OPTIMAL MEETING LOCATIONS

Snehal Borude , Vrushali Ranmalkar

[1] *Masters in Engineering, Computer Science Department, VACOE, Maharashtra, India*
[2] *PHD, Lecturer At Computer Science Department, VACOE, Maharashtra, India*

ABSTRACT

Equipped with state-of-the-art mobile and smart phones devices, today's highly interconnected urban population is increasingly dependent on these gadgets to organize and plan their daily lives. These applications often rely on preferred locations of individual users or a group of users to provide the desired service, which jeopardizes their privacy; users do not necessarily want to reveal their current locations to the service provider or to any other, possibly untrusted users. In this paper, we propose privacy- preserving algorithms for finding optimal meeting locations for a group of users. In order to study the performance of our algorithms in a real deployment, we test and implement their execution efficiency on Nokia smart phones. By means of a targeted user-study, we attempt to get an insight into the privacy awareness of users in location based services and the usability of the proposed solutions.

Keywords*: Optimal locations, Privacy, Global Positioning System (GPS), Position Based Servers, Mobile application.*

1. INTRODUCTION

Speedy teemingness of smart-phone technology in city profession has enabled cell-phone users to use context aware services on their system or devices. Facilities providers take benefit of this growing and dynamic technology landscape by proposing advance context-dependent services for cell subscribers. Location based Services (LBS), for e.g., are used by billions of cell phone subscribers every day to get location-specific information. [1]

Only two region that causes in mobile phone environment to challenging location privacy preservation. Interceptions of Wireless communications are simple; example eavesdropper can store transmitted data of cell-phone users at some public place. Since people are publicly notice, context information can easily be got from their conversations. As a result, partial trajectory data related with a user's real identity is necessarily exposed to the eavesdropper and the second one, the limited resources of mobile phones greatly bound secrecy raising Technologies one could deploy and apply in wireless network.

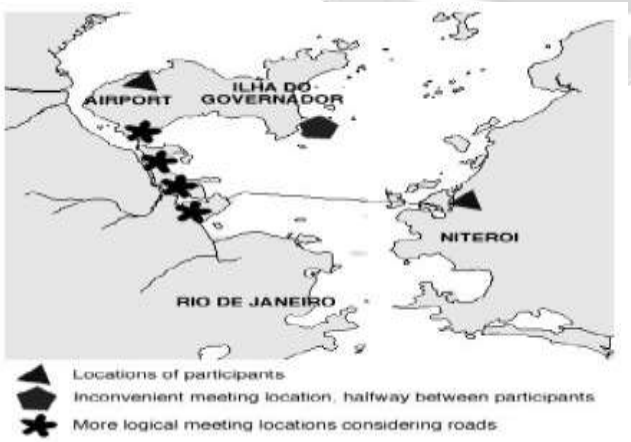

Fig 1: Optimization for geographic centers might miss logical meeting points.

Current solutions reply on easy rule to hide the real identity of a cell phone user from a passive opposer, rather than complex cryptographic technologies.

Location check-ins and location sharing are two popular characteristics of location-based services. Examine in an area, users can deal their present location with friends and family or find location-specific services from third-party supplier.

The obtained service does not depend on the area of other users and other type of location-based services, which depend on sharing of locations by a bunch of users in order to receive some service for the whole group or bunch, are also seemly famous. Privacy of a user's location or area preferences, compare to other users and the third-party service supplier, is a difficult matter in such type location-sharing based applications. For e.g., this type of information can be used to distract users and their availableness, to search their preferences or to recognize their social networks. A third-party Service provider could easily guess home or work location more than one users who use their service on regular basis in the application of taxi-sharing. Without effective security, if the stored data is pass in an unknown fashion with corporate peoples, which could have dangerous result on the user's social, personal and financial life.

2. LITERATURE SURVEY

2.1 DBGlobe: A Service-Oriented P2P System for Global Computing.

We see the multitude of peers carrying services and data as a super-database in the DBGlobe project. Our aim is to create a data management system for indexing, modeling and querying data hosted by such widely distributed, possibly and free mobile peers. We apply a service-oriented to come near, in that data are capsulize in services. Directly querying of data is also supported by an XML query language. Here, we look our research output along the following topics: (a) infrastructure support, with mobile peers and the making of context-dependent communities, (b) metadata system management for services and peers, including location dependent information, (c) filters for frequently routing path problems on hierarchical data, and (d) querying using the AXML language that incorporates service calls in the XML documents. Here, ongoing project is a DBGlobe and the future plans with others applicable notions of data flexibility as well as giving a more diplomatic treatment of updates.

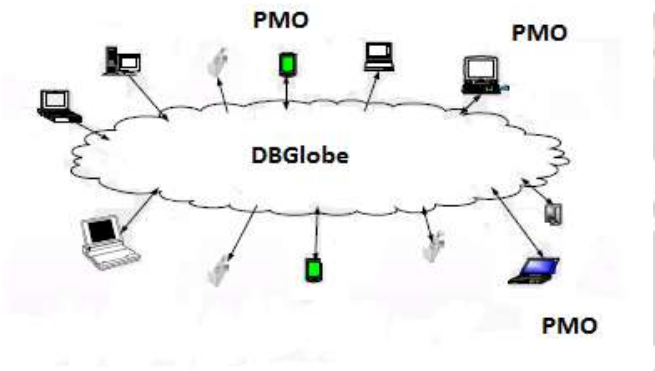

Fig 2 : The DBGlobe Layer

2.2 Secrecy of Community Pseudonyms in Wireless Peer-to- Peer Networks

To improve social relations wireless network play an important role. In particular, line-to-line wireless communication activate, direct and real-time interaction with nearly devices and communities and could improve current online social networks systems by giving correlative services adding real-time community detection and friend's and localized data sharing without requirement of infrastructure. After more years of research, the result of such as mobile to mobile wireless networks is finally being allowed. A fundamental primitives the ability to discover geographic proximity of specific communities of people (e.g, friends or neighbours). So that, mobile phone devices must interchange some community identifiers or messages. We examine privacy threats developed by such systems communications, in particular, adversarial community detection. We use the logic of community pseudonyms to abstract anonymous community identification mechanisms and explain two distinct notions of community secrecy by using challenge response techniques. A wide cost duplicate and investigation results throw further light on the consistency of these mechanisms in the

further coming generation of wireless device to device networks. This part, included the problem of community secrecy in line-to-line wireless networks and look over secrecy risks of information sharing within communities in such networks. Finding the need to secure community privacy, we proposed a frame-work based on great challenge response games to study it. An impressive result of the framework is the analytical relation received between community unlink ability and community anonymity. The relations between these two properties was studied previously. To the study of our knowledge, we are the one to analyse how to relate these properties. By means of simulated results, we evaluate the privacy provided by different pseudonym-based community secrecy-conserving schemes. Our output results throw light on the relationship between community pseudonym based and secret handshake schemes: shrinking the number of possible community pseudonyms significantly reduces the achievable secrecy. The result describe the soft trade-off between the obtainable community privacy and the cost of community pseudonym schemes. Our research allow system designers to tune their compress or shrunk scheme to a desired secrecy level, for example, daily changing the set of community pseudonyms. We also observed that reusing pseudonyms across communities (Hints) can provide a good cost or secrecy trade-off and exposed that anonymous schemes are at best harmful to community secrecy. In the future, we intend to check other communication design and by means of practical performance, study the extra overhead introduced by community pseudonym schemes.

2.3 Quantifying Location Privacy: The Case of Sporadic Location Exposure

Mobile users show their area location to potentially unauthorized entities by using location-based services system. Based on the no. of times of sharing location in these applications, we cut them into mainly two types: One is Continuous and the other is infrequent and these two sharing location types lead to different hazards. Let's an example, in the continuous case the attacker can detect users over time and space, whereas in the infrequent case, his object is more on localizing users at few points in time. We introduce an analytical way to estimate user's location secrecy by modeling both the location-based applications and the location-privacy preserving mechanisms (LPPMs), and by mentioning a well-defined working model. This framework enables us to customize the LPPMs to the employed location based application, in order to furnish higher location secrecy for the users. In this paper, we illustrate localization attacks for the case of few sharing location, using Bayesian inference for Hidden Markov Processes. We also evaluate user location secrecy with respect to the attackers with two different way of background knowledge: Those who knows the geographical structure distribution of users over the mentioned regions or area, and those who also know how users move out between the different regions (such that, their mobility pattern system). Using the Location secrecy Meter tool, we check the effectualness of the following techniques in increasing the likely error of the adversary in the localization attack: Location breaking and fake location injection mechanisms for anonymous traces We propose to the best of our idea, the first formal framework for evaluating location privacy in the case where users display their location sporadically. We validate irregular location-based applications. By using this formalization, we model different location secrecy conserve mechanisms, i.e., location obfuscate and fraud-location area injection. Formalizing both area location-privacy and location-based applications conserving mechanisms in the same framework active us to design more effective safe mechanism that are applicable tailored to each location-based service. We also built a logical framework, based on Bayesian inference in Hidden Markov Processes system, to perform localization fire on anonymized traces (for attackers with different background knowledge). The results get from the simulations of the attacks on mobility traces un-veil the strength of different mechanisms, such as the location breaking, the false-location injection, and anonymization, in conserving location-secrecy of cell phone users.

2.4 Privacy in Mobile Computing for Location-Sharing-Based Services

Location-Sharing-Based Services (LSBS) usually Location-Based Services by using locations from a bunch of users, and not just private, to share some contextualized facility based on the locations in the group. However, there are improving task about the misuse of location data by third-parties, which fuels the need for more privacy secures in such services. We relate the suited problem of privacy. In LSBSs by giving practical and capable solutions to the secrecy problem in one such service, namely the fair rendezvous point determination service. The privacy conserving FRVP (PPFRVP) problem is general sufficient and nicely captures the computations and secrecy requirements in LSBSs. In this project, we take two secrecy-conserving algorithms for the FRVP problem and logically describe their privacy in both active and passive adversarial scenarios. We study execution and the feasibility of the proposed approaches by implementing them on Nokia mobile phone devices. By the targeted user-survey, we effort to gain further understanding of the popularity, the privacy and acceptance of the proposed solutions. This part, notifies the problem of privacy in LSBS by giving practical and effective solutions to one such popular and relevant service. The PPFRVP problem looks the essential

computational and secrecy building blocks present in any LSBS offered on mobile devices. We architect and implemented on real mobile devices and analyses the performance of our privacy-preserving protocols16 for the fair rendezvous problem. Our outputs are effective in terms of secrecy, have acceptable performance, and do not make additional overhead for the users. Moreover, our user's-survey showed that the proposed privacy features are important for the acceptance of any such application, which reinforces the need for further exploration in secrecy of LSB services. To the best of our knowledge, this is the first such type effort in this direction.

2.5. Secure Actor Directed Localization in Wireless Sensor and Actor Networks

Wireless sensor network and actor networks are both fully automated and actor nodes are introduces to communicate with sensor nodes directly and reduce the communication time caused by base station or sink nodes. Sometimes, the actor node is directly access without the adding of any other control room. Actor node is head for taking a prompt action against the reported event by a sensor node. For safe communication, it is important that sensor and actor nodes be aware of their existing location and the data must be encrypted before execution. Due to energy constraints, secure and safe localization in wireless sensor networks is a wide issue. To date, the researchers have proposed many approaches for localization of sensor nodes in the network. In this section, we provide new insights for secure actor directed localization technique in wireless sensor and actor networks. A secure connectivity based localization approach for sensor and actor nodes localization is included. This approach helps to locate a sensor node efficiently and effectively. We have also decreased the possibility of the registration of attacker nodes and attacks with other legitimate nodes in the network. The proposed idea prevents man-in-the-middle attacks and safely deployed data to the destination. In this paper we proposed a safe mechanism for localization of sensor nodes in wireless sensor networks. Using an encryption algorithm for safe data deployment and registration of sensors with anchor node, we effectively block and minimize the external attacks. After simulation results, we conclude that efficient localization in sensor networks can be greatly improved by the understanding of both connectivity of sensor nodes and to which nodes they are not connected. The mechanism shows a particular area in which a node can be localized and we can find it easily there. Once the anchor node locates its own position, the sensor nodes are able to localize each other. This approach is initiated by the anchor node having higher resources than sensor node; therefore, it will reduce energy consumption as well as increase networks lifetime. However the future work is to stop the internal attacks and reduce the number of compromised sensor nodes in the network.

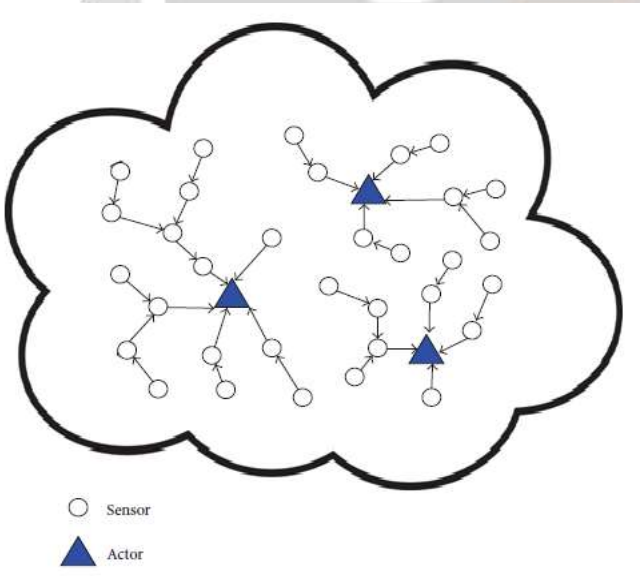

Fig 3 : Wireless sensor and actor network.

3. PROPOSED SYSTEM

In the proposed system have following modules proposed which is described given below:

3.1 Employee

In this module, user registers to the system using android phone. Then login to the system by entering valid username and password. When employee gets the meeting request from server, he sent the two locations to the server. Then, he chooses any one optimal location which sent by server and sends it to the server.

3.2 Server/Admin Module

This module works as the controlling and authorizing module for the users who are registering to the system. The Server module takes care of storing the choice locations in encrypted format in the database and fetching the choice locations given by users from the database. The Geo midpoint calculation algorithm works at server end once all the choice locations from all the users have been received. Post completion of calculation of oml, the final oml is stored in dataset, so that it can be accessed by the users.

Server sends the request for meeting to the employees. When server gets the two-two locations from every employee then it send these locations to the optimal meeting calculation module. Then, it sends two optimal locations calculated by optimal meeting calculation module to the employees. Then, it finalize one optimal location from two optimal locations which sent by employees. And send finalized location to the employees as final optimal meeting location for the meeting.

3.3 Optimal Meeting calculation

After getting two lists of locations from server, it calculates the two optimal locations from location lists send by employees. It sends both optimal locations to the server.

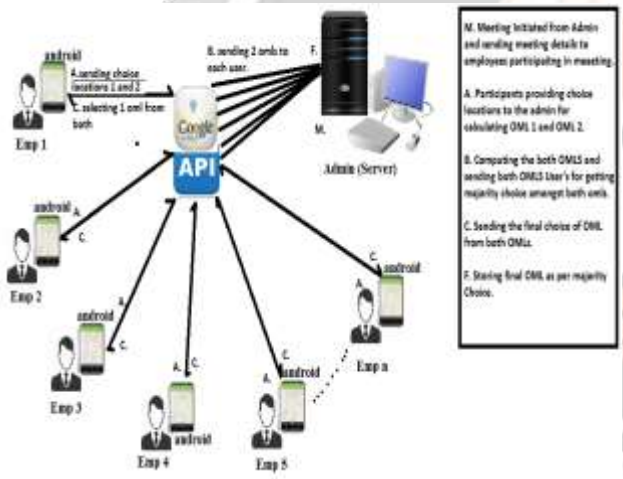

Fig 4 : System Architecture

Proposed system will have two algorithms for solving the Fair Rendez-Vous Point (FRVP) problem in a privacy-preserving fashion, where each user participates by providing only a single location preference to the FRVP solver or the service provider. In addition to the theoretical analysis, we will evaluate the practical efficiency and performance of the proposed algorithms by means of a prototype implementation on a test bed of mobile devices. It will address the multi-preference case, where each user may have multiple prioritized location preferences. Goal is to provide practical privacy preserving techniques to solve the FRVP problem, such that neither a third-party, nor participating users, can learn other user's locations; participating users only learn the optimal location. The privacy problem in the FRVP problem is representative of the relevant privacy threats in LSBSs. It addresses the privacy issue in Location-Sharing-Based Services (LSBS) by focusing on a specific problem called the Fair Rendez-Vous Point (FRVP) problem, given a set of user location preferences, the FRVP problem is to determine a location among the proposed ones such that the maximum distance between this location and all other users' locations is minimized, i.e. it is fair to all users. We will first formulate the FRVP problem as an optimization problem, specifically the k-center problem, and then analytically outline the privacy requirements of the participants with respect to each other and with respect to the third-party service provider. We will use two algorithms for solving the above formulation of the FRVP problem in a privacy- preserving fashion, where each user participates by providing only a single location preference to the FRVP service provider. The proposed algorithms take advantage of the homo- morphic properties of well-known cryptosystems, such as BGN, ElGamal and Paillier, in order to privately compute an optimally fair

rendezvous point from a set of user location preferences. Apart from that, the multi-preference case, where each user may have multiple prioritized location preferences can be considered.

4. MATHEMATICAL MODEL

4.1 System Description

Input: Employee login to the system and send two locations to the server.

Output: Final Optimal Location.

Identify data structures, classes, divide and conquer strategies to exploit distributed/parallel/concurrent processing, constraints. Our system work as a distribute manner. It means that one module is dependent on the another module. The output of previous module is required as a input to the next module. So that before executing previous module we cannot execute the next module.

Functions: Identify Objects, Morphisms, Overloading in functions, Functional relations.

1. Employee:

Set(U)= {s0,s2,s3,u0,u1,u2,u3}
U0- User authentication
U1- send two locations to server
U2- choose any one location from both location
U3- send selected location to the server

2. Server:

Set(S)= {u1,u3,m2,s0,s1,s2,s3}
S0- send message for meeting to the employee
S1- Send the locations to the Optimal Meeting Calculation Module
S2- send both optimal location to the employee
S2- select maximum count from both location
S3- send final location to the employee

3. Optimal Meeting calculation:

Set(M)= {s1,m0,m1,m2}
M0- find optimal location from first list
M1- find optimal location from second list
M2- send both optimal locations to server

Union and intersection of sets:
Set(U)= {s0,s2,s3,u0,u1, u2,u3}
Set(S)= {u1,u3,m2,s0,s1,s2,s3}
Set(M)= {s1,m0,m1,m2}
U union S = { s0,s2,s3,u0,u1, u2,u3,m2,s1}
U intersection S= {s0,s2,s3,u1,u3}
S union M= {u1,u3,m2,s0,s1,s2,s3,m0,m1,m2}
S intersection M= {m2,s1}

4.2 Venn Diagrams

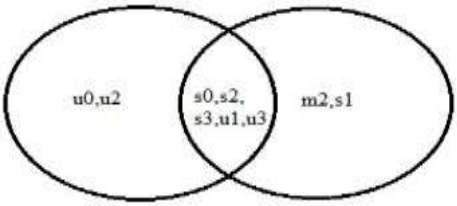

Fig 5: U union S

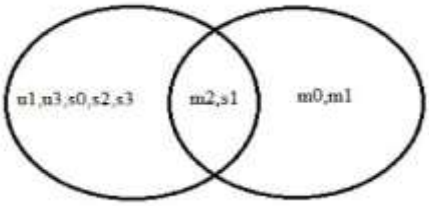

Fig 6: U intersection S

Success Conditions: Our system will give the expected result.
Failure Conditions: Without android phone we cannot run this application.

5. ALGORITHMS

5.1 Proposed System Pseudo Algorithm

Steps:

- Server send meeting request to employee
- Employee sends to location L1 and L2 to server
- Server forward these two locations to optimal meeting calculation
- Optimal meeting calculation find Optimal location OL1
- Optimal meeting calculation find Optimal location OL2
- Optimal meeting calculation sends these optimal locations OL1 and OL2 to server
- Server forward these optimal locations OL1 and OL2 to the employee
- Employee choose any one optimal location from OL1 and OL2
- Employee send selected Optimal location to the Server
- Server selects final optimal location FOL which get maximum count for from both Optimal location
- Server sends the final optimal location FOL to the employee
- Employee attained the meeting.

5.2 Geo Mid-point calculation algorithm:

- For the first location given the values in the list:Lat1, lon1, years1, months1 and days1. Then convert Lat1 and Lon1 from degrees to radians by using,

  lat1 = lat1 * PI/180
  lon1 = lon1 * PI/180

- Then, convert lat/lon to Cartesian coordinates for first location by using,

  X1 = cos (lat1) * cos (lon1)
  Y1 = cos (lat1) * sin (lon1)
  Z1 = sin (lat1)

- If locations are to be weighted equally, set w1, w2 etc all equal to 1.

- Repeat steps 1-3 for all remaining locations in the list.

- Compute combined total weight for all locations.

- Compute weighted average x, y and z coordinates by using,

x = ((x1 *w1)+(x2 *w2)+:::+(xn *wn))=totweight.
y = ((y1 *w1)+(y2 *w2)+:::+(yn *wn))=totweight
z = ((z1 *w1)+(z2 *w2)+:::+(zn wn))=totweight

- Convert average x, y, z coordinate to latitude and longitude. Note that in Excel and possibly some other applications, the parameters need to be reversed in the atan2 function, for example, use atan2(X,Y) instead of atan2(Y,X).

  Lon = atan2(y,x)
  Hyp = sqrt(x * x + y * y)
  Lat = atan2(z,hyp)

- Convert lat and lon to degrees.
  lat = lat *180/PI
  lon = lon * 180/PI

6. RESULTS

Result description of the proposed system is as described below:

6.1 Admin Login to the system

Fig 7 : Admin Login

6.2 Employee Registration

Fig 8 : Employee Registration

6.3 Employee Activation

Fig 9 : Employee Activation

6.4 Schedule Meeting

Fig 10 : Schedule Meeting

6.5 Final Optimal Location Calculation:

Fig 11 : Final Optimal Location Calculation

6.6 Server Setting

Fig 12: Server IP Setting

6.7 Login Screen

Fig 12 : Login Screen

6.8 Registration Screen

Fig 13: Registration Screen

6.9 Home Page

Fig 14 : Home Page

6.10 View Meeting List

Fig 15 : View Meeting List

6.11 Optimal Choice Location

Fig 16: Optimal Choice Location

6.12 Optimal Choice Location Rejection

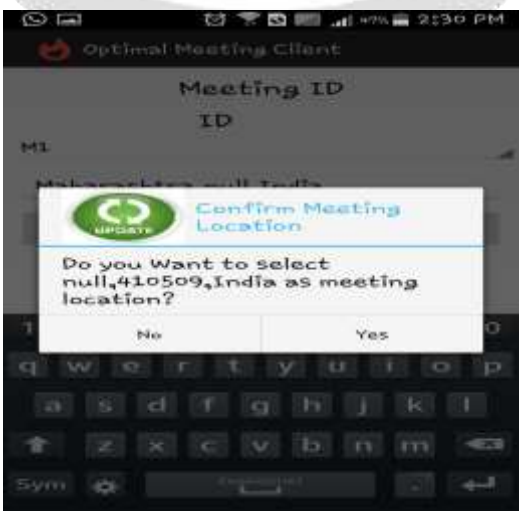

Fig 17 : Optimal Choice Location Rejection

6.13 Final Optimal Meeting Location

Figm18: Final Optimal Meeting Location

6.14 View Meeting Location on Map

Fig 19 : View Meeting Location on Map

7. CONCLUSION

In this system, we addressed the privacy issue in the Fair Rendez-Vous Problem (FRVP). Our solutions are based on the homomorphic properties of well-known cryptosystems. We implemented, designed and evaluated the performance of our algorithms on real mobile devices. We showed that our solutions preserve user preference privacy and have acceptable performance in a real implementation. We extended the proposed algorithms to include cases where users have several prioritized locations preferences. Finally, based on an extensive user-study, we showed that the proposed privacy features are crucial for the adoption of any location haring or location-based applications.

8. REFERENCES

[1] Igor Bilogrevic, Murtuza Jadliwala, Vishal Joneja, Kubra Kalan ”Privacy- Preserving Optimal Meeting Location Determination on Mobile Devices,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 7, pp. 1141-1156, JULY 2014.

[2] P.Golle and K.Partridge, ”On the anonymity of home/work location pairs,” in Proc. 7th Int. Conf. Pervasive Computing, pp. 390-397, 2009.

[3] J.Freudiger, R.Shokri, and J.P. Hubaux, ”Evaluating the privacy risk of location-based services,” in Proc. 15th Int. Conf. Financial, pp. 31-46, 2011.

[4] J.Freudiger, M.Jadliwala, J.P. Hubaux, V.Niemi, P.Ginzboorg, and I.Aad, ”Privacy of community pseudonyms in wireless peer-to-peer networks, Mobile Netw. Appl., vol. 18, no. 3, pp. 413-428, 2012.

[5] J.Krumm, ”A survey of computational location privacy,” Personal Ubiquitous Computing, vol. 13, no. 6, pp. 391-399, 2009.

[6] K.B.Frikken and M.J.Atallah, ”Privacy preserving route planning,” in Proc. ACM WPES, pp. 8-15, 2004.

[7] P.Santos and H.Vaughn, ”Where shall we meet? Proposing optimal locations for meetings,” in Proc. MapISNet, 2007.

[8] G.Zhong, I.Goldberg, and U.Hengartner, ”Louis, Lester and Pierre: Three protocols for location privacy,” in Proc. 7th Int. Conf. PrivacyEnhancing Technologies, pp. 62-76, 2007.

[9] F.Berger, R.Klein, D.Nussbaum, J.R. Sack, and J.Yi, ”A meeting scheduling problem respecting time and space,” GeoInformatica, vol. 13, no. 4, pp. 453-481, 2009.

[10] S.Jaiswal and A.Nandi, ”Trust no one: A decentralized matching service for privacy in location based services,” Proc. ACM MobiHeld, 2010.

[11] S.Guha, M.Jain, and V.Padmanabhan, Koi: A location-privacy platform for smartphone apps,” Proc. 9th USENIX Conf. NSDI, 2012.

[12] B.Carbunar, R.Sion, R.Potharaju, and M. Ehsan, ”The shy mayor: Private badges in geosocial networks,” in Proc. 10th Int. Conf. ACNS, pp. 436-454, 2012.

[13] S.Pidcock and U. Hengartner, ”Zerosquare: A privacy-friendly location hub for geosocial applications,” Proc. 2nd ACM SIGCOMM Workshop Networking, Systems, and Applications Mobile Handhelds, 2013.

[14] R.Rivest, A.Shamir, and L.Adleman, ”A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[15] D.Boneh, E.J.Goh, and K.Nissim, ”Evaluating 2-DNF formulas on ciphertexts,” in Proc. TCC, pp. 325-341, 2005.

BIOGRAPHIES

	Snehal Borude Masters in Engineering, computer science department, VACOE,Ahmednagar, Maharashtra. Bachelors in Information Technology,JSPM'S BSIOTR,Pune Maharashtra.
	Vrushali Ranmalkar PHD, Dr. Babasaheb Ambetkar Marathwada university,Aurangabad, Maharashtra. Lecturer At Computer Science Department, VACOE, Maharashtra, India