Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Semantic Web Significant Privacy Using In Geosocial Networks by Zero Knowledge

K Sreenivasulu Reddy*, D. Bullarao, P. Nageswara Rao
Departmentof CSE, SITS JNTUA
Andhra Pradesh, India

Abstract— Real report is the main participation costs of bringing to market for geo social network providers. Its Dependency on user profiles, built from a wealth of intentionally revealed personal information, exposes users to a variety of privacy vulnerabilities. Online graphical social networks have become a significant source of personal information In this paper, propose to take first steps toward connecting the conflict between Reality and privacy in geo social networks.

This paper introduce , a framework for constructing location centric profiles (LCPs), aggregates built over the profiles of users that have visited discrete locations . Preserve endows users with strong privacy guarantees and user with correctness assurances. In addition to a venue centric approach, we propose a decentralized solution for computing real time LCP snapshots over the profiles of co-located users. An Android or windows implementation shows that Preserving is efficient; the end-to-end overhead is small even under strong privacy and correctness assurances.

Keywords— Social implications of technology, technology social factors, privacy, mobile device.

I. INTRODUCTION

The exponential growth of Information Technology (IT) in Africa has led to an increase in data transaction across Africa's communication networks, with 110 million Internet users and 500 million mobile phone subscriptions as of 2010[1]. higher education institutions routinely post student admission and graduation data online and grant access to student records online [2]. The Electoral Commission posted the national voter's register online [3][4]. 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. GeoSNs currently offer different types of services, including photo sharing, friend tracking, and "check-ins." However, this ability to reveal users' locations causes new privacy threats, which in turn call for new privacy-protection methods. The authors study four privacy aspects central to these social networks - location, absence, co-location, and identity privacy - and describe possible means of protecting privacy in these circumstances.Geo location on web-based social network services can be IP-based or use hotspot trilateration. For mobile social networks, texted location information or mobile phone tracking can enable location-based services to enrich social networking.Geo-social networks (GeoSNs) provide context-aware services that help associate location with users and content. Location planning or social-mapping, users are able to search and browse nearby stores, restaurants, etc. Users' venues are assigned profiles and users can rate them, share their opinions and post pictures. These networks use the location of mobile phones to connect users and may also provide directions to and from the venue by linking to a GPS service.[9] In our everyday lives, we may have hundreds of activities, which form meaningful sequences that shape our lives. In this paper, we use the word activity to specifically refer to the actions taken in the order of seconds, such as “sitting”, “walking”, or “typing”, while we use the phrase life style to refer to higher-level abstractions of daily lives, such as “office work” or “shopping”. For instance, the “shopping” life style mostly consists of the “walking” activity, but may also contain the “standing” or the “sitting” activitiesTo model daily lives properly, we draw an analogy between people’s daily lives and documents, as shown in Figure 1..

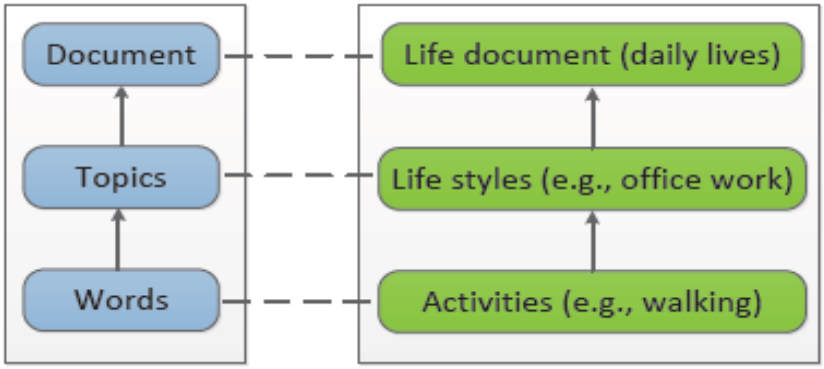


Fig.1Anology between word document.

In this paper, we proposed addressing the location conflict. Our approach is based on the concept of location centric profiles (LCPs). LCPs are statistics built from the profiles of (i) users that have visited a certain location or (ii) a set of co-located users.Contributions. We introduce Preserving framework that allows the construction of LCPs based on the profiles of present users, while ensuring the privacy and correctness of participants. Informally, we define privacy as the inability of venues and the GSN provider to accurately learn user information, including even anonymized location trace profiles. Verifying the correctness of user data is necessary to compensate for this privacy constraint: users may cheat and bias LCPs anonymously. We consider two user correctness components. First, location correctness, where users should only contribute to LCPs of venues where they are located. This requirement is imposed by the recent surge of fake checkins [5], motivated by their use of financial incentives. Second, LCP correctness, where users should be able to modify LCPs only in a predefined manner.

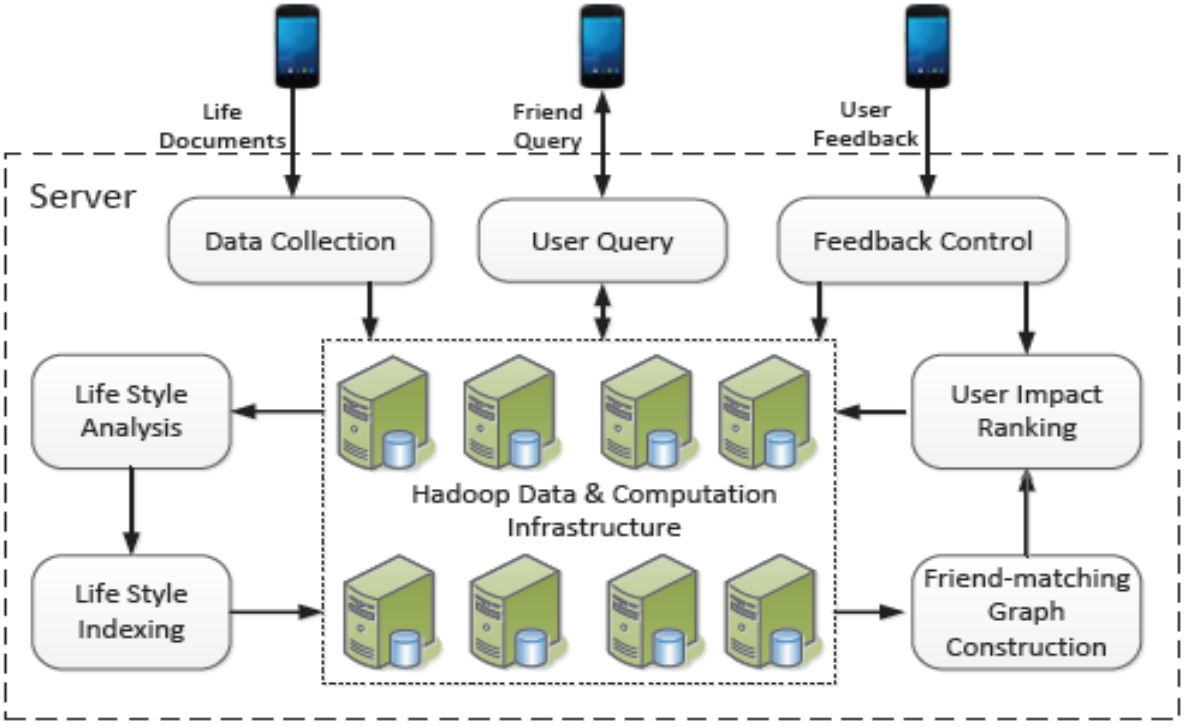


Fig.2: Hadoop Data Storage Schema

On the client side, each smartphone can record data of its user, perform real-time activity recognition and report the generated life documents to the servers. It is worth noting that an offline data collection and training phase is needed to build an appropriate activity classifier for real-time activity recognition on smartphones. We spent three months on collecting raw data of 8 volunteers for building a large training data set. As each user typically generates around 50MB of raw data each day, we choose MySQL as our low level data storage platform and Hadoop MapReduce as our computation infrastructure. After the activity classifier is built, it will be distributed to each user's smartphone and then activity recognition can be performed in real-time manner. As a user continually uses Friendbook, he/she will accumulate more and more activities in his/her life documents, based on which, we can discover his/her life styles using probabilistic topic model.

On the server side, seven modules are designed to fulfill the task of friend recommendation. The data collection module collects life documents from users' smartphones. The life styles of users are extracted by the life style analysis module with the probabilistic topic model. Then the life style indexing module puts the life styles of users into the database in the format of (life-style, user) instead of (user, life-style). A friend-matching graph can be constructed accordingly by the friend-matching graph construction module to represent the similarity relationship between users' life styles. The impacts of users are then calculated based on the friend-matching graph by the user impact ranking module. The user query module takes a user's query and sends a ranked list of potential friends to the user as response. The system also allows users to give feedback of the recommendation results which can be processed by the feedback control module. With this module, the accuracy of friend recommendation can be improved.

First, we propose a venue centric preserving, that relieves the GSN provider from a costly involvement in venue specific activities. To achieve this, Data stores and builds LCPs at venues. Furthermore, it relies on Benaloh's homomorphic cryptosystem and zero knowledge proofs to enable oblivious and provable correct LCP computations. We prove that Hadoop Data satisfies the introduced correctness and privacy properties.

Second, we propose a completely decentralized Privacy extension, built around the notion of snapshot LCPs. The distributed Privacy preserving 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 location of interest. Communications in both server &client implementations are performed over ad hoc wireless connections. Below shown System architecture of social networks using preserving location of users.

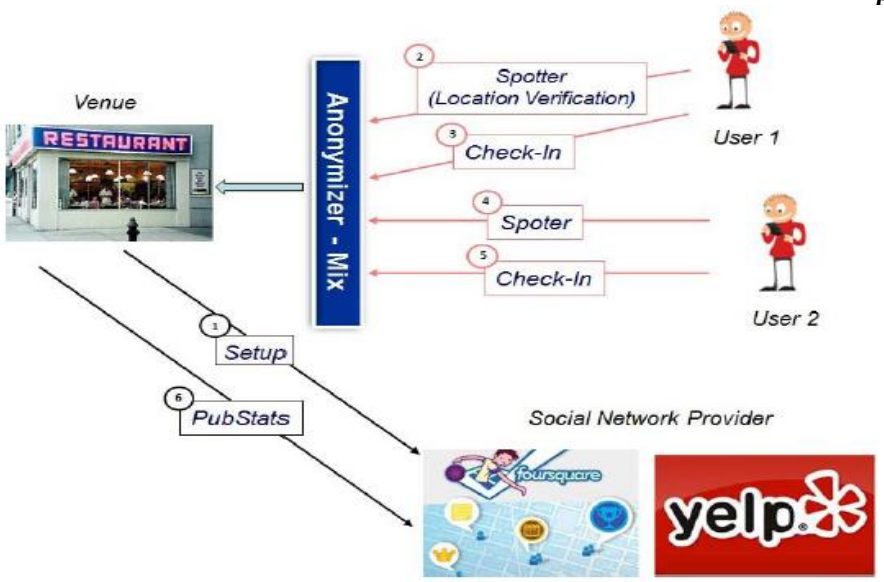


Fig 3. System Architecture Of Venue Centric process

i. Public Safety & News Media

Most criminal investigations and news events happen in a geographical location. Geo-social investigation tools provide the ability to source social media from multiple networks (such as Twitter, Flickr, and YouTube) without the use of hashtags or keyword searches. Some vendors provide subscription based services to source real-time and historical social media for events.

ii. Privacy policies

Some sites, like Facebook, have been scrutinized for allowing users to "tag" their friends via email while checking in "Check-in vs. Check-out"An "check-in" is a permission-based network that requires a user to join or sign up. The host is then given permission to access the user's information and to contact him or her. An "check-out" network is defaulted to have the user included in a group. Users must remove themselves from the network if they wish to not be included.

II. EXISTING SYSTEMS

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, e.g., rewarding frequent customers through accumulated badges.There exists therefore a conflict.

iii. DISADVANTAGES

- Providing personal information exposes however users to significant risks, as social networks have been shown to leak and even sell user data to third parties
- Without privacy people may be reluctant to use geosocial networks.
- without user information the provider and venues cannot support applications and have no incentive to participate.

III. PROPOSED SYSTEMS

This paper introduce a WEBlocation, a framework that allows the construction of LCPs based on the profiles of present users, while ensuring the privacy and correctness of participants. First, we propose a venue centric web, that relieves the GSN provider from a costly involvement in venue specific activities. To achieve this, web stores and builds LCPs at venues. Furthermore, it relies on Benaloh's homomorphic cryptosystem and zero knowledge proofs to enable oblivious and provable correct LCP computations.

Second, this paper propose a completely decentralized web extension, built around the notion of snapshot LCPs. The distributed web sematic 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 location of interest. Communications in both web significant implementations are performed over ad hoc wireless connections.

iv. ADVANTAGES

- Introduce the problem of computing location centric profiles (LCPs) while simultaneously ensuring the privacy and correctness of participants.
- Propose semantic web, a framework for computing LCPs. Devise both a venue centric and a decentralized solution. Prove that weblocation satisfies the proposed privacy and correctness properties.
- Provide two applications for semantic web location: (i) privacy preserving, personalized public safety recommendations and (ii) privately building real time statistics over the profiles of venue patrons with Yelp accounts.

- Evaluate weblocation through an Android implementation. Show that weblocation is efficient even when deployed on previous generation smart phones.

IV. EXPERIMENTAL BAG ROUND:

A. Venue Centric Process

This paper describes the user process based on the geosocial networks .In that time its identify the compute the present users and collocated users related present users.Venue centric semantic web, that relieves the GSN provider from a costly involvement in venue specific activities. To achieve this, web stores and builds LCPs at venues. Furthermore, it relies on Benaloh's homomorphic cryptosystem and zero knowledge proofs to enable oblivious and provable correct LCP computations. This paper prove that weblocation satisfies the introduced correctness and privacy properties. This paper use one of the protocols proposed in to verify the location claims of users checking-in. We assume venue owners are malicious and will attempt to learn private information from their patrons.In that time need the security for the geo-social networks applications.

A core functionality is supported by the most influential geosocial network (GSN) providers, APP [1]and Foursquare [2]. This functionality is simple and general enough to be applicable to most other GSNs (e.g., Facebook Places, Google Latitude). In this model, a provider S hosts the system, along with information about registered venues, and serving a number of users. To use the provider's services, a client application, the "client", needs to be downloaded and installed. Users register and receive initial service credentials, including a unique user id. The provider supports a set of businesses or venues, with an associated geographic location (e.g., restaurants, yoga classes, towing companies, etc). Users are encouraged to report their location, through check-ins at venues where they are present. During a check-in operation, performed upon an explicit user action, the user's device retrieves its GPS coordinates, reports them to the server, who then returns a list of nearby venues. The device displays the venues and the user needs to choose one as her current check-in location.

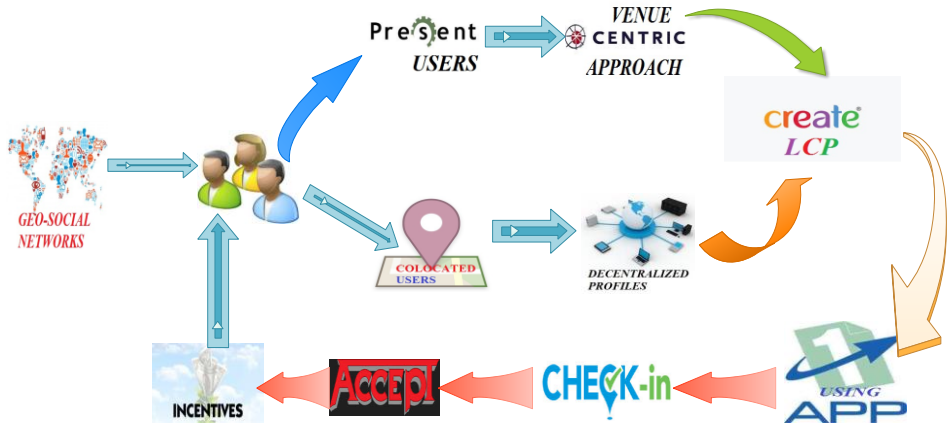


Fig 4 Semantic web check In user App

Each user has a profile PU = {pU1, pU2 , .., pUd}, consistingof values on d dimensions (e.g., age, gender, home city, etc).Each dimension has a range, or a set of possible values. Given a set of users U at location L, the location centric profile at L, denoted by LCP(L) is the set {LCP1, LCP2, .., LCPd }, where LCPi denotes the aggregate statistics over the i –th dimension of profiles of users from U. The intuition behind location privacy (i.e., the first privacy notion given in Section 1) is that users perceive their location as private information. However, they may tolerate that some location information is disclosed if it is sufficiently unlikely that the adversary discovers [4] their precise location. To achieve this result, techniques based on different ideas have been proposed. One idea is to send requests from fake locations together with the request from the real user's location (e.g., [15]). The main problem with the techniques implementing this idea is that a large number of fake request is necessary in order to guarantee privacy protection, while the system costs grow linearly in the number of fake requests. Another solution consists in sending a request (e.g.,a K-NN query) from a fake location and incrementally retrieve results (e.g., NN resources) from the SP until the client can reconstruct the result to the query centered in the real user's location [28]. Privacy is guaranteed because the SP can only discover that the user is located within a region without learning the exact location. The distance between the real user's location and the fake location used in the request determines a trade-o between privacy and performance. Indeed, if the distance is large, the size of region discovered by the SP is also large, but this results in high system costs. These techniques have been applied mostly for LBS performing k-NN spatial queries, and do not apply to proximity detection. A third family of techniques to enforce location privacy is based on the idea of enlarging the user's precise location before it is sent to the SP to a generalized region in order to decrease its sensitivity (among others, [18,25,8]). Some of these techniques are specially designed for proximity services. The main technical problem is how to process spatial queries in which the parameters are generalized regions instead of exact locations. On the other hand, the advantage is that the generalized region can be specifie as a user preference before any information is sent by the client. Indeed, this is the solution we adopt in this paper to protect a user's privacy with respect to her buddies. We actually prove that when a user specifies a generalized region, her buddies do not acquire any location information about that user, except the fact that she is inside the generalized region.

Algorithm Computing users' machingimpact ranking
Input: The user-matching Data k check In.
Output:Impact Check Out r for all users.
1:for i=1 to n do
2: r0(i)=1/n
3: end for
4:$\delta = \propto$
5: $\epsilon = \epsilon^{-9}$
6: while $\lambda > \epsilon \ do$
7: for I = 1 to n do
$r_{k+1}(i) = \sum_j \frac{1-\varphi}{n} rk(j) + \varphi \sum_j \frac{w(i,j).rk(j)}{\sum_j w(i,j)}$
8:
9: end for
$\lambda = \sum_1^n rk + 1(i) - rk(i)$
10:
11: end while

B.The Decentralization service setting

A Decentralization service allows its users to publish a resource (e.g., a picture, a text message, a check-in) tagged with the current location and time, as well as a set of users related to the resource. A resource is either tagged automatically (e.g. an integrated GPS can provide location and time), or tagged manually. Since resources and their tags become available to other users as well as to service providers, we are concerned with the privacy violations that the publication can lead to. Formally, a resource r is a tuple:

{Udata; STdata; Contenti}

where the first two elements are meta-data tags with r. U data being a set of identifiers of users, r.STdata being a spatio temporal tag and r.Content being the resource itself. In the following, when referring to a resource r, we also denote with r:Sdata and r:Tdata the spatial and temporal components, respectively, of r:STdata. We assume that all the users in r:Udata are in the location r:Sdata at the time r:Tdata. As an example, recall the user Charlie performing a sta- tus update informing his friends about his presence in the pub together with Alice and Bob. In our formalization, the update is a resource with Alice, Bob, and Charlie as r:Udata, and the location of the pub with the current timeas r:STdata.

We consider techniques for privacy preservation based on the generalization of resources before publication. In partic ular, we consider generalization functions that generalize the spatio-temporal tag of a resource. Formally, STdata for an original resource is a point in the spatio-temporal domain, while STdata for a generalized resource is a 3D volume in the spatio-temporal domain that contains the point of the corresponding original resource.3 In case of generalized resources r0, we denote by r0:Tmax and r0:Tmin the maximum and minimum time instant of r0 Tdata, respectively.

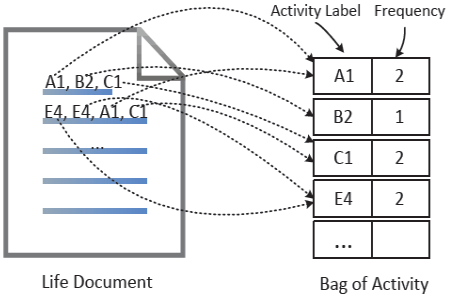


Fig 5 Life Style documents of users

C. Private LCP Requirements

Let k be a security parameter, denoting the level of privacy we need to provide for users at any location. We then define a private LCP solution to be a set of functions,

PP(k) = {Setup, Spotter, Check In, PubStats},

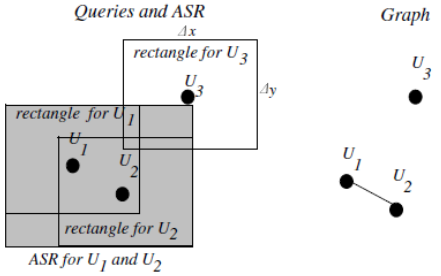


Fig.6 Setup is run by each venue where ASR graph

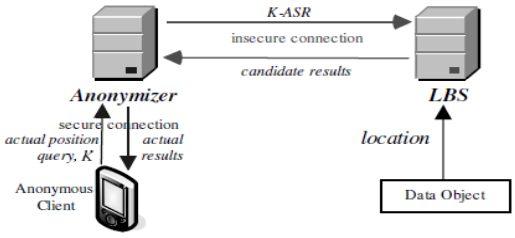
user statistics are collected, to generate parameters for user check-ins. To perform a checkin, a user first runs Spotter, to prove her physical presence at the venue. Spotter returns error if the verification fails, success otherwise. If Spotter is successful, Check In is run between the user and the venue, and allows the collection of profile information from the user. Specifically, if the user's profile value v on dimension D falls within the range Ri , the counter ci is incremented by 1. Finally, PubStats publishes collected LCPs. In the following, we use the notation Prot (P1(args1), .., Pn(argsn)) to denote protocol Prot run between participants P1, .., Pn, each with its own arguments. Let CV be the set of counters defined at a venue V. We use .CV to denote the set of sets derived from CV as follows. Each set in .C V differs from CV in exactly one counter, whose value increments the value of the corresponding counter in CV . For instance, if CV = {2, 5, 9}, then .C V ={{3, 5, 9}, {2, 6, 9}, {2, 5, 10}}. A private LCP solution needs to satisfy the following properties:

k-Privacy: Let A denote an adversary that controls any number of venues and let C denote a challenger controlling k users. C runs Spotter followed by Check In at a venue V controlled by A on behalf of i < k users. Let Ci denote the resulting counter set. For each j = 1..b, A outputs c[j] its guess of the value of the j -th counter of Ci . The advantage of A, Adv(A) = |Pr[Ci [j] = c[j] − 1/(i + 1)|, defined for each j = 1..b, is negligible.

Location Correctness: Let A denote an adversary that controls the GSN provider and any number of users. Let C be a challenger that controls a venue V . A running as a user U not present at V , has negligible probability to successfully complete Spotter at V .

LCP Correctness: Let A denote an adversary that controls the GSN provider and any number of users. Let C be a challenger that controls a venue V. Let CV denote the set of counters at V before A runs Check In at V and let C V be the set of counters afterward. If C V /∈ .CV , the Check In completes successfully with only negligible probability.

K-anonymity [25], [27] has been used for publishing microdata,such as census, medical and voting registration data. A dataset is said to be K-anonymized, if each record is indistinguishable from at least K-1 other records with respect to certain identifying attributes. In the context of location based services, the Kanonymity concept translates as follows: given a query, guarantee that an attack based on the query location cannot identify the query source with probability larger than 1/K, among other K-1 users.



(a) General framework

Fig 7 General frame work of K Anonmity

Most of the existing work adopts the framework of Figure 1a. In this framework, a user sends his location and query to the anonymizer through a secure connection. The anonymizer removes the id of the user and transforms his location through a technique called cloaking. Cloaking hides the actual location by a K-anonymizing spatial region (K-ASR or ASR), which is an area that encloses the client that issued the query, as well as at least K-1 other users. The anonymizer then sends the ASR to the LBS,which returns to the anonymizer a set of candidate results that satisfy the query condition for any possible point in the ASR.

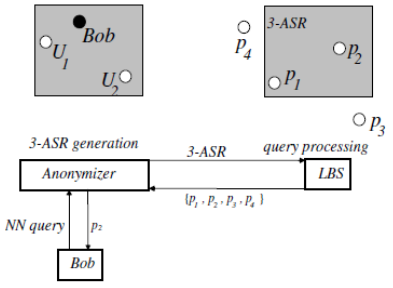
Algorithm:Anonymization algorithm

Input: T1, T2 a k-privacy requorement, a taxonomy tree for each categorical attribute in xn.

Output:a generalized T2 satiisfying the privacy require ment.

1. Generalize entry value of Ai to ANYwhere Ai€Xi
2. While there is a valid candidate in Ucut, do
3. Find the paire of near root (xi)from Úcut.
4. Specialized or on t2 and remove Xifrom Úcut.
5. Replace new (xi) and the valid status of xi for all in Úcut.
6. Out put the generalized T2 and Úcut.

User Interface



(b) Example of NN query

Fig 8 Example of ASR NN Query K Anonymity

User use the applications for the incentive and some application implementation. in this process user search the application from the database.In that time user location stored into the database. Provide two applications for semantic location: (i) privacy preserving, personalized public safety recommendations and (ii) privately building real time statistics over the profiles of venue patrons with Yelp accounts. Evaluate location through an Android implementation. Show that weblocation is efficient even when deployed on previous generation smartphones.Users can verify the results of their queries, relying only on their trust of the data owner. In addition to assuming a different environment, web location does not assume venue owners to be trustworthy. Users have a profile that allows the private matching of relevant ads. While location can be used to privately provide location centric targeted ads, its main goal is different - to compute location (venue) centric profiles that preserve the privacy of contributing users.

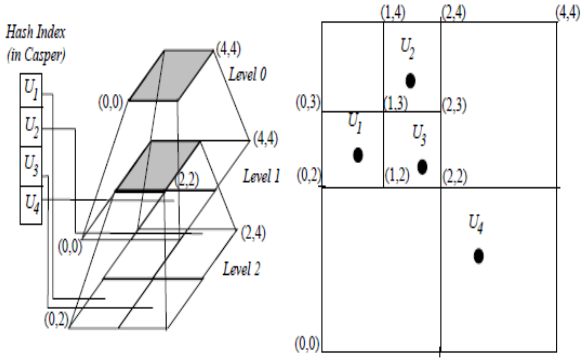


Fig 9 NN query K Anonymity Hash index

Check-in Process

When user use the application,In that time server check the lcp for the user correctness.This process perform with some actors like Setup, Spotter, Check In, PubStats.This paper use one of the protocols proposed in to verify the location claims of users checking-in. This method assume a honest challenger, who does not run Spotter and Check In twice for the same (user, epoch) pair. Otherwise, the use of the signed pseudonyms provides an advantage to some process. Note that if pseudonyms are not used, this requirement is not necessary. No identifying information is sent by users during the Spotter and Check In procedures. Users are encouraged to report their location, through check-ins at venues where they are present. During a check-in operation, performed upon an explicit user action, the user's device retrieves its GPS coordinates, reports them to the server, who then returns a list of nearby venues. The device displays the venues and the user needs to choose one as her current check-in location by

A zero-knowledge proof must satisfy three properties:

Completeness: if the statement is true, the checkIn (that is, one following the protocol properly) will be convinced of this fact by an correct user.

Soundness: if the statement is false, no check In user can convince the true verifier that it is true, except with some small probability.

Zero-knowledge: If the statement is true, no cheating user learns anything other than this fact.

V. EXPERIMENTAL EVALUATION

This section evaluates the proposed anonymization and query processing algorithms. We implemented prototypes for both the anonymizer and the LCP using JAVA. All experiments were executed on an Intel Xeon 2.8GHz machine with 2.5GB of RAM and Linux OS/windows 7. Our workload for user positions and landmarks/points of interest consists of the NA dataset [30], which contains 569K locations on the continent (Figure 16). Performance is measured in terms of CPU time, I/O time and communication cost. At the anonymizer we employed main memory structures, therefore we measured only the CPU time. At the LCP, we used an R*-Tree and measured the total time (i.e., I/O and CPU time); in all experiments we maintained a cache with size equal to 10% of the corresponding R*-Tree. The communication cost was measured in terms of number of candidates sent from the LCP back to the anonymizer.

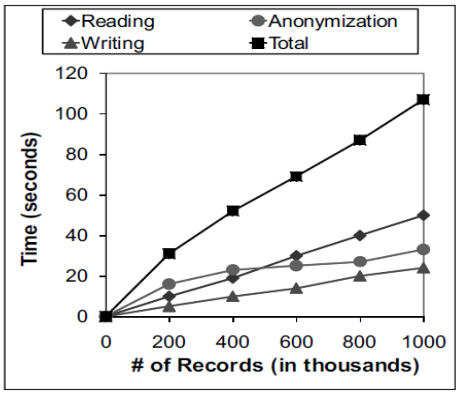


Fig 10 LCP Time measurement result

We propose to use PROFILR to build finer grained personalized safety recommendations, with privacy. PROFILR divides the safety index interval ([0, 1]) into sub-intervals, and associates a counter with each. PROFILR enables then a set of users to privately and correctly compute the distribution of their safety index values.

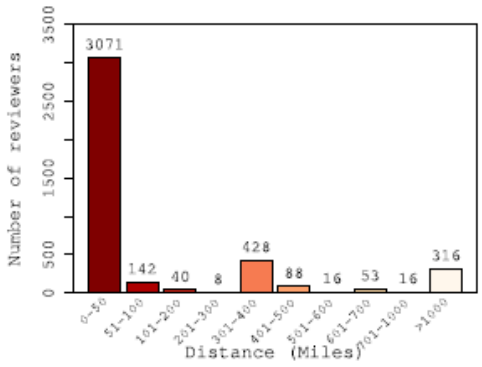


Fig 11 Histogram for LCP Measurement result

The computation overhead of Check In is TCI = bTRE + TZK, where TRE is the Benaloh re-encryption cost and TZK is the overhead of the ZK-CTR protocol. The formula does not consider the cost of modular multiplication, random number generation and random permutation operations, that are neglibile compared to the other costs. Given s, the number of rounds of ZK-CTR, TZK = 2sbTRE + sbTRE + s2 bTRE =72 sbTRE. The communication overhead is Tcom_CI = bN +Tcom_ZK. The communication cost of ZK-CTR, Tcom_ZK is s(2bN + 12 4bN + 122bN) = 5sbN.

VI. CONCLUSION

In this paper we have proposed semantic web , a framework and mechanisms for privately and correctly building location centric profiles. We have proved the ability of our solutions to satisfy the privacy and correctness requirements. We have introduced two applications for web location. We have shown that semantic web is efficient, even when executed on resource constrained mobile devices.

VII. FUTURE ENHANCEMENTS

There are some potential future directions of this work. In particular, besides the power-law distribution, it is promising to consider other methods for modeling the geographical mobility patterns of users. Moreover, it is also interesting to explore the performance of different combinations of geographic influence and social influence in addition to their product. An interesting direction for future work is to process Geo-Social queries based on the trajectories of the mobile users. The main challenge is how to calculate the geo-distance between users based on the history of the locations, not only the current locations.

REFERENCES

[1] Needleman, Rafe; Claire Cane Miller; Adrianne Jeffries (3 September 2010). "Reporters' Roundtable: Checking in with Facebook and Foursquare". CNET. Retrieved 8 October 2010.

[2] "Recommending Social Events from Mobile Phone Location Data", Daniele Quercia, et al., ICDM 2010 Facebook To Open Your Status Updates to Developers. Mashable.com (2009-04-26). Retrieved on 2012-01-09.

[3] Lampos V, Cristianini N (2010). "Tracking the flu pandemic by monitoring the Social Web". Cognitive Information Processing (CIP). pp. 411–416.

[4] Mobile Geo-Location Application Types. Socialtimes.com (2010-04-22). Retrieved on 2012-01-09. Apple's Working on a New Social Location App Called iGroups. The Next Web. Retrieved on 2012-01-09.

[5] Blog.twitter.com (2010-06-24). Retrieved on 2012-01-09. N. R. Adam and J. C. Wortmann, "Security-Control Methods for Statistical Databases: A Comparative Study," ACM Computing Surveys, vol. 21, no. 4, pp. 515–556, 1989.

[6] C. C. Aggarwal, "On k-Anonymity and the Curse of Dimensionality."in Proc. of VLDB, 2005, pp. 901–909. R. Agrawal and R. Srikant, "Privacy-Preserving Data Mining," in Proc.of SIGMOD, 2000, pp. 439–450. R. Bayardo and R. Agrawal, "Data Privacy through Optimal k-Anonymization." in Proc. of ICDE, 2005, pp. 217–228.

[7] N. Beckmann, H.-P. Kriegel, R. Schneider, and B. Seeger, "The R*-Tree:An Efficient and Robust Access Method for Points and Rectangles." In Proc. of SIGMOD, 1990, pp. 322–331.

[8] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing,"IEEE Pervasive Computing, vol. 2, no. 1, pp. 46–55, 2003.

[9] C. Bettini, X. S. Wang, and S. Jajodia, "Protecting Privacy Against Location-Based Personal Identification," in Proc. of VLDB Workshopon Secure Data Management (SDM), 2005, pp. 185–199.

[10] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, "Preserving User Location Privacy in Mobile Data Management Infrastructures." in Proc.of Privacy Enhancing Technologies, 2006, pp. 393–412.

[11] Algorithm for Anonymous Location-based Services," in Proc. of ACMGIS,2006, pp. 171–178.

[12] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIVE: Anonymous Location-based Queries in Distributed Mobile Systems." in Proc. ofWorld Wide Web Conf. (WWW), 2007, pp. 371–380.

[13] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "MOBIHIDE: A MobilePeer-to-Peer System for Anonymous Location-Based Queries." in Proc.of the Int. Symposium in Spatial and Temporal Databases (SSTD), 2007,pp. 221–238.

[14] G. Ghinita, P. Karras, P. Kalnis, and N. Mamoulis, "Fast Data Anonymization with Low Information Loss." in Proc. of VLDB, 2007.

[15] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking." in Proc. of USENIX MobiSys, 2003, pp. 31–42.

[16] B. Hoh and M. Gruteser, "Protecting Location Privacy Through Path Confusion," in Proc. of SecureComm, 2005, pp. 194–205.

[17] H. Hu and D. L. Lee, "Range Nearest-Neighbor Query," IEEE TKDE,vol. 18, no. 1, pp. 78–91, 2006.

[18] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," in Proc. of ICDCS, 2005,pp. 599–608.

[19] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan, "Incognito: EfficientFull-Domain K-Anonymity." In Proc. of SIGMOD, 2005, pp. 49–60.

ABOUT AUTHOR

[1] **K Sreenivasulu Reddy** pursuing MTech Department Of Computer Science in Sweetha Instute of Technology and science affiliated by JNTU Anantapurm, India. I worked in Computer networks in specialization of specific areas .I interested Data Mining , Database management system,,Mobile Computing , Data Structure an ad-hoc networks.

[2] **D Bulla Rao** MTech Completed in JNTU Kakinada presently working as a assistant professor in department of Computer Science and Engeenering he published more number of journals in research and development of the Data Mining , Database management system,,Mobile Computing , Data Structure and ad-hoc networks.

[3] **P Nageswara Rao** PhD., presently working as a Associate professor in department of Computer Science and engeenering he published more number of journals in research and development of the DataMining, Database management system,,Mobile Computing , Data Structure and ad-hoc networks.

