ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Towards Secure Privacy Preserving In Geographic Services in Social Network

Kadiyala Lakshmi Lahari
M.Tech (CSE) Student,
Department of Computer Science and Engineering,
Sri Vasavi Engineering College, Tadepalligudem.

M.R.Raja Ramesh
Associate Professor,
Department of Computer Science and Engineering,
Sri Vasavi Engineering College, Tadepalligudem.

Abstract:

Many of online social networking and mobile phone services has resulted in increased to geo-location attention to mobile social networking. In this paper, we implement and propose to take first steps toward addressing the conflict between profit and privacy in geosocial networks. We introduce geographic services and capabilities such as geocoding and geotagging are used to enable additional social dynamics, a framework for constructing location centric profiles (LCPs), it stores discrete locations to aggregates built over the profiles of users. Geo graphic capabilities endow users with strong privacy guarantees and providers with correctness assertion.

By using the profiles of collocated users In addition to a venue centric approach, we propose a decentralized solution for computing real time LCP snapshots over. We useHomomorphism Cryptosystems further define the re-encryption function to be Note that the re-encryption function can be invoked without knowledge of the message m. Furthermore, the encryption of the same plaintext, it is possible to show that two ciphertexts are without revealing the plaintext.

The above properties are ideal to enable a user to (i) without knowing the counter's value or the encryption key, we can increment the counter of a bucket even and (ii) to re-encrypt all counters without knowing the encryption key.An Android implementation shows that geosocial is efficient; the end-to-end overhead is small even under strong privacy and correctness assurances.

Keywords:
Social network, Geographic Services, Privacy, Geo Tagging, LCPs.

I. INTRODUCTION:

Geosocial networking (GeoSNs) 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. The proliferation of GeoSNs indicates that they're rapidly attracting users. [1] [2] 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 newprivacy 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 this paper, we take first steps towardaddressing this conflict. Our approach is based on theconcept of location centric profiles (LCPs). LCPs arestatistics built from the profiles of (i) users that havevisited a certain location or (ii) a set of co-locatedusers. We introduce PROFILR, a framework thatallows the construction of LCPs based on the profilesof present users, while ensuring the privacy andcorrectness of participants. Informally, we defineprivacy 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 check ins [5], motivated by their use of financial incentives. Second, LCP correctness, where users should be able to modify LCPs only in a predefined manner. First, we propose a venue centric PROFILR, that relieves the GSN provider from a costly involvement in venue specific activities. To achieve this, PROFILR stores and builds LCPs at venues. Furthermore, it relies on Benaloh'shomomorphic cryptosystem and zero knowledge proofs to enable oblivious and provable correct LCP computations.
We prove that PROFILR satisfies the introduced correctness and privacy properties. Second, we propose a completely 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 neighbors at any location of interest. Communications in both PROFILR implementations are performed over ad hoc wireless connections.

PUBLIC SAFETY & NEWS MEDIA:

Most criminal investigations and news events happen in a geographical location. Geo-social investigation tools provide the ability to source socialmedia 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.

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.

OBJECTIVE:

The scope of the project is Toward Preserving Privacy and Functionality in Geosocial Networks using the PROFILER method with two types like venue centric and Decentralized.

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.

DISADVANTAGES:

- Providing personal information exposes

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

however users to significant risks, as social networks havebeen 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.

PROPOSED SYSTEMS:

This paper introduce PROFILR, 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 PROFILR, that relieves the GSN provider from a costly involvement in venue specific activities. To achieve this, PROFILR stores and builds LCPs at venues. Furthermore, it relies on Benaloh'shomomorphic cryptosystem and zero knowledge proofs to enable oblivious and provable correct LCP computations. Second, this paper propose a completely 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 neighbors at any location of interest. Communications in both PROFILR implementations are performed over ad hoc wireless connections.

ADVANTAGES:

- Introduce the problem of computing location centric profiles (LCPs) while simultaneously ensuring the privacy and correctness of participants.
- Propose PROFILR, a framework for computing LCPs. Devise both a venue centric and a decentralized solution. Prove that PROFILR satisfies the proposed privacy and correctness properties.
- Provide two applications for PROFILR: (i) privacy preserving, personalized public safety recommendations and (ii) privately building real time statistics over the profiles of venue patrons with Yelp accounts.
- Evaluate PROFILR through an Android implementation. Show that PROFILR is efficient even when deployed on previous generation smart phones.

EXPERIMENTAL BAG ROUND:

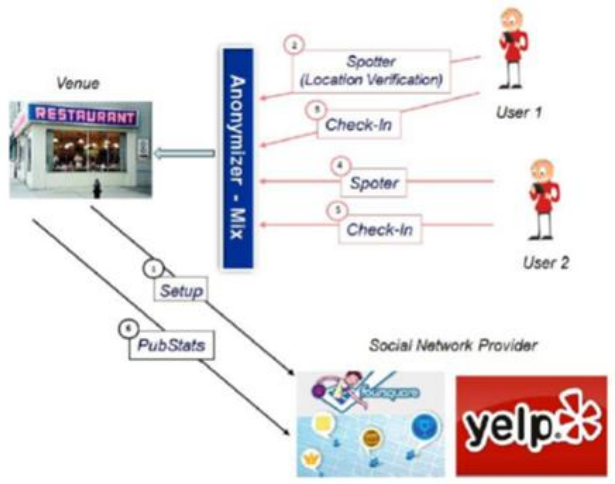
A core functionality is supported by the most influential geosocial network (GSN) providers, APP [1]and Foursquare [2]. This functionality is simple and general enough to be applicable to most other GSNs (e.g., Facebook Places, Google Latitude). In this model, a provider S hosts the system, along with 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 displaysthe venues and the user needs to choose one as her current check-in location.

System Design and Architecture:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



LOCATION CENTRIC PROFILE:

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 untilthe 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.

CkNN-Circ(D: the set of objects)
1. for every object p ∈ D do
2. if SL = ∅ then SL := {[0, 2π] → p}
3. else
4. for every interval ϕ ≡ [a, b] → q,ϕ∈ SL do
5. if ⊥pq∩ C= ∅ or ⊥pq is tangent to C then
6. if |pC| < |qC| then SL := (SL − ϕ) ∪ {[a, b] → p}
else break
7. else
8. let s0, s1 be two points such that ⊥pq∩ C= {s0, s1}
9. if ˆ s0 ∈ [a, b] and ˆ s1 ∈ [a, b] then
// Assume ˆ s0 < ˆ s1 (the other case is symmetric)
10. if |pCa| < |qCa| then SL := (SL − ϕ)∪
∪{[a, ˆ s0] → p, [ˆ s0, ˆ s1] → q, [ˆ s1, b] → p}
// Ca, C

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

b are the endpoints of arc [a, b]
11. else SL := (SL − ϕ)∪
∪{[a, ˆ s0] → q, [ˆ s0, ˆ s1] → p, [ˆ s1, b] → q}
12. else if ˆ s0 ∈ [a, b] or ˆ s1 ∈ [a, b] then
// Let only ˆ s0 ∈ [a, b] (ˆ s1 ∈ [a, b] is symmetric)
13. if |pCa| < |qCa| then SL := (SL − ϕ)∪
∪{[a, ˆ s0] → p, [ˆ s0, b] → q}
14. else SL := (SL − ϕ) ∪ {[a, ˆ s0] → q, [ˆ s0, b] → p}
15. else if |pCa| < |qCa| then
SL := (SL − ϕ) ∪ {[a, b] → p}
16. return SL
CkNN(D: the set of objects)
1. call CkNN-Circ(D)
2. return {p : p ∈ D ∧p is inside C}∪
∪{p : p belongs to a mapping of SL}

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 particular, 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.

B 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},

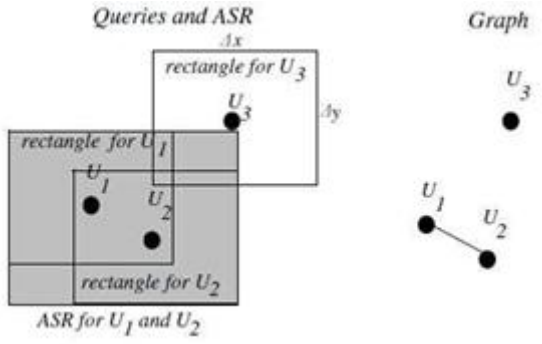


Fig.1 Setup is run by each venue whereuser statistics are collected, to generate parameters for user check-ins. To perform a checkin, a user first runs Spotter, to prove her physical presence at the venue. Spotter returns error if the verification fails, success otherwise. If Spotter is successful, Check 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.

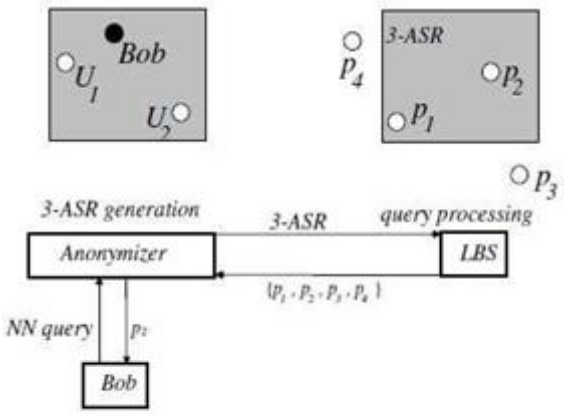
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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,

ALGORITHM:ANONYMIZATION ALGORITHM:
INPUT: T1, T2 a k-privacy requorement, a taxonomy tree for each categorical attribute in xn.
OUTPUT: a generalized T2 satisfying the privacy require ment.

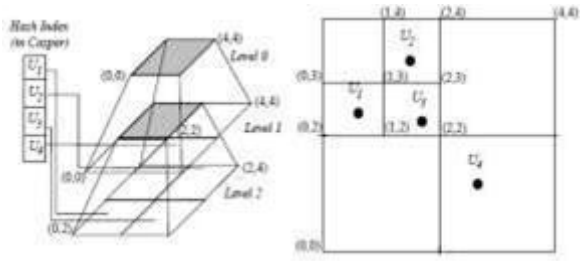
1. Generalize entry value of Ai to Anywhere Ai€Xi
2. While there is a valid candidate in ^{UU}ut, do
3. Find the paire of near root (xi)fromÚcut.
4. Specialized or on t2 and remove XifromÚcut.
5. Replace new (xi) and the valid status of xi for all in Úcut.
6. Out put the generalized T2 and Úcut.

User Interface



(b) Example of NN query

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 PROFILR: (i) privacy preserving, personalized public safety recommendations and (ii) privately building real time statistics over the profiles of venue patrons with Yelp accounts. Evaluate PROFILR through an Android implementation. Show that PROFILR is efficient even when deployed on previous generation smart phones. Users can verify the results of their queries, relying only on their trust of the data owner. In addition to assuming a different environment, PROFILR does not assume venue owners to be trustworthy. Users have a profile that allows the private matching of relevant ads. While PROFILR 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. By Method--Thompson et. al. approach, zero-knowledge process.



CHECK-IN PROCESS:

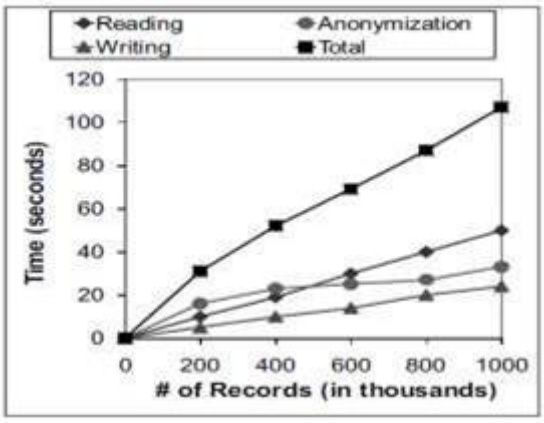
When user use the application,In that time server check the lcp for the user correctness.This process perform with some actors like Setup, Spotter, Check In, PubStats.This paper use one of the protocols proposed in to verify the location claims of users checking-in. This method assume a honest challenger, 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 Method—SPOTRV

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

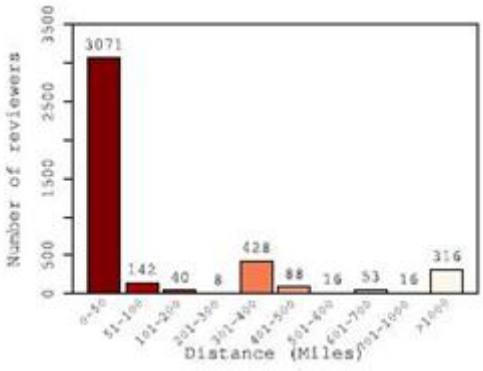
protocol, threshold secret sharing (TSS), Spotter protocol

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.



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 tprivately and correctly compute the distribution of their safety index values.



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.

IMPLEMENTATION:

MODULE:

- System Model
- PROFILR
- Spotter
- Location Correctness

MODULES DESCRIPTION:

System Model

- ✓ In this module, we introduce the problem of computing location centric profiles (LCPs) while simultaneously ensuring the privacy and correctnessof participants.
- ✓ We consider a core functionality that is supported by themost influential geo-social network (GSN) providers
- ✓ 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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 chooseone as her current check-in location.

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

PROFILR

- ✓ Propose PROFILR, a framework for computing LCPs. Devise both a venue centric and a decentralized solution.
- ✓ Prove that PROFILR satisfies the proposed privacy and correctness properties.
- ✓ In this section we propose a solution, that when used in conjunction with Sybil detection tools, mitigatesthis problem.
- ✓ No identifying information is sent by users during the Spotter and Check In procedures: the pseudonyms are blindly signed by S, all communication with S takes place over an anonymizer, and all communication with a venue is done usingrandomly chosen MAC and IP addresses.

Spotter

- ✓ Let L and T denote U's location and current time. To ensure anonymity, U generates fresh random MAC and IP addresses. These addresses are used for a single execution of the Spotter and Check In protocols. SPOTRV uses one of the location verification procedures proposed to verify U's presence at L and T.
- ✓ For simplicity of presentation, we have avoided the Sybil attack problem: participants that cheat through multiple accounts they control or by exploiting the anonymizer.

Location Correctness

- ✓ The user's location is verified in the Spotter protocol. A malicious user not present at venue V, is unable to establish a connection with the device deployed at V, SPOTRV .
- ✓ Thus, the user is unable to participate in the challenge/response protocol and receive at its completion a provider signed share of the Benaloh secret key. Without the share, the user is unable to initiate the Check In protocol.
- ✓ We use one of the protocols proposed to verify the location claims of users checking-in. For completeness, we now briefly describe this protocol. Let SPOTRV denote the device installed at venue V. When a user U expresses interest to check-in at venue V, SPOTRV initiatesa challenge/response protocol.

CONCLUSION &FUTURE ENHANCEMENTS:

In this paper we have proposed PROFILR, 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 PROFILR. We have shown that PROFILR is efficient, even when executed on resource constrained mobile devices. 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

REFERENCES:

[1] BogdanCarbunar, MahmudurRahman, Jaime Ballesteros, Naphtali Rishe, and Athanasios V. Vasilakos, PROFILR: Toward Preserving Privacy andFunctionality in Geosocial Networks, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014

[2] M Bharath, M Sreenivasulu Reddy & N Mahipal Reddy, A New System for Constructing Location Centric Profiles (LCPS)Of Users That Have Visited Discrete Locations in GeosocialNetworks That Guarantees Privacy, IJMETMR,www.ijmetmr.com, Volume 2 Issue 9 Page 1179-1186

[3] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, ―EnhancingSource-Location Privacy in Sensor Network Routing,‖ in Proc. of ICDCS, 2005,pp. 599–608.

[4] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan, ―Incognito:EfficientFull-Domain K-Anonymity.‖ in Proc. of SIGMOD,2005, pp. 49–60.

[5] A. Machanavajjhala, J. Gehrke, D.Kifer, and M.Venkitasubramaniam,―l-Diversity: Privacy Beyond k-Anonymity.‖ in Proc. of ICDE, 2006.

[6] A. Meyerson and R. Williams, ―On the Complexity ofOptimal Kanonymity,‖in Proc. of ACM PODS, 2004, pp.223–228.

[7] M. F. Mokbel,W. G. Aref, and I. Kamel, ―Analysis of Multi-DimensionalSpace-Filling Curves,‖ GeoInformatica, vol. 7,no. 3, pp. 179–209, 2003.

[8] M. F. Mokbel, C. Y. Chow, and W. G. Aref, ―The NewCasper: Query Processing for Location Services without Compromising Privacy,‖ inProc. of VLDB, 2006, pp. 763–774.

[9] B. Moon, H. Jagadish, and C. Faloutsos, ―Analysis of theClustering Properties of the Hilbert Space-Filling Curve,‖ IEEE TKDE, vol. 13, no. 1, pp. 124–141, 2001.

[10] L. Sweeney, ―k-Anonymity: A Model for ProtectingPrivacy,‖ Int. J. ofUncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 5,pp. 557–570, 2002.