



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Finding Secured Optimal Meeting Location Using Mobile Phones

Vilas Shelke^{#1}, Prof.Ritesh Thakur^{#2}

Student, Dept. of Computer Engineering, SP's IOKCOE, Pimple, Jagtap, Pune, India^{#1}

Head of Department, Dept. of Computer Engineering, SP's IOKCOE, Pimple, Jagtap, Pune, India^{#2}

ABSTRACT: The mobile phones play a vital role in today's highly interconnected world. Users arrange and plan their daily routines using such high end devices. These Mobile devices contains lots of applications to provide services to users, location based services is including in the scenario. Users of mobile devices are not comparable to share their current and preferred location which may harm their private, social and financial life. System used to find optimal meeting location for mobile users by preserving their location privacy. Location privacy is preserved by using secured encryption. 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 Privacy Preserving Fair Rendez-Vous Point. This approach is used to show the possible set of meeting point locations between source and destination and allow the user to fetch the favorable location.

KEYWORDS: Mobile Applications, Location Privacy, Encryption.

I. INTRODUCTION

Mobile phones offers different services like online payment, online shopping, weather forecasting and location based services. Online payment includes payment to ISP (internet service provides), Electricity Bill, mobile recharge, banking services, money transfer. Through online shopping users can order different equipments like electronics gadgets, furniture, cloths etc. Weather services provide information about rain, humidity, temperature etc. Location based services include GPS (Global Positioning System), navigation, traffic information. While using the location based services user location privacy is important issues. This paper is based on finding optimal meeting location for number of users using location based services while preserving their location privacy.

Location privacy preservation in mobile setting is challenging for 2 reasons. First wireless Communications is straightforward to intercept e.g. auditor will collect transmitted information of mobile users at sure public place. Besides, since individuals are publically noticeable, context data will easily be obtained from their spoken communication or behaviours. As a result, partial flight data related to users real identity is inevitably exposed to the auditor. Second, the restricted resources of mobile devices greatly restrict Privacy Enhancing Technologies one might apply and deploy in wireless network. Current solutions rely on straightforward schemes to cover the 64000 identity of a mobile user from a passive mortal, instead of advanced cryptology technologies. Two widespread options of location-based services are location check-ins and site sharing. By checking into a location, users will share their current location with family and friends or acquire location-specific services from third-party suppliers. The obtained service doesn't rely on the locations of different users. The opposite varieties of location-based services, which rely on sharing of locations by a gaggle of users so as to get some service for the complete cluster, are changing into widespread.

II. RELATED WORK

MobiShare:[2] Sharing context-dependent information and services from mobile sources The speedy advances in wireless engineering and mobile computing have Enabled personal mobile devices that we have a tendency to use in daily life to become data and Service suppliers by complementing or replacement. Location hosts connected to the wire line Network. Such mobile resources are extremely vital for different moving users, creating significant opportunities for several attention-grabbing and novel applications. The MobiShare design provides the infrastructure for present



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

mobile access and mechanisms for Publishing, discovering and accessing heterogeneous mobile resources in an exceedingly giant space, taking into account the context of each sources and requestors. Any wireless communication Technology may well be used between a tool and also the system. What is more, the utilization of XML related Languages and protocols for describing and exchanging information provide the system a uniform and simply labile interface, permitting a spread of devices to use it. The general Approach is data-centric and service-oriented, implying that every one devices area unit treated as Producers or requestors of knowledge of data wrapped as information services.

Privacy Preserving route designing: In 2004, Frikken and Atallah [3] projected Secure Multiparty Computation (SMC) protocols for firmly computing the distance between the points. One problem with route planning protocols is that the demand that the device recognize where it's at, which might appear to need some type of query to a GPS system, however this is able to reveal the situation of the device.

Shall we meet: In 2007, port and Vaughn [4] projected optimum locations for conferences, conferred a survey of existing literature on meeting-location algorithms and propose aa lot of comprehensive solution for such a drag. Automating system defaults when users offer inadequate information from calendars or begin points will facilitate, however preferences concerning times, venues, and travel methods is sophisticated even once proverbial. Associate organizer, or participants who vote, to judge decisions and finetune results to suit cluster criteria.

Koi A location-privacy platform for smart phone app: In 2012,[5] Guha projected a privacy-preserving location based matching as a basic platform primitive and as a tentative to exposing low-level, latitude-longitude coordinates to applications. Applications set wealthy location-based triggers and have these be discharged supported location updates either from the native device or from aforeign device. But issue pertains to malicious applications registering an oversized variety of triggers at sensitive locations, and reverse-engineering a victim user's location supported triggers matched. A weak defence against this attack would be rate-limit to the quantity of trigger registrations from associate application.

Disadvantages of existing system

Privacy of a users location or location preferences, with relation to different users and also the third-party service provider, could be a vital concern in such location sharing based sharing based applications. For example, such data is wont to de-anonymize users and their availabilities, to trace their preferences or to identify their social networks. For instance, in the taxi-sharing application, a curious third-party service provider might simply deduce home/work location pairs of users WHO often use their service. While not effective protection, evens take apart location information has been shown to produce reliable data about a user's personal sphere that might have severe consequences on the user's social, financial and private life. Even service suppliers who legitimately track user's location data so as

to improve the offered service will unknowingly harm users privacy, if the collected information is leaked in an unauthorized fashion or improperly shared with corporate partners.

III. PROPOSED SYSTEM

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 two location preference to the FRVP solver or the service provider

Proposed system has three modules.

1. Meeting Participant (Employee)
2. Server.
3. Optimal Meeting Location calculator.

1. Meeting Participant (Employee)

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

It is mobile user who wants to attend meeting at convenient location. There are n number of mobile users these are also called meeting participants. Each participant send two preferred meeting location as response to server meeting request. There is n*2 number of preferred meeting locations which server receives.

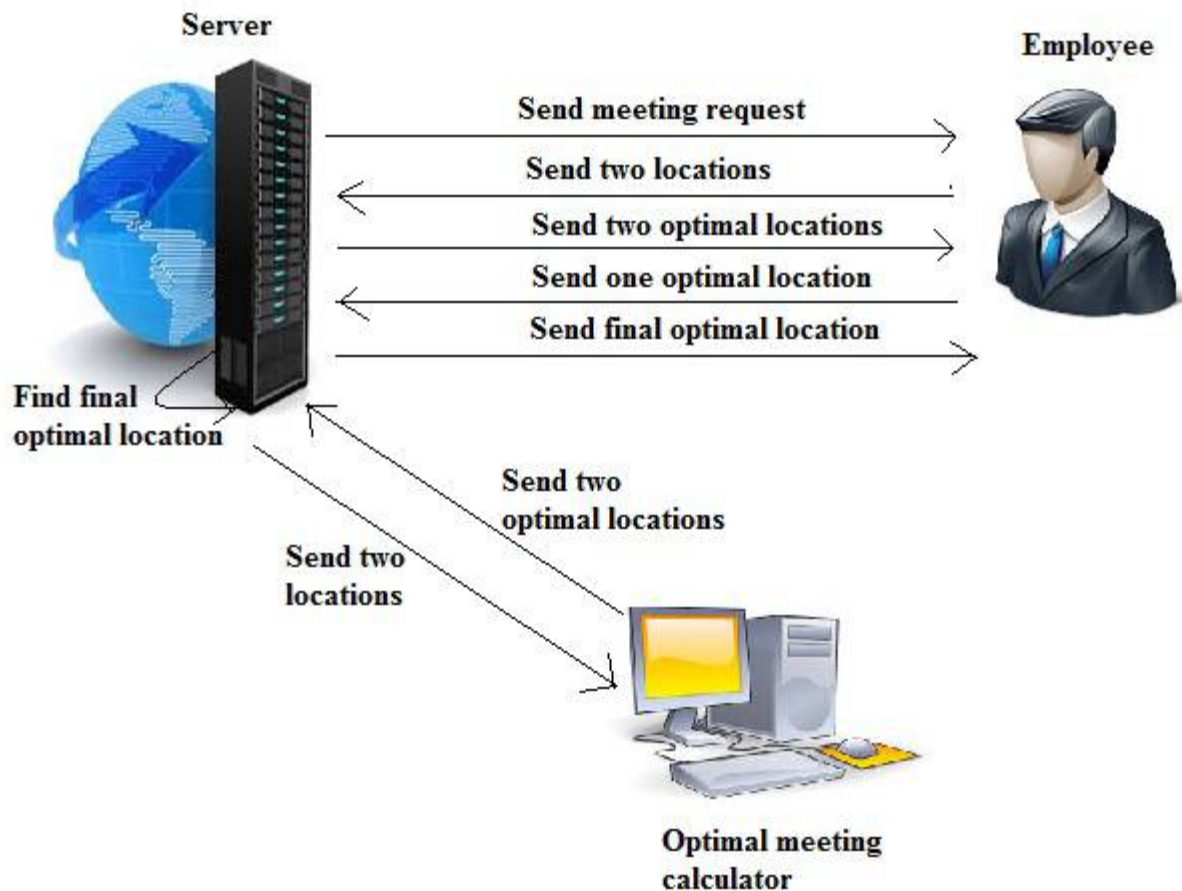


Fig.1 System Architecture

2. Server

Server send meeting request to meeting participants. It is responsible for meeting initialization. It collects all participants preferred meeting locations and sends it to Optimal Meeting Location calculator. It acts as intermediary between participant and Optimal Meeting Location calculator. It send final two optimal meeting locations to participants then all participants vote for final optimal meeting location and on voting server select one optimal meeting location and distribute to participants.

3. Optimal Meeting Location calculator

It is responsible for finding two optimal meeting locations from user preferred locations. Optimal locations are such that it should minimize the maximum displacement of end user from its current location to optimal location.

Each user's mobile device is able to communicate with the LDS through Internet connection. Each user u_i has to find the coordinates $L_i = (x_i, y_i)$ of his preferred rendez-vous location. Users can either use their current location as their preferred rendez-vous location or they can give some other convenient location such as a known restaurant) away from their current position. Users determine their current position by using a positioning service, such as Global Positioning System (GPS). We need to make assumption that the positioning service is fairly accurate. GPS has an average positioning error between 3 and 7.8 meters. Users can continue to use the service of the LDS for privately



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

computing the fair rendezvous location without using the positioning service, say by manually estimating their preferred rendezvous location. If positioning service is used, it can continuously track users based on the positioning requests or it can behave maliciously and provide incorrect position information to the users. We do not consider these adversarial scenarios involving the positioning service. We define the set of the preferred rendezvous locations of all users as $L = \{L_i\}_{i=1}^n$. For simplicity, we consider line of sight Euclidean distances between preferred rendezvous locations. Even though the actual real-world distance (road, railway, boat, etc.) between two locations is at least as large as their Euclidean distance.

IV. PROPOSED ALGORITHM

Steps:

1. Server send meeting request to employee
2. Employee sends to location L1 and L2 to server
3. Server forward these two locations to optimal meeting calculation
4. Optimal meeting calculation finds optimal location OL1
5. Optimal meeting calculation finds optimal location OL2
6. Optimal meeting calculation sends these optimal locations OL1 and OL2 to Server
7. Server forward these optimal locations OL1 and OL2 to the employee
8. Employee choose any one optimal location from OL1 and OL2
9. Employee send selected optimal location to the Server
10. Server selects final optimal location FOL which get maximum count for from both Optimal location
11. Server sends the final optimal location FOL to the employee
12. Employee attained the meeting.

AES Algorithm

AES is a new cryptographic algorithm which can be used to protect electronic data. AES is a block cipher of symmetric-key which uses the keys of 128, 192, and 256 bits, and encrypts as well as decrypts contents in blocks of 128 bits. AES uses a key pair, the same key used by the symmetric-key ciphers to encryption and decryption of data. The same number of bits has the data which encrypted which obtained by block ciphers that the input data had. A loop structure used by iterative ciphers that permutations as well as substitutions of the input data performs repeatedly.

The AES algorithm is depends on permutations and substitutions. Permutations mean that rearrangements of data and substitutions are the replacement of the data i.e. replaces one unit of data with another. Using several different techniques,

AES performs permutations and substitutions. The AES cipher key size represents the number of repetitions of transformation rounds which performs conversion the input, which is known as the plaintext, into the final output, which is known as the cipher text. Following there are shows the number of cycles of repetition:

- For 128-bit keys 10 cycles of repetition
- For 192-bit keys 12 cycles of repetition.
- For 256-bit keys 14 cycles of repetition.

Several processing steps are consist by each round, each containing four similar but which are different stages. In those, one that based on the key encryption itself. To transform cipher text back into the original plaintext, a set of reverse rounds are applied using the same encryption key.

Algorithm:

Step 1: Key Expansions

For each round AES needs a different 128-bit block of round key also one more.

Step 2: Initial Round

Add Round Key with a block of the round key, each byte of the state is combined using bitwise xor.

Step 3: Rounds

- Sub Bytes in this step each byte is replaced with another byte.
- Shift Rows for a certain number of steps, the states last three rows are moved



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Cyclically.

- Mix Columns on the columns of the state a mixing operation operates, in each column combining the four bytes.

Step 4: AddRoundKey

Step 5: Final Round (no Mix Columns)

- Sub Bytes
- Shift Rows
- AddRoundKey.

Time Complexity

The AES algorithms is normally only working on a fixed block size, and take approximately the same time independently of input, thus they are $O(1)$. If we put them into a mode of operation to encrypt longer messages, you usually get an $O(m)$ complexity, where m is the message size, as you have $O(m)$ blocks of data to encrypt.

V. MATHEMATICAL MODEL

Steps to find optimal Location

Steps:

1. 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,

$$\text{lat1} = \text{lat1} * \text{PI}/180$$

$$\text{lon1} = \text{lon1} * \text{PI}/180$$

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

$$X1 = \cos(\text{lat1}) * \cos(\text{lon1})$$

$$Y1 = \cos(\text{lat1}) * \sin(\text{lon1})$$

$$Z1 = \sin(\text{lat1})$$

3. Then for first location compute weight (by time).

$$w1 = (\text{years1} * 365.25) + (\text{months1} * 30.4375) + \text{days1}$$

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

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

5. Compute combined total weight for all locations.
Totweight = $w1 + w2 + \dots + wn$

6. Compute weighted average x, y and z coordinates by using,

$$x = ((x1 * w1) + (x2 * w2) + \dots + (xn * wn)) / \text{totweight}$$

$$y = ((y1 * w1) + (y2 * w2) + \dots + (yn * wn)) / \text{totweight}$$

$$z = ((z1 * w1) + (z2 * w2) + \dots + (zn * wn)) / \text{totweight}$$

7. 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).



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

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

8. Convert lat and lon to degrees.

lat = lat *180/PI
lon = lon *180/PI

9. Special case:

If $\text{abs}(x) \leq 10^{-9}$ and $\text{abs}(y) \leq 10^{-9}$ and $\text{abs}(z) \leq 10^{-9}$ then the geographic midpoint is the center of the earth.

SET THEORY APPLIED TO THE PROJECT

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, Homomorphisms, Overloading in functions, Functional relations Mathematical formulation if possible

Mathematical Model:

1. Employee:

Set (U) = {s0,s2,s3,u0,u1,u2,u3}

U0- User authentication

U1- sends two locations to server

U2- choose any one location from two selected 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- sends both optimal location to the employee

S2- selects 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}

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

U union S={ s0,s2,s3,u0,u1, u2,u3,m2,s1}
 U intersection S={ s0,s2,s3,u1,u3}
 S U M={ u1,u3,m2,s0,s1,s2,s3,m0,m1,m2}
 S intersection M={m2,s1}

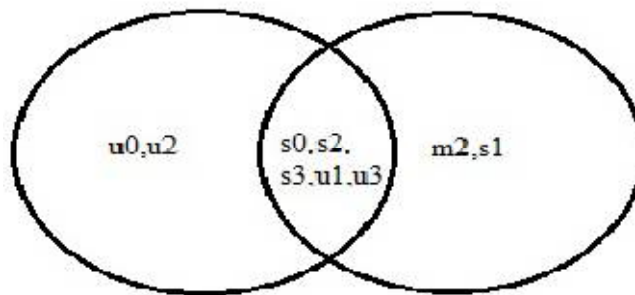


Fig.2 Figure 5.2.4: U intersection S

Success Conditions: Our system will give the expected result

Failure Conditions: Without android phone we cannot run this application

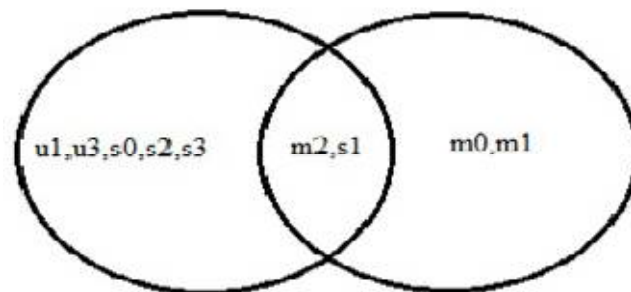


Fig.2 S intersection M

VI. RESULT AND ANALYSIS

In this chapter we display the results of our proposed system.

1. Admin Login



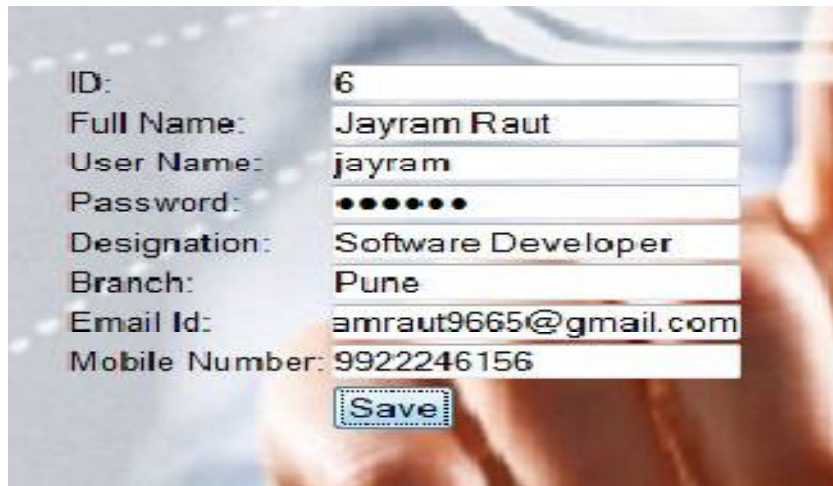
Figure 2. Admin Login

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

2. Employee Registration



ID: 6
 Full Name: Jayram Raut
 User Name: jayram
 Password: ●●●●●●
 Designation: Software Developer
 Branch: Pune
 Email Id: amraut9665@gmail.com
 Mobile Number: 9922246156

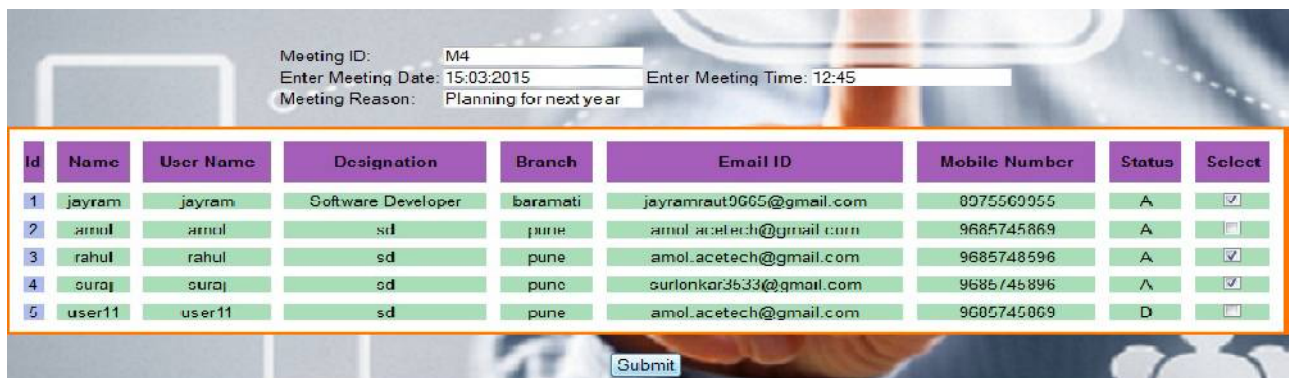
Figure3. Employee Registration form

3. Employee Activation

Id	Name	User Name	Designation	Branch	Email Id	Mobile Number	Status	Activate
1	jayram	jayram	Software Developer	baramati	jayramraut9665@gmail.com	8975569955	A	Activate
2	amol	amol	sd	pune	amol.acetech@gmail.com	9685745869	A	Activate
3	rahul	rahul	sd	pune	amol.acetech@gmail.com	9685748596	A	Activate
4	suraj	suraj	sd	pune	surlonkar3533@gmail.com	9685745896	A	Activate
5	user11	user11	sd	pune	amol.acetech@gmail.com	9685745869	D	Activate

Figure 4. Employee Activation

4. Schedule Meeting



Meeting ID: M4
 Enter Meeting Date: 15:03:2015
 Meeting Reason: Planning for next year
 Enter Meeting Time: 12:45

Id	Name	User Name	Designation	Branch	Email ID	Mobile Number	Status	Select
1	jayram	jayram	Software Developer	baramati	jayramraut9665@gmail.com	8975569955	A	<input checked="" type="checkbox"/>
2	amol	amol	sd	pune	amol.acetech@gmail.com	9685745869	A	<input type="checkbox"/>
3	rahul	rahul	sd	pune	amol.acetech@gmail.com	9685748596	A	<input checked="" type="checkbox"/>
4	suraj	suraj	sd	pune	surlonkar3533@gmail.com	9685745896	A	<input checked="" type="checkbox"/>
5	user11	user11	sd	pune	amol.acetech@gmail.com	9685745869	D	<input type="checkbox"/>

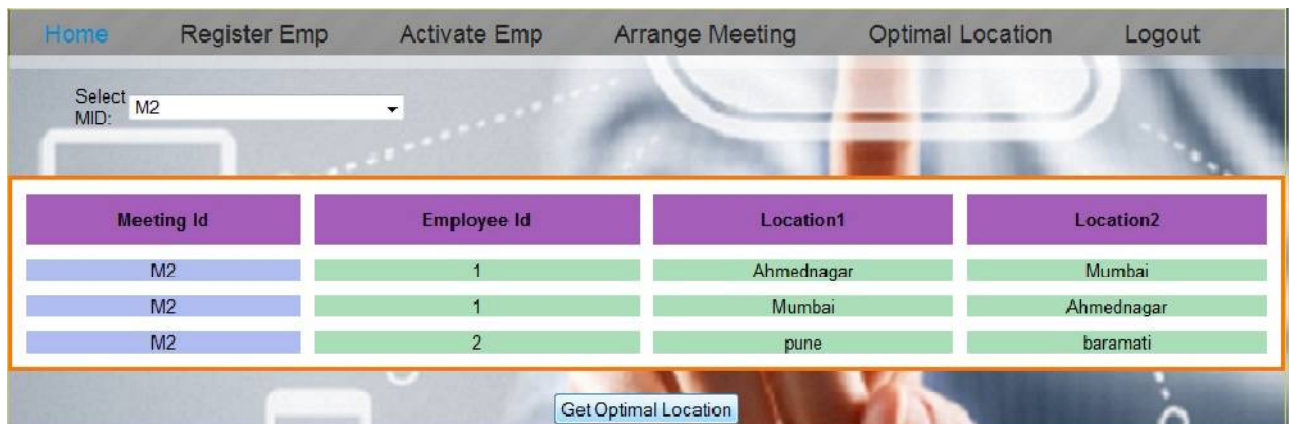
Figure 5. Schedule Meeting

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

5. Final Optimal Location Calculation



Meeting Id	Employee Id	Location1	Location2
M2	1	Ahmednagar	Mumbai
M2	1	Mumbai	Ahmednagar
M2	2	pune	baramati

Figure 6. Final Optimal Location Calculation

VII. ADVANTAGES AND LIMITATION

ADVANTAGES

1. Provide optimal meeting location.
2. Preserve user privacy by encrypting his location details.
3. Provide choice to user for meeting location.
4. System keeps track of attendance of meeting members.

LIMITATIONS

1. Encryption process is not that much secure need to change it to 1024 bit advanced encryption process based on mobile supportively.
2. Proposed system fully not mobile. Server cannot run on mobile.

APPLICATIONS

1. The proposed system helps to find the optimal meeting location for any kind of organizations.
2. System is useful to maintain the location privacy of user.
3. System can be used in any kind of LBS (location based services) to preserve privacy of user.

VIII. 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 designed, implemented 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. Moreover, 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.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

REFERENCES

1. Igor Bilogrevic, MurtuzaJadliwala, Vishal Joneja, KbraKalkan, Jean-Pierre Hubaux, and ImadAad "Privacy-Preserving Optimal MeetingLocation Determination on Mobile Devices" , IEEE Transactions on Information Forensics and Security, vol. 9, no. 7, pp. 1141-1156, JULY2014.
2. 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.
3. K. B. Frikken and M. J. Atallah, Privacy preserving route planning, in Proc. ACM WPES, pp. 815, 2004.
4. P. Santos and H. Vaughn, Where shall we meet? Proposing optimal locations for meetings, in Proc. MapISNet, 2007.
5. S. Guha, M. Jain, and V. Padmanabhan, Koi: A location-privacy platform for smartphone apps, Proc. 9th USENIX Conf. NSDI, 2012.
6. S. Jaiswal and A. Nandi, Trust no one: A decentralized matching service for privacy in location based services, Proc. ACM MobiHeld, 2010.
7. B. Gedik and L. Liu, "Location privacy in mobile systems: A personalizedanonymization model," in *Proc. 25th IEEE ICDCS*, Jun. 2005, pp. 620–629.
8. P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, in Proc. 17th Int. Conf. Theory Application CryptographicTechniques, pp. 223238, 1999.