INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1671 - 1674
RECEIVED : 29.02.2017 PUBLISHED : 15.03.2017
March 15, 2017

# A METHOD TO PRESERVE USER PROFILE AND FUNCTIONALITYIN GEOSOCIAL NETWORKS

[1]P.Manikandan, [2]S.Venkatesan, [3]A.Tamilendhi, [4]Mr.S.Kumarasamy,
[1,2,3]UG Scholar, Dept Of IT, SKP Engineering College,
[4]Asst Prof, Dept Of IT, SKP Engineering College.

## ABSTRACT

Online Social Networks have become a significant source to store personal information. A recent addition to this space, geo-social networks (GSNs) such as Yelp or Foursquare, collects user locations, through check-ins performed by users at visited venues. Overtly, personal information allows GSN providers to offer a variety of applications, including personalized recommendations and targeted advertising, and venue owners to promote their business through spatio-temporal incentives. Without privacy people may be reluctant to use geo-social networks; without user information the provider unable to use applications and have no incentive to participate in geo-social networks.

**Keywords**: Profile, location centric profiles (LCP),Identity fake news, and Benaloh's Cryptosystem .

## 1. INTRODUCTION

In this paper, we introduce $PROFILE_R$, a framework for constructing location centric profiles (LCP), aggregates built over the profiles of users that have visited discrete locations (i.e., venues) and a set of co-located users. $PROFI_R$ endows users with strong privacy guarantees and providers with correctness assurances. In addition to a venue centric approach, we propose a decentralized solution for computing real time LCP snapshots over the profiles. The scope of this project is to protect user's personal information of geo-social network by social network provider with correctness, assurances and strong privacy guarantees. The verifier or social network provider will find user's location and verifies user's details which they have registered. If the user's location and details are valid the spotter (anonymizer) allows the user to proceed check-ins using geo-social network. The anonymizer cannot be able to access and modify the user details, because the anonymizer only can check whether the user details and requests are valid to publish in the network and accept the user requests. The anonymizer is the mediator to provide privacy and operates geo-social network correctly. The user details or personal information preserved based on encryption.

## 2. SYSTEM ANALYSIS

### 2.1 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

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1671 - 1674
RECEIVED : 29.02.2017 PUBLISHED : 15.03.2017
March 15, 2017

their businesses through spatio-temporal incentives, e.g., rewarding frequent customers through accumulated badges.

### .2.2PROPOSED 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'shomomorphic 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 bound to venues, but instead 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.

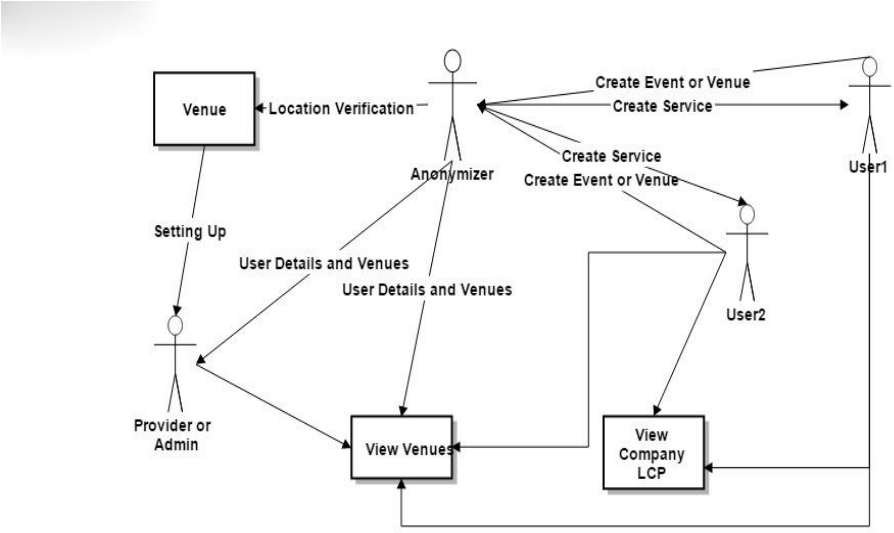


**Fig.1. Architecture Diagram**

## 3.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 input .

**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.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1671 - 1674
RECEIVED : 29.02.2017 PUBLISHED : 15.03.2017
March 15, 2017

**User Panel**

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

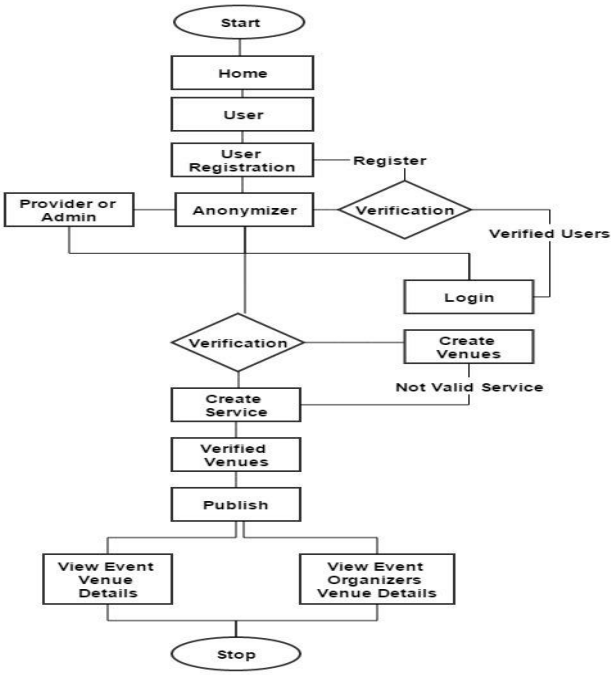


**Fig.2. Flow Chart**

**Admin Panel**

Admin or Provider will manage the user details in the network. The user detail after the acceptance of anonymizer it will send to the admin. But if the profile once accepted the users details no longer to be in the anonymizerpart.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. Admin have the entire responble of this system. Admin maintain the frequent updation and resolve the the user requirement and their issues in the system.

## 4. ALGORITHM DETAILS

**PROFIL$_R$**

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 functionsKey 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.**Key Generation**

## 5. LITERATURE SURVEY

### I.*Location-Related Privacy in Geo-Social Networks*

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

## CONCLUSION

In this paper we have proposed PROFILR, a framework and mechanism for privately and correctly.We have proved the ability of our solutions to satisfy the privacy and correctness requirements.We have shown that PROFILR is efficient , even when executed on resource constrained all domains.

## REFRENCES

[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/SB10001424052702304772804575584840752369%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.