International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume3, Issue 4 (April '2017)

A TECHNIQUE TO CONSERVE LOCATION CENTRIC IN GEOSOCIAL NETWORKS

Dr .C.K.Gomathy,
Assistant Professor,
Department of Computer Science Engineering,
SCSVMV University,
India.

V.Geetha,
Assistant Professor,
Department of Computer Science Engineering,
SCSVMV University,
India.

T.Jayanthi,
Assistant Professor,
Department of Computer Science Engineering,
SCSVMV University,
India.

P.Charan,
UG Scholar,
Department of Computer Science Engineering,
SCSVMV University,
India.

P.U.Kirtthikaa,
UG Scholar,
Department of Computer Science Engineering,
SCSVMV University,
India.

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 businessthrough 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 geosocial networks. In this paper, here PROFILER, 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 is introduced. PROFIR endows users with strong privacy guarantees and providers with correctness assurances. In addition to a venue centric approach, in thisa proposeddecentralized solution for computing real time LCP snapshots over the profiles is implemented.

Keyterms: Geo Social networks, PROFILER, Location Centric Profile(LCP),Admin,Anonymizer.

I. INTRODUCTION

A FEW decades ago, location-based services (LBS) were used in military only. Today, thanks to advances in information and communication technologies, more kinds of LBS have appeared, and they are very useful for not only organizations but also individuals. Let us take the spatial range query, one kind of LBS that we will focus in this paper, as an example. Spatial range query is a widely used LBS, which allows a user to find points of interest (POIs) within a given distance to his/her location, i.e., the query point. As illustrated with this kind of LBS, a user could obtain the records of all restaurants within walking distance (say 500 m). Then, the user can go through these records to find a desirable restaurant considering price and reviews. While LBS are popular and vital, most of these services today including spatial range query require users to submit their locations, which raises serious concerns about the leaking and misusing of user location data. For example, criminals may utilize the data to track potential victims and predict their location.

II. RELATED 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 spatiotemporal incentives, e.g., rewarding frequent customers through accumulated badges.

Geo-social Networking is a type of social networking in which geographic services and capabilities such as geo-coding and geo tagging are used to enable additional social dynamics. User-submitted location data or geo-location techniques can allow social networks to connect and coordinate users with local people or events that match their interests.

Under the outsourced LBS system model, our design goal is to develop an efficient, accurate, and secure solution for

privacy-preserving spatial range query. Specifically, the following three objectives should be achieved.

1) Efficiency. As discussed in Section I, spatial range query has stringent performance requirements. A good solution should not consume many resources of mobile LBS users, and the POIsearchlatencyshouldbeacceptablefor online query.

2) Accuracy. It is desirable that a query result contains the exact records matching the query. False negatives would hurt user experience, while false positives would increase communication cost. Additional computational cost is also required at the user side to filter out false positives.

3) Security. The proposed solution should be resilient to ciphertext-only attacks and known-sample attacks. An accurate and efficient solution for spatial range query already exists, which is resilient to ciphertext-only attacks but not to known-sample attacks and more powerful attacks. The proposed solution should be more secure.

LBS users have the information of their own locations, and query the encrypted records of nearby POIs in the cloud. Cryptographic or privacy-enhancing techniques are usually utilized to hide the location information in the queries sent to the cloud. To decrypt the encrypted records received from the cloud, LBS users need to obtain the decryption key from the LBS provider in advance.

III.METHODOLOGIES

In this , a venue centric PROFILR that relieves the GSN provider from involvement in venue specific activities. To achieve this, PROFILR 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 PROFILR extension, built around the notion of snapshot LCPs. The distributed PROFILR 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 neighbours at any locations of interest. The communications in both PROFILR implementations are performed over ad hoc wireless connections.

MODULES:

After careful analysis the system has been identified to have the following modules:

- Registration panel.
- Anonymizer panel.
- User panel.
- Admin panel**.**

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

Anonymizer having following functionality

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.

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 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.

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 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.

IV.SYSTEMARCHITECTURE.

This system impolemented to protect user's personal information of Geo-social networkby the social network provider with correctness, assurances and strong privacy guarantees.The verifier or social network provider will find the user's location and verifies user's detailswhich 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 anonymizercannot 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.

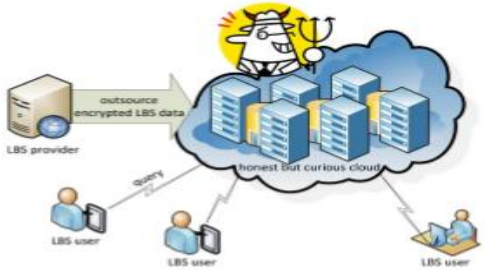


Figure1: System Model For Out Sourced Lbs Under Consideration

V.ALGORITHM DESCRIPTION

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 precede encryption.
It contains following functions

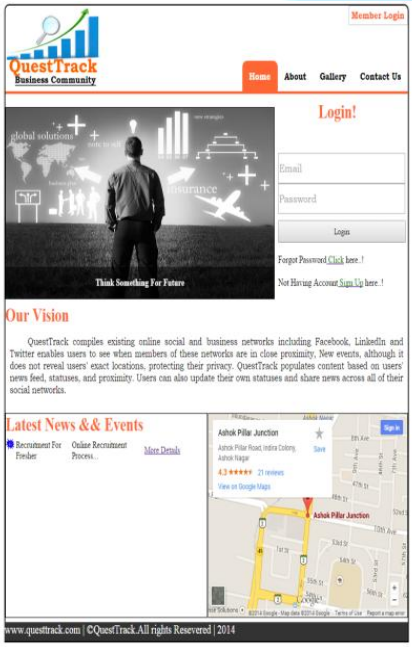
- Key Generation,
- Encryption,
- Decryption.

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**.**

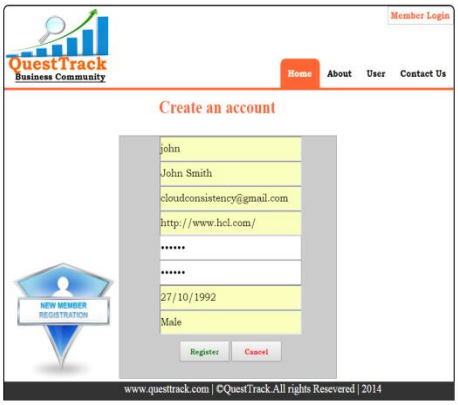
VI. RESULTS

The paper concerns with 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 geosocial networks. In this paper, we introduce PROFILER, 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. PROFIR 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.

HOME PAGE



ACCOUNT CREATION
Here new user creates his account by entering his information.



ANONYMIZER
Anonymizer accepts the user requests and venue requests and builds a service for user venues.

PROVIDER
Provider or Admin oversee all the user accounts and venues that are created and hosted in his website.

The future enhancement such as a particular criteria can be fixed for the user. In order to make the user as a permanent user. Additional security features can also be implemented.

VII.CONCLUSION

In this paper,the aim 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 allow check-ins using geo-social network. The anonymizer is the mediator to provide privacy and operates geo-social network correctly. The user details or personal information preserved based on encryption.

The anonymizer unable 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. Hence, the user personal information preserved.

X.REFERENCES

[1]. Lichun Li, Rongxing Lu, Senior Member, IEEE, and Cheng HuangEPLQ: Efficient Privacy-Preserving Location-Based Query Over Outsourced Encrypted DataIEEE INTERNET OF THINGS JOURNAL, VOL. 3, NO. 2, APRIL 2016.

[2]. Gomathy, C.K. and S. Rajalakshmi, 2014. A business intelligence network design for service oriented architecture. Int. J. Eng. Trends Technol., 9: 151-154.

[3]. W.K.Wong , D.W. Cheung, B.Kao and N.Mamoulis ,"Secure kNN computation on encrypted DATA bases ," 2009.

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

[5]. X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, "Practical k nearest neighbor queries with location privacy,"inICDE. IEEE,2014.