GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES
OPTIMAL MEETING LOCATION SELECTION BASED ON USER PRIVACY

Dipali D. Kosare[*1] and Prof. D. M. Sable[2]
[*1]Computer Science & Engineering, RTMNU University, A.C.E, Wardha, Maharashtra, India
[2]Computer Science & Engineering, RTMNU University, A.C.E, Wardha, Maharashtra, India

ABSTRACT
Outfitted with front line Smartphone and cell telephones, today's remarkably interconnected urban individuals is intelligently subject to these contraptions to manage and strategy their common lives. These applications a great part of the time depend on upon current (or favored) locales of individual clients or a party of clients to give the searched for association, which imperils their security; clients would slant toward essentially not to uncover their ebb and flow (or supported) territories to the association supplier or to other, perhaps untrusted, clients. In this paper, we propose certification saving means picking a flawless meeting zone for a social event of clients. We play out a heightened security evaluation by formally measuring protection loss of the proposed techniques. With a specific choosing goal to concentrate on the execution of our figuring's in a true blue affiliation, we understand and test their execution practicality. By technique for a focused on client study, we attempt to get an understanding into the certification acknowledgment with clients in locale based associations and the solace of the proposed arrangements.[1]

Keywords: Mobile application, neglectful calculation, security.

1. INTRODUCTION
        Two definitely comprehended segments of extent based associations are zone enlistment and zone sharing. By selecting with an extent, clients can allow their present zone to family and relates or acquire locale particular associations from untouchable suppliers. The got association does not rely on upon the scopes of different clients. The other kind of zone based associations, which depend on after sharing of locales (or zone inclines) by a get-together of clients to get some association for the entire gathering, are correspondingly finding the opportunity to be caught on. As indicated by a late study, range sharing associations are utilized by essentially 20% of all telephone clients. One unmistakable layout of such an association is the taxi-sharing application, offered by a general telecom director, where PDA clients can give a taxi to different clients at a sensible region by uncovering their flight and destination ranges. Along these lines, another unquestionably comprehended association empowers a party of clients to locate the most geologically steady spot to meet [1].

        Security of a client's zone or locale inclines, regarding different clients and the outcast association supplier, is a key anxiety in such zone sharing-based applications. For instance, such data can be utilized to deanonymize clients and their availabilities [1], to track their inclinations or to see their social networks.[2] In this paper, we address the security issue in LSBSs by concentrating on a particular issue called the Fair Rendez-Vous Point (FRVP) issue. Given a game-plan of client extent inclines, the FRVP issue is to focus a domain among the proposed ones such that the most convincing allotment between this district and every last other client's zones is minimized, i.e. it is sensible to all clients. We will probably offer rational protection saving procedures to handle the FRVP issue, such that neither an outsider, nor sharing clients, can learn other clients' domains; taking a premium clients just take in the ideal reach. The confirmation issue in the FRVP issue is illustrative of the material security hazards in LSBSs.

        Our obligations in this paper are to make security game-plan alternatives for clients. To perform meeting range mapping with Google maps. To give client data choice. Giving locale sharing associations utilizing GMaps. We in addition address the multi-incline case, where every client may have distinctive sorted out extent inclinations[3].

2.   RELATED WORK

Igor Bilogrevic, proposed 1. Security Preserving Optimal Meeting Location Determination on Mobile Devices. These applications regularly depend on current (or favored) areas of individual clients or a gathering of clients to give the sought administration, which imperils their protection; clients would prefer fundamentally not to uncover their current (or favored) areas to the administration supplier or to other, conceivably untrusted, clients. In this paper, we propose protection safeguarding calculations for deciding an ideal meeting area for a gathering of users[3]. We play out an exhaustive protection assessment by formally evaluating security loss of the proposed approaches. With a specific end goal to concentrate on the execution of our calculations in a genuine deployment.[1]

2. This paper are complete and test their execution effectiveness.[2]

E. Valavanis , proposed 3. MobiShare: Sharing Context-Dependent Data and Services from Mobile Sources. mobile phones that we use in customary life to twist up information and organizations suppliers by supplementing or supplanting settled region has connected with the wireline framework. Such adaptable resources can be significantly crucial for other moving customers, making gigantic open entryways for some entrancing and novel applications. finding and getting to heterogeneous versatile resources in a far reaching zone, considering the association of both sources and requestors[4].

M. Jadliwala , proposed 4. Secure Distance-based Localization in the Presence of Cheating Beacon Nodes. This paper tries to find a secured division based region divulgence in region of reference point center points and affirm the exactness and profitability of the examinations using sensible partition estimation botch models[5].

3.   PROPOSED SYSTEM

The proposed work is planned to be carried out in the following manner
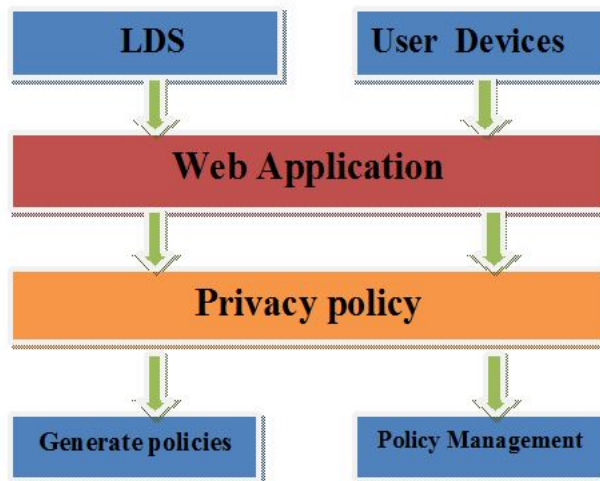
Fig.1: Basic system architecture.

We propose security protecting calculations for deciding an ideal meeting area for a gathering of clients. We play out an exhaustive protection assessment by formally evaluating security loss of the proposed approaches. In any Location-Sharing-Based Service (LSBS) is a noteworthy concern and should be tended to. We will likely give useful protection safeguarding methods to fathom the FRVP(Fair Rendez-Vous Point) issue, such that neither an outsider, nor taking an interest clients, can learn other clients' areas. In these design web application can decide the quantity

of strategies of client. Area Determination Server (LDS) can finding the area on client gadgets and give a protection strategy on meeting area.

Executing the security approach for the client on meeting area. Give the protection to every client who get the meeting area. What's more, we utilize the altered PPFRV(Privacy-Preserving Fair Rendz-Vous Point) calculation. Furthermore utilize the MD5 calculation.

JSON API
It is utilized to interface with google map. JSON API is a particular for how a customer ought to demand that assets be gotten or altered, and how a server ought to react to those solicitations.

JSON API is intended to minimize both the quantity of solicitations and the measure of information transmitted amongst customers and servers. This effectiveness is accomplished without trading off coherence, adaptability, or discoverability. JSON API require utilization of the JSON API media sort application for trading information.

Google Map service
It is utilized to interface with google map. JSON API is a particular for how a customer ought to demand that assets be gotten or altered, and how a server ought to react to those solicitations.

JSON API is intended to minimize both the quantity of solicitations and the measure of information transmitted amongst customers and servers. This effectiveness is accomplished without trading off coherence, adaptability, or discoverability. JSON API require utilization of the JSON API media sort application for trading information.

4.   METHODOLOGY

4.1 Retrieve Locations
When we are using this application For retrieve location for meeting with the third party providers first we have to retrieve the location of the user.

4.2 Check User Location
Checking into a location, users can share their current location with family and friends or obtain location-specific services from third party providers. And also user can schedule their meeting by checking the other user locations.

4.3 Schedule Meeting
After retrieving the location of the each user and checking location of the each user we can schedule the meeting on one specific space as per the user convenience, date and time.

4.4 Check Meeting Status
 After schedule the meeting all users can send their opinion about meeting if they are possible to attend the meeting by using approve or denied.
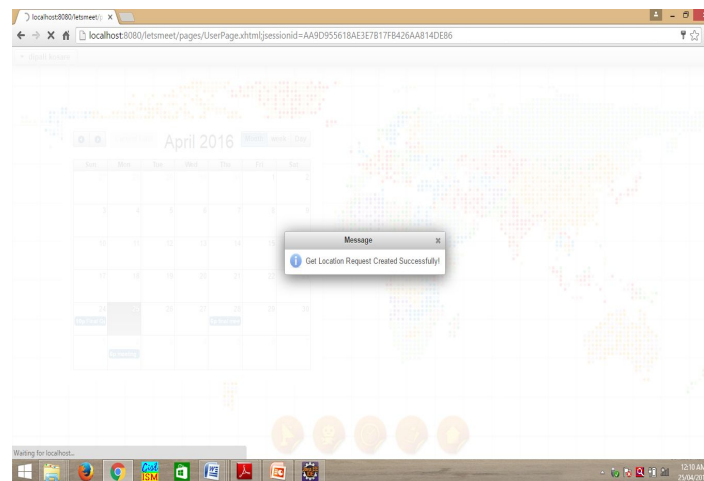
5.   DESIGN WORK

The Design work is planned to be carried out in the following manner :

Firstly, implemented the retrieve location for retrieving the location of the other user. Figs 5.1 shows the retrieve location for meeting from the other user and select the user for meeting and call them for the meeting.
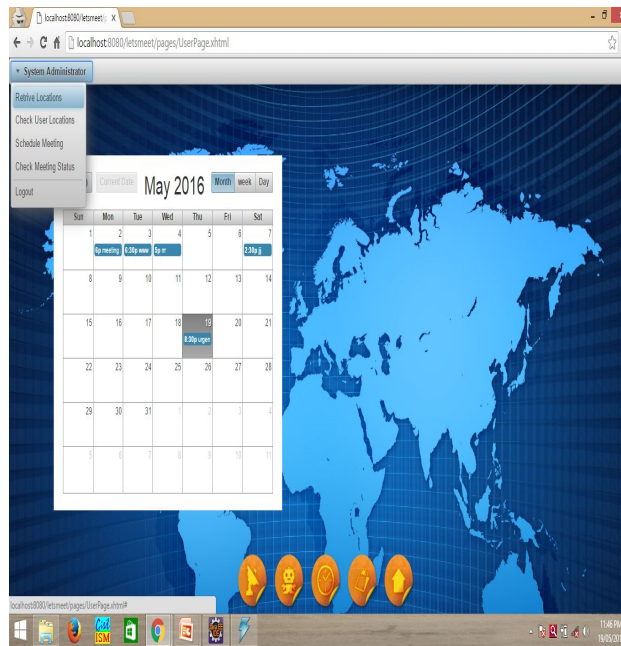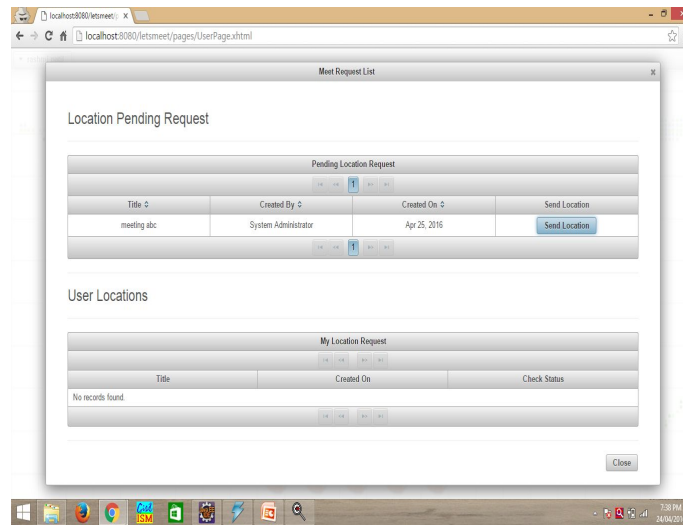
Fig 5.1: Retrieve location[1]

Fig 5.2: Request send successfully for retrieve location[2]

In above fig 5.2 the user can send the request to the other list of user for retrieve the their location after sending the message to list of user then display the message get location request created successfully.

(C) *Global Journal Of Engineering Science And Researches*

Fig 5.3 check user location[2]

Secondly, Designed the check user location after sending the message to the list of user that user can get the message and then they are send the location to that other. Fig 5.3 shows the send location for meeting.
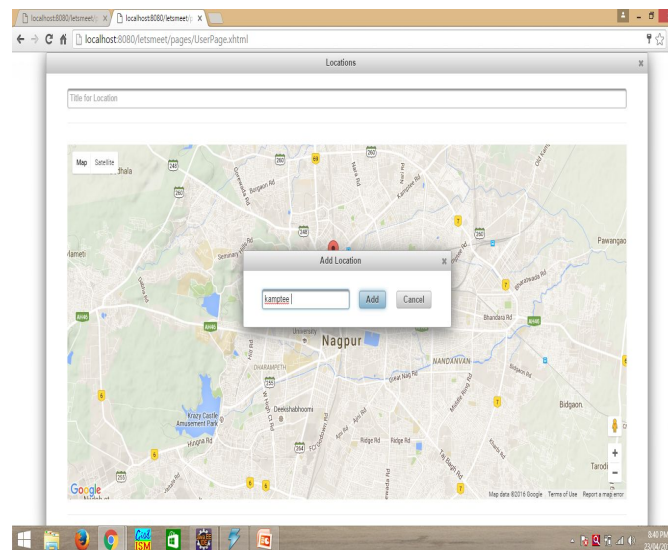
Fig 5.4 Sending the Location[2]

In above fig 5.4 to send the location to the user clicking on to the send location after that open the google map and choose the location and then send to the user.
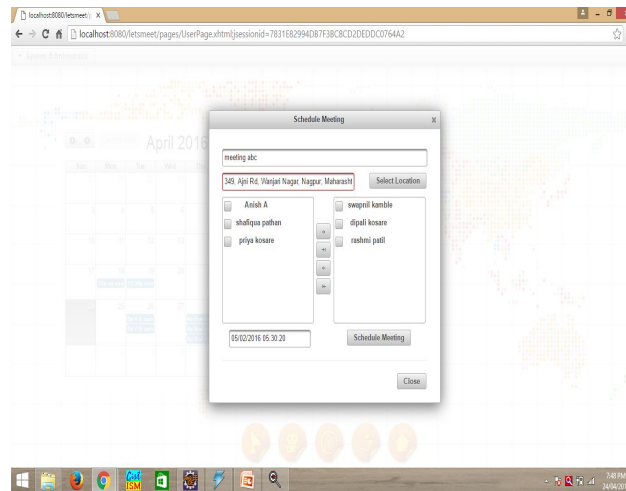
(C) *Global Journal Of Engineering Science And Researches*

Fig 5.5 Schedule Meeting [3]

Thirdly, designed the schedule meeting after user can get the location of the list of user then the user can schedule the location that is convenient to each and every user and also schedule the date and time of the meeting.

6. CONCLUSION

With a specific end goal to concentrate on the execution of our calculations in a genuine organization, we actualize and test their execution effectiveness. By method for a focused on client study, we endeavor to get an understanding into the protection familiarity with clients in area based administrations and the convenience of the proposed solutions.

REFERENCES

[1] Igor Bilogrevic, Member, IEEE, Murtuza Jadliwala, Member, IEEE, Vishal Joneja, Kübra Kalkan, Jean-Pierre Hubaux, Fellow, IEEE, and Imad Aad "Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 7, JULY 2014.

[2] [1]Dipali D. Kosare, [2]Prof. D. M. Sable,"A Survey paper on Optimal Confrontation Location Decision Based on User Privacy", International Journal of Research (IJR) e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015.

[3] [1]Dipali D. Kosare, [2]Prof. D. M. Sable, [3]Prof. D. S. Dabhade," Optimal Confrontation Location Decision Based on User Privacy", IJRITCC ISSN: 2321-8169 Volume: 4 Issue : 1 14 – 19 January 2016.

[4] 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.

[5] M. Jadliwala, S. Zhong, S. J. Upadhyaya, C. Qiao, and J.-P. Hubaux, "Secure distance-based localization in the presence of cheating beacon nodes," IEEE Trans. Mobile Comput., vol. 9, no. 6, pp. 810– 823, Jun. 2010.

[6] C. Zhang and Y. Huang, ―Cloaking locations for anonymous location based services,‖ GeoInformatica, vol. 13, no. 2, pp. 159–182, 2009

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

[8] 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.

[9] C. Ardagna, M. Cremonini, E. Damiani, S. Vimercati, and P. Samarati, ―Location privacy protection through obfuscation-based techniques,‖ in Proc. 21st IFIP WG 11.3 Working Conf. Data and Applications Security, 2007.

[10] Zhong, I. Goldberg, and U. Hengartner, ―Louis, Lester and Pierre: Three protocols for locationprivacy,‖ in Proc. 7th Int. Conf. Privacy Enhancing Technologies, 2007, pp. 62–76.

[11] A. Solanas and A. Martínez-Ballesté, ―Privacy protection in locationbased services through a public-key privacy homomorphism,‖ in Proc. 4th European Conf. Public Key Infrastructure, Theory and Practice, 2007, pp. 362–368.

[12] C.-H. O. Chen et al., ―GAnGS: Gather, authenticate 'n group securely,‖ in Proc. 14th ACM Int. Conf. Mobile Computing Networking, 2008, pp. 92–103.

[13] J. Krumm, ―A survey of computational location privacy,‖ Personal Ubiquitous Comput., vol. 13, no. 6, pp. 391–399, 2009. [14] 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.

[15] 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.

[16] B. Gedik and L. Liu, ―Location privacy in mobile systems: A personalized anonymization model,‖ in Proc. 25th IEEE ICDCS, Jun. 2005, pp. 620–629.

[17] S. Pidcock and U. Hengartner, ―Zerosquare: A privacy-friendly location hub for geosocial applications,‖ in Proc. 2nd ACM SIGCOMM Workshop Networking, Systems, and Applications Mobile Handhelds, 2013. [18] S. Guha, M. Jain, and V. Padmanabhan, ―Koi: A location-privacy splatform for smartphone apps,‖ in Proc. 9th USENIX Conf. NSDI, 2012.

[19] M. Herrmann, A. Rial, C. Diaz, and B. Preneel, ―Privacy-preserving location-sharing-based services,‖ COSIC, Katholieke Univ. Leuven, Leuven, Belgium, Tech. Rep., 2013.

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

[21] K. B. Frikken and M. J. Atallah, "Privacy preserving route planning,‖ in Proc. ACM WPES, 2004, pp. 8–15.

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

[23] 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.