PROVIDING PRIVACY IN GEOSOCIAL NETWORKS

Priyanka.N[1]*

[1]**Computer Science and Engineering IFET College of Engineering Villupuram.*
Email: priyankanatarajan222@gmail.com

*Corresponding Author: -
Email ID - priyankanatarajan222@gmail.com

Abstract: -
Social Network providers concentrate more on profit. Users reveal their personal information and make themselves into trouble. So a framework is proposed to face the conflict between the privacy and profit. The framework that consists of Location Profiles and a venue centric profiles and decentralized approach is provided for strong privacy and also implemented in android.

Keywords—*location; social networks;*

I. INTRODUCTION

Social networks have become a significant source of personal information. Their users voluntarily reveal a wealth of personal data, including age, gender, contact information, preferences and status updates. Social Networks even sell [1] information to third parties. There exists therefore a conflict without privacy [11] people may be reluctant to use geosocial networks; without user information the provider and venues cannot support applications and have no incentive to participate. To address this problem we propose a framework with location profiles [6] that first fix the user location and the set of co-located users. A framework that allows the construction of LCPs based on the profiles of present users, while ensuring the privacy [7],[9] and correctness of participants For better implementation it is implemented in android because android phones are the fastest selling phones and easy for users to use.

II. REALATED WORK

Social Networks collect fine grained location information, through check-ins [2] 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 businesses through spatio-temporal incentives [8] e.g., rewarding frequent customers through accumulated badges.

 Users are encouraged to requested to report their location through a check-in. The user retrieves the GPS coordinates, report to the server and android implementation display the nearby venues the user is checking.

 To use the application the user needs to download and install the application. And then the user needs to register him to the framework to search for places

III. DRAWBACKS OF EXISTING SYSTEM

Users provide their personal information that exposes users to risk. Because Social Network providers may sell the information to others. This is the drawback in the existing system.

IV. ADVANTAGES OF PROPOSED SYSTEM

The main advantage is that the applications have been developed in android platform and so it is easy to use. More privacy is achieved through building the real time statistics over the profiles.

V. ARCHITECTURE OF PROVIDING
PRIVACY IN GEOSOCIAL NETWORKS
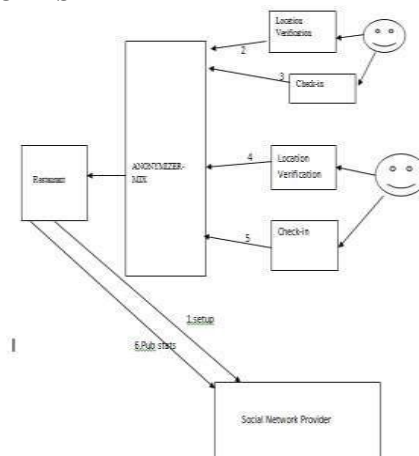
Fig. 1. System Architecture

Geosocial Network provider are the social networks that incorporates the Geographical information.[10] Anonymizer – Mix [3]-[5] is used to determine which input element corresponds to which output element.

VI. METHODOLOGY

When the user wants to check the next nearby location. He has to first register the current location .The admin is the person one who decide whether he is a valid user or not. If he is a valid user he can view the location.

 If he is not a valid user he cannot view the details. He can only see the contents in the encrypted form. If the user is moving from the current location to other. In such case, though he may be a valid user he has to get permission from admin to view the location in this framework.

VII. WORKING MODULE

 In this framework, there are three modules namely Admin, User and Android Test Book. In User module there can be n number of users. The users can search for nearby places such as reataurant, pubs, temples. The user should enter key word and search, it will display all related contents with their tags such as area name, name of place, distance and Google view. In Admin, the admin have two main works to give permission and to add places. Here all register users are stored with the details such as user ID, user name, E mail ID, mobile no, register date, DL id and permission. The admin will give

access permission to particular user. If the access permission is yes, then only user can view restaurants, view pubs, view temples and railway stations.

The admin can add n-number of restaurants. If the admin want to add a new restaurants, then admin will enter a place name, restaurants name, specialize for, description, distance from specified place, latitude and longitude domain, then submit and that data will stored in data base.

The next module describe about the implementation of android. Before using this application user should register, after registration he should login by using authorized user name and password. After login successful he will do some operations such as search restaurant, send user details, search key word, view connectivity and logout.

VIII.   CONCLUSION

By using this Framework, Privacy is preserved, and it is very easy to use because of android implementation. It is also efficient on resource constraint mobile devices.

IX. REFERENCES

[1].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.

[2].B. Carbunar and R. Potharaju, "You unlocked the Mt. Everest badge on foursquare! countering location fraud in geosocial networks," in *Proc. 9th IEEE Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Feb. 2012, pp. 182–190.

[3].D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[4].M. Abe, "Universally verifiable mix-net with verification work indendent of the number of mixservers," in *Proc. EUROCRYPT*, 1998, pp. 437–447.

[5]. R. Dingledine, N. Mathewson, and P. F. Syverson, "Tor: The secondgeneration onion router," in *Proc. USENIX Security Symp.*, 2004, pp. 303–320.

[6].B. Carbunar, M. Rahman, J. Ballesteros, and N. Rishe, "Private location centric profiles for geosocial networks," in *Proc. 20th ACM SIGSPATIAL Int. Conf. Adv. Geograph. Inf. Syst. (GIS)*, 2012, pp. 458– 461.

[7].M. Rahman, J. Ballesteros, B. Carbunar, N. Rishe, and A. V. Vasilakos, "Toward preserving privacy and functionality in geosocial networks," in *Proc. 18th Int. Conf. Mobile Comput. Netw.*, 2013, pp. 1–3.

[8].M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. MobiSys*, 2003, pp. 31–42.

[9].K. P. N. Puttaswamy and B. Y. Zhao, "Preserving privacy in locationbased mobile social applications," in *Proc. 11th Workshop Mobile Comput. Syst. Appl.*, New York, NY, USA, 2010, pp. 1–6.

[10]. S. Mascetti, D. Freni, C. Bettini, X. Sean Wang, and S. Jajodia, "Privacy in geo-social networks: Proximity notification with untrusted service providers and curious buddies," *VLDB J.*, vol. 20, no. 4, pp. 541–566, Aug. 2011.

[11]. D. Freni, C. Ruiz Vicente, S. Mascetti, C. Bettini, and C. S. Jensen, "Preserving location and absence privacy in geosocial networks," in *Proc. 19th ACM CIKM*, New York, NY, USA, 2010, pp. 309–318.