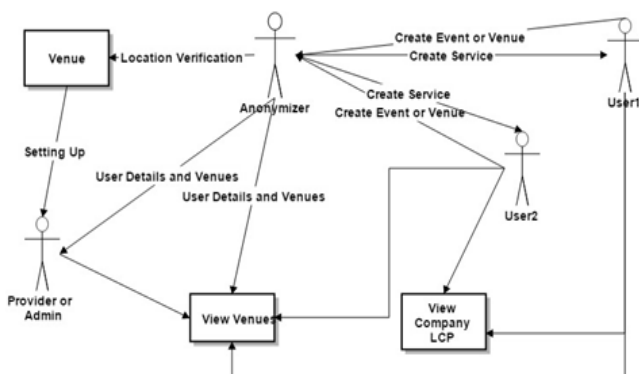
- In proposed system, a venue centric $PROFIL_R$ that relieves the GSN provider from involvement in venue specific activities. To achieve this, $PROFIL_R$ stores and builds LCPs at venues.
- It relies on Benaloh's homomorphic cryptosystem and zero knowledge proofs to enable oblivious and provable correct LCP computations.
- A complete decentralized $PROFIL_R$ extension, built around the notion of snapshot LCPs.

- The distributed PROFIL_R enables user devices to aggregate the profiles of co-located users, without assistance from a venue device.
- Snapshot LCPs are not certain to venues, but in its place user devices can compute LCPs of neighbors at any locations of interest.
- The communications in both PROFIL_R implementations are performed over ad hoc wireless connections.

FLOW CHART



2. Architecture Diagram



3. Literature Survey

Location-Related Privacy in Geo-Social Networks

Geo-social networks (Geo SNs) provide context-ware services that help associate location users and content. The proliferation of Geo SNs indicates that they are rapidly attracting users. Geo SNs currently offer different types of services including photo sharing, friend tracking, check-ins.

III. RESULTS AND DISCUSSION

1. MODULE DESCRIPTION

Registration Panel

The registration of user is mandatory to create account. Only after the registration, the user able to access the system. Then, the registration only for users not for admin.

Anonymizer Panel

Operates correctly – the output corresponds to a permutation of the inputs.

Provides privacy – an observer is unable to determine which input element corresponds to a given output element in any way better than guessing.

All the activity of the user part in the network will be preserved by this spotter or anonymizer. Then the anonymizer will create the service for all user venues.

User Panel

The Users requested to register their details for login. Users can able to see their Venues and other user venues.

After the login, the user can start creating venues or events. When the user once creating venue the LCP of particular company will be tracked, the user and non-user of the network user also view LCP of the company.

If there is a suggestion, the user can able to send query to send provider of the network. Other user i.e. non-registered user also can send suggestions to provider.

Admin Panel

Admin or Provider will manage the user details in the network. The user detail after the acceptance of anonymizer will send to the admin. But if the profile once accepted the users details no longer to be in the anonymizer part.

Provider or admin will manage the query or suggestions from the user or visitors.

All the venues which are published by the user will be managed by the admin.

2. ALGORITHM DETAILS

PROFILR

Construction and computation of location centric profiles (LCPs) while simultaneously ensuring privacy and correctness of participants. Obtain both a venue centric and a decentralized solution.

HOMOMORPIC CRYPTOSYSTEM

Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on cipher text and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. It has Benaloh's cryptosystem method to proceed encryption.

It contains following functions

- Key Generation,
- Encryption,
- Decryption.

BENALOH'S CRYPTOSYSTEM

The Benaloh's cryptosystem is an extension of the Goldwasser-Micali cryptosystem (GM) blocks of data can be encrypted at once, whereas in GM each bit is encrypted individually.

IV. CONCLUSION

In this paper we have proposed the PROFILR, a framework and components for individual and correctly. We should have proved the ability of our solutions to satisfying the information about themselves and

correctness requirements. We should have shown that PROFILR, is an familiar with , even when completed on resource constrained all domains. The communication should have both PROFILR implementations are performed over ad hoc wireless connection. We show that PROFILR is efficient even when deployed on previous generation smartphones.

V. REFERENCES

- [1]. Yelp, Inc., San Francisco, CA, USA. (2014, Feb. 28) [Online]. Available: <http://www.yelp.com>
- [2]. Foursquare, New York, NY, USA. (2014, Feb. 28) [Online]. Available: <https://foursquare.com/>
- [3]. B. Krishnamurthy and C. E. Wills, "On the leakage of personally identifiable information via online social networks," *Comput. Commun.Rev.*, vol. 40, no. 1, pp. 112–117, 2010.
- [4]. E. Steel and G.Fowler.(2010). Facebook in Privacy Breach [Online]. Available: <http://online.wsj.com/article/SB100014240527023047728045755584840752369%68.html>
- [5]. Foursquare Official Blog, New York, NY, USA. (2011). On Foursquare, Cheating, and Claiming Mayorships from your Couch [Online]. Available: <http://goo.gl/F1Yn5>
- [6]. G. Zhong, I. Goldberg, and U. Hengartner, "Louis, Lester, and Pierre: Three Protocols for Location Privacy," *Privacy Enhancing Technologies, LNCS 4776*, Springer, 2007, pp. 62–76.
- [7]. G. Ghinita et al., "Private Queries in Location-Based Services: Anonymizers Are Not Necessary," *Proc. SIGMOD*, ACM Press, 2008, pp. 121–132.
- [8]. M.L. Yiu et al., "SpaceTwist: Managing the Trade-Offs among Location Privacy, Query Performance, and Query Accuracy in Mobile Services," *Proc. Int'l Conf. Data Eng., IEEE CS Press*, 2008, pp. 366–375
- [9]. S. Mascetti et al., "Privacy in Geo-Social Networks: Proximity Notification with Untrusted Service Providers and Curious Buddies," *Very Large Databases J.*, 2011; www.springerlink.com/content/y6m385570364876j/.
- [10]. D. Freni et al., "Preserving Location and Absence Privacy in Geo-Social Networks," *Proc. Conf. Information and Knowledge Management*, ACM Press, 2010, pp. 309–318.