International Journal on Applications in Information and Communication Engineering
Volume 2: Issue 1: January 2016, pp 9-13. www.aetsjournal.com ISSN (Online) : 2394-6237

Optimal Meeting Location Determination on Mobile Devices with Privacy Preservation

C.Titus, A.Vijayalakshmi, M.Jenolin Rex

Abstract— In a modern data sharing society most of the people depends some additional mechanisms to share their resources with the help of devices. The mobile phones play a vital role in it. These Mobile devices contains lot and lots of applications to provide services to users, location based services is including in the scenario. But the question arises to everybody's mind that the sharing resource is how much secure? For answering these questions each and everyone depends on the third party provider devices or regular service providers. But many of the people (may be individual or group) do not want to reveal their location based information to service providers or third party vendors, because of maintaining their privacy. A new technique is introduced to provide service between source and destination persons to share the optimal meeting point locations safely without any security issues, called PPFRVP (Privacy Preserving Fair Rendoz-Vous Point). The PPFVRP approach is used to show the possible set of meeting point locations (n-Locations) between source and destination and allow the user to fetch the favorable one. The Secure Hash Algorithm is used by the source end for cipher process and shares the Meeting point locations to destination. For all the quoted rules of FVRP and SHA provides an efficient result to share the optimal meeting points between source and destination end.

Index Terms— Data Sharing, Third Party Provider Devices, Privacy Preserving Fair Rendoz-Vous Point (PPFRVP), Secure Hash Algorithm.

I. INTRODUCTION

The rapid proliferation of Smartphone technology in urban communities has enabled mobile users to utilize context ware services on their devices. Service providers take advantage of this dynamic and ever-growing technology landscape by proposing innovative context-dependent services for mobile subscribers. Location-based Services (LBS), for example, are used by millions of mobile subscribers every day to obtain location-specific information. Two popular features of location-based services are location check-ins and location sharing. By checking into a location, users can share their current location with family and friends or obtain location-specific services from third-party providers.

C.Titus, A.Vijayalakshmi, M.Jenolin Rex, Department of Computer Science and Engineering, Mahendra College of Engineering, Salem. (Email: titusc@mahendracollege.com, vijayalakshmia@mahendracollege.com, jenolinrexm@mahendracollege.com)

The obtained service does not depend on the locations of other users. The other types of location-based services, which rely on sharing of locations (or location preferences) by a group of users in order to obtain some service for the whole group, are also becoming popular. According to a recent study, location sharing services are used by almost 20% of all mobile phone users. One prominent example of such a service is the taxi-sharing application, offered by a global telecom operator, where Smartphone users can share a taxi with other users at a suitable location by revealing their departure and destination locations. Similarly, another popular service enables a group of users to find the most geographically convenient place to meet. Privacy of a user's location or location preferences, with respect to other users and the third-party service provider, is a critical concern in such location-sharing-based applications. For instance, such information can be used to de-anonymize users and their availabilities, to track their preferences or to identify their social networks. For example, in the taxi-sharing application, a curious third-party service provider could easily deduce home/work location pairs of users who regularly use their service. Without effective protection, even sparse location information has been shown to provide reliable information about a users' private sphere, which could have severe consequences on the users' social, financial and private life. Even service providers who legitimately track users' location information in order to improve the offered service can inadvertently harm users' privacy, if the collected data is leaked in an unauthorized fashion or improperly shared with corporate partners. Recent user studies show that end-users are extremely sensitive about sharing their location information. Our study on 35 participants, including students and non-scientific staff, showed that nearly 88% of users were not comfortable sharing their location information.

Thus, the disclosure of private location in any Location-Sharing-Based Service (LSBS) is a major concern and must be addressed. In this paper, we address the privacy issue in LSBSs 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. Our 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 users' locations; participating users only learn the optimal location.

The privacy issue in the FRVP problem is representative of the relevant privacy threats in LSBSs. Our contributions in this paper are as follows. We 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 solver (in this case, a third-party service provider). We then propose 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 solver or the service provider. Our proposed algorithms take advantage of the homomorphic properties of well-known cryptosystems, such as BGN, ElGamal and Paillier, in order to privately compute an optimally fair rendez-vous point from a set of user location preferences. In this significantly extended version of our earlier conference paper, we evaluate the security of our proposal under various passive and active adversarial scenarios, including collusion. We also provide an accurate and detailed analysis of the privacy properties of our proposal and show that our algorithms do not provide any probabilistic advantage to a passive adversary in correctly guessing the preferred location of any participant. In addition to the theoretical analysis, we also evaluate the practical efficiency and performance of the proposed algorithms by means of a prototype implementation on a testbed of Nokia mobile devices. We also address the multi-preference case, where each user may have multiple prioritized location preferences. We highlight the main differences, in terms of privacy and performance, with the single preference case, and also present initial experimental results for the multi-preference implementation. Finally, by means of a targeted user study, we provide insight into the usability of our proposed solutions.

II. PROBLEM STATEMENT

The rapid production of smart phone technology in urban communities has enabled mobile users to utilize context aware services on their devices. Service providers take advantage of this dynamic and ever-growing technology landscape by proposing innovative context-dependent services for mobile subscribers. Location-based Services (LBS), for example, are used by millions of mobile subscribers every day to obtain location-specific information .Two popular features of location-based services are *location check-ins* and *location sharing*. By checking into a location, users can share their current location with family and friends or obtain location-specific services from third-party providers, the obtained service does not depend on the locations of other users. The other types of location-based services, which rely on sharing of locations (or location preferences) by a group of users in order to obtain some service for the whole group, are also becoming popular. According to a recent study, location sharing services are used by almost 20% of all mobile phone users. One prominent example of such a service is the taxi-sharing application, offered by a global telecom operator, where smart phone users can share a taxi with other users at a suitable location by revealing their departure and destination locations. Similarly, another popular service enables a group of users to find the most geographically convenient place to meet.

- Service Providers takes an advantage of this kind of data sharing,
- Third Party providers or their devices can easily catch the location of the source person intend,
- Privacy of a user's location or location preferences, with respect to other users and the third-party service provider, is a critical concern in such location sharing based applications. For instance, such information can be used to de-anonymize users and their availabilities, to track their preferences or to identify their social networks. For example, in the taxi-sharing application, a curious third-party service provider could easily deduce home/work location pairs of users who regularly use their service.
- Without effective protection, evens parse location information has been shown to provide reliable information about a users' private sphere, which could have severe consequences on the users' social, financial and private life. Even service providers who legitimately track users' location information in order to improve the offered service can inadvertently harm users' privacy, if the collected data is leaked in an unauthorized fashion or improperly shared with corporate partners.
- Possibility to redirect the destination parties to the favorable place of the Service providers or third party providers.

1. Privacy in mobile computing for location-sharing-based services

Location-Sharing-Based Services (LSBS) complement Location Based Services by using locations from a group of users, and not just individuals, to provide some contextualized service based on the locations in the group. However, there are growing concerns about the misuse of location data by third-parties, which fuels the need for more privacy controls in such services. We address the relevant problem of privacy in LSBSs by providing practical and effective solutions to the privacy problem in one such service, namely the fair rendez-vous point (FRVP) determination service. The privacy preserving FRVP (PPFRVP) problem is general enough and nicely captures the computations and privacy requirements in LSBSs. In this paper, we propose two privacy-preserving algorithms for the FRVP problem and analytically evaluate their privacy in bothnpassive and active adversarial scenarios. We study the practical feasibility and performance of the proposed approaches by implementing them on Nokia mobile devices. By means of a targeted user-study, we attempt to gain further understanding of the popularity, the privacy and acceptance of the proposed solutions.

2. Private queries in location based services: Anonymizers are not necessary

Mobile devices equipped with positioning capabilities (e.g., GPS) can ask location-dependent queries to Location Based Services (LBS). To protect privacy, the user location must not be disclosed. Existing solutions utilize a trusted anonymizer between the users and the LBS. This approach has several drawbacks: (i) All users must trust the third party anonymizer, which is a single point of attack. (ii) A large number of

cooperating, trustworthy users is needed. (iii) Privacy is guaranteed only for a single snapshot of user locations; users are not protected against correlation attacks (e.g., history of user movement). We propose a novel framework to support private location dependent queries, based on the theoretical work on Private Information Retrieval (PIR). Our framework does not require a trusted third party, since privacy is achieved via cryptographic techniques. Compared to existing work, our approach achieves stronger privacy for snapshots of user locations; moreover, it is the first to provide provable privacy guarantees against correlation attacks. We use our framework to implement approximate and exact algorithms for nearest-neighbor search. We optimize query execution by employing data mining techniques, which identify redundant computations. Contrary to common belief, the experimental results suggest that PIR approaches incur reasonable overhead and are applicable in practice.

3. Secure distance-based localization in the presence of cheating beacon nodes

Localization or location discovery in the presence of cheating beacon nodes is an important problem in mobile wireless ad hoc and sensor networks. Despite many significant research efforts in this direction, there is no sufficient condition to estimate the error bound. Although many algorithms were proposed to calculate the error bound using necessary and sufficient condition there occur some problems which cause the error in correct location discovery. This paper attempts to find a secure distance based location discovery in presence of beacon nodes and verify the accuracy and efficiency of the experiments using practical distance estimation error models.

III. APPROACH

We then propose 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 solver or the service provider. In this significantly extended version of our earlier conference paper, we evaluate the security of our proposal under various passive and active adversarial scenarios, including collusion. We also provide an accurate and detailed analysis of the privacy properties of our proposal and show that our algorithms do not provide any probabilistic advantage to a passive adversary in correctly guessing the preferred location of any participant. In addition to the theoretical analysis, we also evaluate the practical efficiency and performance of the proposed algorithms by means of a prototype implementation on a test bed of Nokia mobile devices. We also address the multi-preference case, where each user may have multiple prioritized location preferences. We highlight the main differences, in terms of performance, with the single preference case, and also present initial experimental results for the multi-preference implementation. Finally, by means of a targeted user study, we provide insight into the usability of our proposed solutions.

- We address the privacy issue in LSBSs 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.
- The Secure Hash Algorithm (SHA) is implemented to provide the optimal location oriented transmission with privacy preserving concern.
- In this method we achieve two processes simultaneously without the help of third party service providers. There are:
    1. Location Check-Ins
    2. Location Sharing

Range & Bandwidth: Mobile Internet access is generally slower than direct cable connections, using technologies such as GPRS and EDGE, and more recently HSDPA and HSUPA 3G and 4G networks. These networks are usually available within range of commercial cell phone towers. Higher speed wireless LANs are inexpensive but have very limited range.

Security standards: When working mobile, one is dependent on public networks, requiring careful use of VPN. Security is a major concern while concerning the mobile computing standards on the fleet. One can easily attack the VPN through a huge number of networks interconnected through the line.

Power consumption: When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive batteries must be used to obtain the necessary battery life.

Transmission interferences: Weather, terrain, and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.

Potential health hazards: People who use mobile devices while driving are often distracted from driving and are thus assumed more likely to be involved in traffic accidents. (While this may seem obvious, there is considerable discussion about whether banning mobile device use while driving reduces accidents or not.) Cell phones may interfere with sensitive medical devices. Questions concerning mobile phone radiation and health have been raised.

Human interface with device: Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

IV. ARCHITECTURAL DESIGN

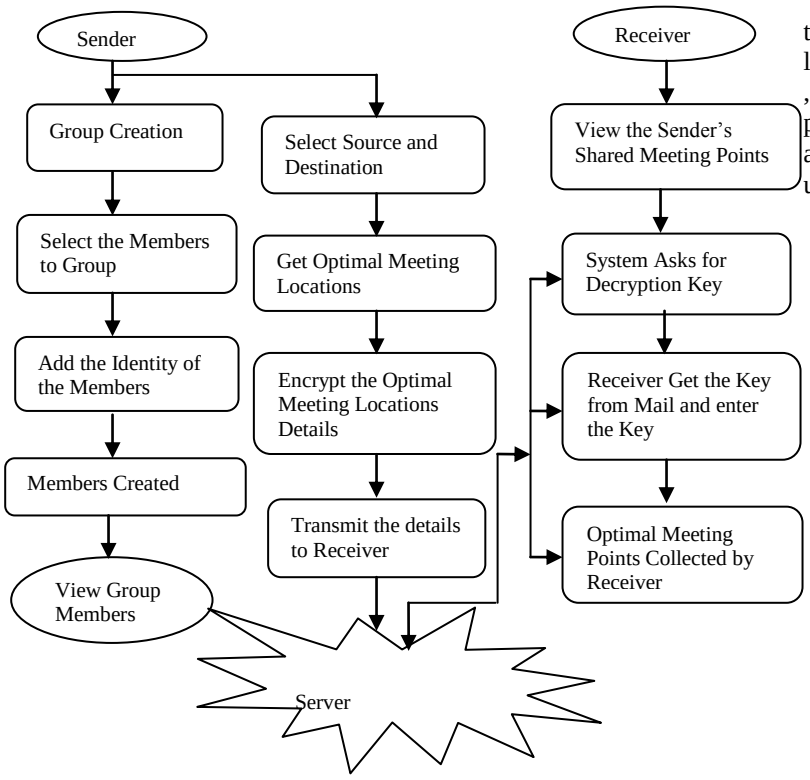

Fig.1 System Architecture

The major part of the project development sector considers and fully survey all the required needs for developing the project. Once these things are satisfied and fully surveyed, then the next step is to determine about the software specifications in the respective system such as what type of operating system the project would require, and what are all the necessary software are needed to proceed with the next step such as developing the tools, and the associated operations. Generally algorithms shows a result for exploring a single thing that is either be a performance, or speed, or accuracy, and so on. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. System architecture can comprise system components, the externally visible properties of those components, the relationships (e.g. the behavior) between them.

V. METHODOLOGY

Following are the most frequently used project management methodologies in the project management practice:

1. User Privacy
2. Server Privacy
3. PPFRVP protocol
4. Privacy Under Multiple Dependent Executions

1) User Privacy

The user-privacy of any PPFRVP algorithm A measures the probabilistic advantage that an adversary a gains towards learning the preferred location of at least one other user ,except the final fair rendez-vous location, after all users have participated in the execution of the PPFRVP protocol. An adversary in this case is a user participating in A. We express user-privacy as three different probabilistic advantages.

- We measure the probabilistic advantage of an adversary ua in correctly guessing the preferred location Li of any user ui _= ua. This is referred to as the identifiability advantage.
- The second measure of user-privacy is the distance linkability advantage, which is the probabilistic advantage of an adversary ua in correctly guessing whether the distanced i, j between any two participating users ui _= u j, is greater than a given parameter s, without learning any users' preferred locations Li , L j.
- The coordinate-linkability advantage, denoted as Advc−LNKa, is the probabilistic advantage of an adversary ua in correctly guessing whether a given coordinate xi (or yi) of a user ui is greater than the corresponding coordinate(s) of another user u j _= ui without learning the users' preferred locations Li, L j.

2) Server Privacy

For the third-party (LDS) adversary, the game definitions are similar to those defined for a user adversary, except that the LDS does not receive L f air in the Step 2 of the game. Then, the server-privacy of a PPFRVP algorithm A can then be defined as follows. Definition 3: An execution of the PPFRVP algorithm A is server-private if the identifiability advantage DTLDS (A), the distance-linkability advantage Advd−LNKLDS and the coordinate linkability advantage Advc−LNKLDS of an LDS are negligible. In practice, users will execute the PPFRVP protocol multiple times with either similar or completely different sets of participating users, and with the same or a different location preference in each execution instant. Thus, although it is critical to measure the privacy leakage of the PPFRVP algorithm in a single execution, it is also important to study the leakage that may

occur over multiple correlated executions, which in turn depends on the intermediate and final output of the PPFRVP algorithm.

3) PPFRVP Protocol

The PPFRVP protocol has three main modules:
(A) The distance computation module,
(B) The MAX module and

A) Distance Computation: The distance computation module uses either the BGN-distance or the Paillier- ElGamal distance protocols. We note that modules (B) and (C) use the same encryption scheme as the one used in module (A). In other words, (*E).It* refers to encryption using either the BGN or the Paillier encryption scheme.

B) MAX Computation: In Step B.1, the LDS needs to hide the values within the encrypted elements (i.e., the pair wise distances computed earlier) before sending them to the users. This is done in order to

(i) Ensure privacy of real pair wise distances,
(ii)Be resilient in case of collusion among users and
(iii) Preserve the internal order (the inequalities) among the pair wise distance from each user to all other users.

4) Privacy Under Multiple Dependent Executions

As defined earlier, in a dependent execution of the PPFRVP protocol, all the involved parties possess information from the previous executions, in addition to the current input, output and intermediate data. It is clear that, due to the oblivious or blind nature of the computations, the privacy guarantees of the proposed PPFRVP protocols with respect to the LDS independent executions remains the same as that for independent executions. Furthermore, dependent executions in which the information across executions is completely uncorrelated (e.g., different set of users in each execution or different and unrelated preferences in each execution) reduce to independent execution. We analyze two different scenarios of dependent executions involving differential information. First, we consider the case of dependent executions with different subsets of participants. We assume that, in each sequential execution, the set of users or participants is reduced by exactly one (the adversary participant remains until the end), and that the retained participants preferences remain the same as the previous execution(s). The following information is implicitly passed across executions in this scenario:

(i) Participant set,
(ii)Optimal fair location $L\ f\ air$, permuted and randomly scaled pair wise distances from the participant to every other participant, and (iv) scaled (but order preserving) maximum distance from every participant to every other participant.

VI. CONCLUSION

The Privacy Issue in the Fair Rendez-vous Problem (FRVP) Is Addressed Deeply. The Security And Privacy Measures Are Handled By Well-known Cryptographic Concepts Like SHA And BGN. This system experimentally shows that the solutions preserve user preference privacy and have acceptable performance in a real implementation. Moreover, the proposed approach is extended by algorithms to include cases where users have several prioritized locations preferences. Finally, based on an extensive user study, this approach showed that the proposed privacy features are crucial for the adoption of any location sharing or location-based applications.

VII. FUTURE WORK

The Privacy Issue in the Fair Rendez-vous Problem (FRVP) is addressed deeply via the proposed implementations but we can extend the proposed algorithms to include cases where users have several prioritized locations preferences. We can provide fully mobile based data services in future for more reliable and efficient data services. Covert the encryption process to 1024 bit advanced encryption process based on mobile supportively. Attribute based encryption process can be achieved.

REFERENCES

[1] (2011, Nov.). Facebook Statistics [Online].Available: http://www.facebook.com/press/info.php?statistics
[2] (2011, Nov.). Facebook Deals [Online]. Available: http://www.facebook.com/deals/
[3] E. Valavanis, C. Ververidis, M. Vazirgianis, G. C. Polyzos, and K. Norvag, "MobiShare: Sharing context-dependent data & services from mobile sources," in Proc. IEEE/WIC Int. Conf. WI, Oct. 2003, pp. 263–270.
[4] (2011). Microsoft Survey on LBS [Online]. Available: http://go.microsoft.com/?linkid=9758039
[5] (2011, Nov.). Orange Taxi Sharing App [Online]. Available:http://event.orange.com/default/EN/all/mondial
[6] (2011). Let's Meet There [Online]. Available: http://www.letsmeetthere.net/
[7] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in Proc. 7th Int. Conf. Pervasive Computing, 2009, pp. 390–397.
[8] J. Freudiger, R. Shokri, and J.-P. Hubaux, "Evaluating the privacy risk of location-based services," in Proc. 15th Int. Conf. Financial, 2011, pp. 31–46.