iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** IV **Month of publication:** April 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Determination of Optimal Meeting Location for Preserving on Mobile Devices

A. Munikumar[1], Munikekhar Prudhvi[2]
[1]*M. Tech, Department of CSE, SITE Engg. College, Tirupati*
[2]*Asst. Professor, Department of CSE, SITE Engg. College, Tirupati*

Abstract: Presently a-days, individuals of urban and rustic are utilizing PDAs and cell phones seriously. Specifically urban populace relies on upon the applications and devices which are given by the cell phones and PDAs to arrange their every day life. The applications which are based on these gadgets for the most part rely on upon the present or favored areas of the client to give the administrations they wish, which might make harm the security of cell phone clients. When all is said in done no client wish to uncover their present area or the area they wish to go. In this paper, we proposed security protecting calculations which will give an ideal area to gathering of clients
Keywords: Mobile devices, applications, privacy preserving.

I. INTRODUCTION

In urban regions because of the quick improvement of advanced cell innovation made the general population to utilize area construct administrations with respect to their cell phones. Advantage has been taken by the administration suppliers by giving regularly developing area based administrations for cell phone clients. A huge number of individuals are utilizing area based administrations (LBS), to get data of specific area [1]. The two components that are famously utilized in view of area administrations are area registration and area sharing. Utilizing area checking, client can share his/her present area to family, companions and so on.., or client can acquire area particular data from outsider administration supplier. Alternate LBS administrations give the area sharing by the gathering or number of clients additionally getting to be famous now-a-days. Very nearly 20% of portable clients are utilizing area sharing administrations as per late study [4]. A standout amongst the most well known utilizations of such sort is taxi sharing application. By utilizing such applications client present and favored areas can be known by administration supplier which might prompts awful results on client's monetary, social, business and political status.

Client's present area and favored areas ought to be kept subtly from other member client and outsider administration supplier which is a critical angle in such LSB applications. In the event that such data like clients and their availabilities [7], are de-anonymized to known the inclinations. The outsider administration supplier can recognize the client area present and favored area combines effectively if the client is utilizing administration supplier application all the time. Indeed, even outsider administration will track the client points of interest to give the quality administration can by implication hurt the security of the client if the subtle elements are spilled in unapproved way.

In this work, we concentrate on specific issue called Reasonable Rendez-Vous point issue which is an issue in LSBSs. By utilizing the arrangement of client area inclinations from the client, the FRVP issue will decide the area from the proposed area so most extreme separation between decided area and the various favored areas can be minimized that implies it is reasonable to all clients. Principle objective of this paper is to give protection saving down to earth procedures to tackle the issue of FRVP, so that both the outsider administration supplier and clients who are taking part can't know areas of different clients. Taking an interest clients can just know the ideal area. We are going to take care of the protection issue of the client first by detailing the issue of FRVP as an issue of enhancement, especially the k-focus issue [12], and afterward security is given among the members appreciation to each other and an outsider administration supplier. Calculations proposed by us will exploit homomorphic properties of cryptosystems to figure an ideal reasonable rendez-vous point by utilizing set of area inclinations from the client. We give an exact investigation to demonstrate that our calculations won't give any method for speculating the member favored area. Counting the hypothetical investigation, we additionally made assessment of pragmatic productivity and proposed calculations execution by utilizing the usage of model on Nokia cell phone test beds. At long last we additionally propose the instance of multi-inclinations of the client taking into account needs of area. We demonstrate the distinction principally as far as execution and security, by utilizing single inclination case and beginning trial results are appeared for the usage of multi-inclination.

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

II. RELATED WORK

The security protecting reasonable rendez-vous area has less or no consideration in past work. Creators Santos and Vaughn [21] examined and displayed a study with respect to meeting area calculations and exhibited every single related answer for such issues. By considering parts of client inclination areas and limitations, the overviewed papers have not introduced any protection or security issues. So also, the proposed work of Berger et al. [22] introduced meeting-area calculation which is productive and considers the season of two sequential gatherings. In Secure Multiparty Calculation (SMC) area, a few creators have displayed protection issues which are identified with the calculation of separation of two focuses [23] or courses [24]. There are additionally numerous outcomes on exploration taking into account security safeguarding area issues. Be that as it may, all the exploration results endeavor to take care of the said issue in extraordinary and distinctive ways. Jaiswal and Nandi [25] proposed a stage of security protecting known as Trust Nobody, for areas which are found secretly adjacent purposes of hobby.

At long last, the creators of paper [26], have proposed a basic design and assessed the execution of various calculations productively which made the protection using so as to save of cell phone clients simple two unique calculations..

III. SYSTEM DESIGN

We were considered a system with two major entities: (i) A group of users or mobile devices U= {u1, u2, . . . , uN } and (ii) a third party service provider, which is known as Location Determination Server (LDS), which is source for computing the fair rendez-vous point or location from the group of user preferred locations. Each and every user can communicate with LDS by using some Internet connection.

Users can determine the coordinates Li=(xi, yi) ∈ N2 of their preferred location of rendez-vous location. We were considered a two-dimensional coordinate system. Users can mention the current or present location as rendezvous location or they can mention some preferred locations such as hotel etc.., away from present position.

We were defined the group of preferred rendez-vous locations of users as L= {Li}N i=1. For simplicity, we use line_of_sight Euclidean distances between user preferred rendez-vous locations. All though actual real-world distance of two locations is at least as same as their Euclidean distance, the proportion between distances is assumed to be correlated with Euclidean respective distances.

To solve FRVP problem, we refer Privacy Preserving Fair Rendez-Vous Point (PPFRVP) algorithm. Generally, PPFRVP algorithm A accepts the inputs and generates the output, described below.

A. *Input: transformation f of preferred locations Li: f* (L1)|| *f (L2)*|| . . . || *f (LN).* Where *f* is nothing but secrete key based encryption function so that it is difficult to determine the input Li without taking the help of the secrete key, by just observing f(Li).

B. *Output:* an output f(L fair)= g(*f*(L1), *f*(L2), . . . , *f*(LN)), where g is called as fairness function and L fair= (x1,y1) ∈ N2 is fair rendez-vous location so that it is difficult for the LDS to identify L fairby just knowing f(L fair). f(L fair) is given, each and every user is capable to compute L fair = f-1(f(L fair)) by using decryption routine and shared secrete key.

Fig. 1. Shown below describes the functional diagram of PPFRVP protocol, where LDS executes PPFRVP algorithm

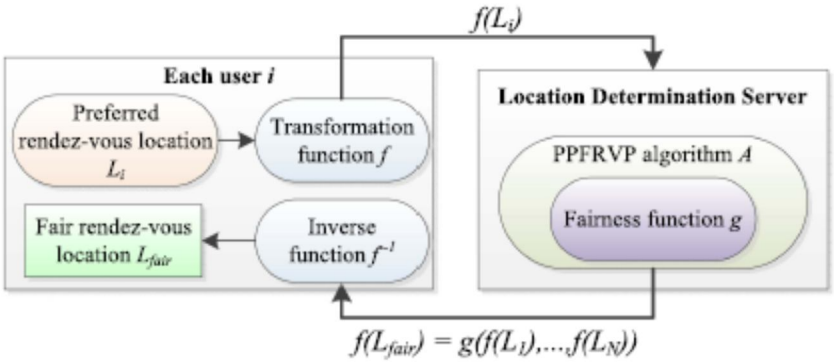


Fig. 1. Functional diagram of the PPFRVP protocol.

C. The fairness function g can be defined in different ways, based on the preferences of the policies or users. The architecture for fair rendez-vous point determination by using privacy-preserving fair rendez-vous point is as shown below.

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Fig. 2 describes one such fairness function that reduces the maximum distance of any user to other locations. unction

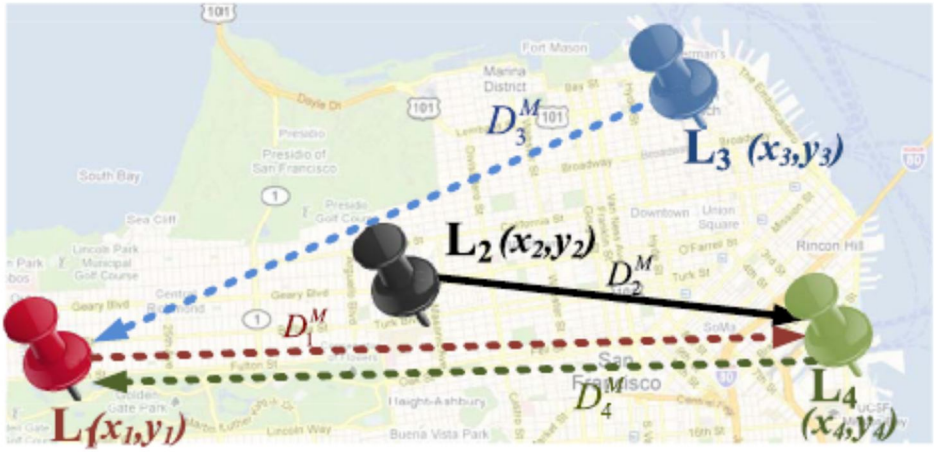


Fig. 2. PPFRVP scenario, where the fairness function is g = argmin$i$ $(DM\ i\ )$. The dashed arrows represent the maximum distance $DM\ i$ from each user ui to any user $j\ \_= i$, whereas the solid line is the minimum of all such maximum distances. The fair rendez-vous location is $L\ f\ air = L2 = (x2, y2)$.
which is considered here is fair globally and can be extended easily to add additional parameters and constraints.

D. Flow Chart for Discovering the Optimal Meeting Location for the Protecting the privacy of Mobile Device Users is as shown in the following figure:

In the fig. 3, first the current and preferred locations are collected from the users. The collected locations are submitted to cryptosystem functions and a secrete key is combined with those inputs and stored in LDS. By retrieving inputs the PPFRVP algorithm A is going to generate an optimal location, the generated optimal location is given to the user. So that user can only know his/ her own preferred or current location but not others. For the first time if the optimal location is not generated, once again PPFRVP is going to generate optimal point so that it will be in minimum distance to all other users.

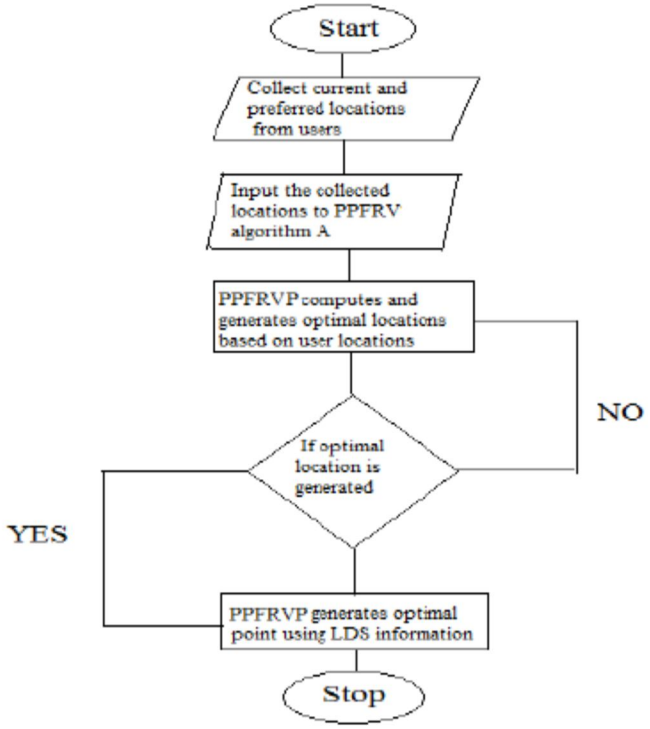


Fig.3. Flow Chart for Discovering the Optimal Meeting Location for the Protection of Privacy of Mobile Device Users.

IV. RESULTS AND DISCUSSION

In this section, We demonstrate the assessment of proposed PPFRVP conventions by utilizing diagram the aftereffects of controlled tests and led client considers utilizing model execution of conventions on cell phones.

A. *Distance Computations*

As we have discussed, the FRVP L fairis nothing but the preference of location that minimizes the maximum distance of any other preference of location and L fair. Our algorithm minimize with respect to the square of the distances, this is because distance square can be easily computed using homomorphic encryptions than distances which are simple. The squaring function will preserve order and the problem which is of finding the arguments which minimizes the maximum distance that is equivalent to finding the argument which minimizes the maximum squared distance.

1) *BGN-Distance*: First let us consider the BGN encryption sceme as a distance computation algorithm. This protocol needs only one time communication with each user and LDS. It utilizes both additive and multiplicative homomorphic properties of BGN. This BGN scheme works in the following fashion.

Ei (a) = < ai1|. . . | ai6> = < E (xi
2) | E (T- 2xi) | E (1) | E (T-2yi) | E (yi
2) | E (1) >
Ei (b) =< bi1| . . . | bi6> = < E (1) | E (xi
2) | E (yi) | E (1) | E (yi
2) >

Where, E (.) is termed as the encryption which is using the BGN scheme with KP Mvwhich is nothing but fresh session key. Li = (xi,yi) which is called as desired randez-vous user location ui and Tisthe modulus of domain
of plaintext.

2) *Paillier- Elgamal- Distance*: An another schene for computation of distance is based on both ElGamal and Paillier encryptions, Including Elgamal multiplicative homoorphic property, we depend on the two features of paillier encryption as follows:

$E(m1) \cdot E(m2) = E(m1 + m2 \bmod n), \forall mi \in Zn$ (1)

$E(m1)r = E(r \cdot m1 \bmod n), \forall r \in Z^*n$ (2)

Which indicates that

$E(r \cdot m1)r-1 = E(r-1 \cdot r \cdot m1 \bmod n)$
$= E(m1 \bmod n)$(3)

Here, r-1 is called as multiplicative inverse of r mod n. As neither ElGamal or Paillier has both additive and multiplictive properties, resultant algotithm need of extra step to compute the pairwise squared distances i.e. dij
2[13].

B. *Measurement of Performance and Implementations*

Implementation of client application on Nokia N810 mobile devices (256 MB RAM, ARM 400 MHz CPU, Maemo OS, Linux) and the implementation of LDS is running on a standard Linux PC (3 GB RAM, 2 GHz CPU, Linux). Our applications are implemented on Qt programming framework.

We show in fig. 4(a), 4(b) and 4(c) that the time of computation is increased by increasing number of users. However, the ElGamal-paillier based method is more effective and efficient across all other computations, Only 4 seconds are required to execute a protocol with participants of 10 numbers. The 2 BGN algorithms are less effective and efficient required 9 seconds of time compared to ElGamal-paillier algorithm. The reason for this is because of bilinear mapping operations of CPU of the BGN cryptosystem.

Fig. 4(d), 4(e) show different times of computation on Nokia N810 mobile device. We have seen that BGN based algorithm is most efficient in distance computations, which requires 0.3 seconds, independent of number of users. This is because the clients can send only once its own encrypted vectors to allow LDS to compute distances of all pairs, which is opposite to ElGamal-Paillier based algorithm requires that user need to encrypt and decrypt values number of times based on number of users. An another protocol, require 4 seconds for 10 participants. In the following phases, result is not better because the BGN-based protocol use intensively the bilinear mapping operations. If we see the overall performance of ElGamal-Paillier is better.

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

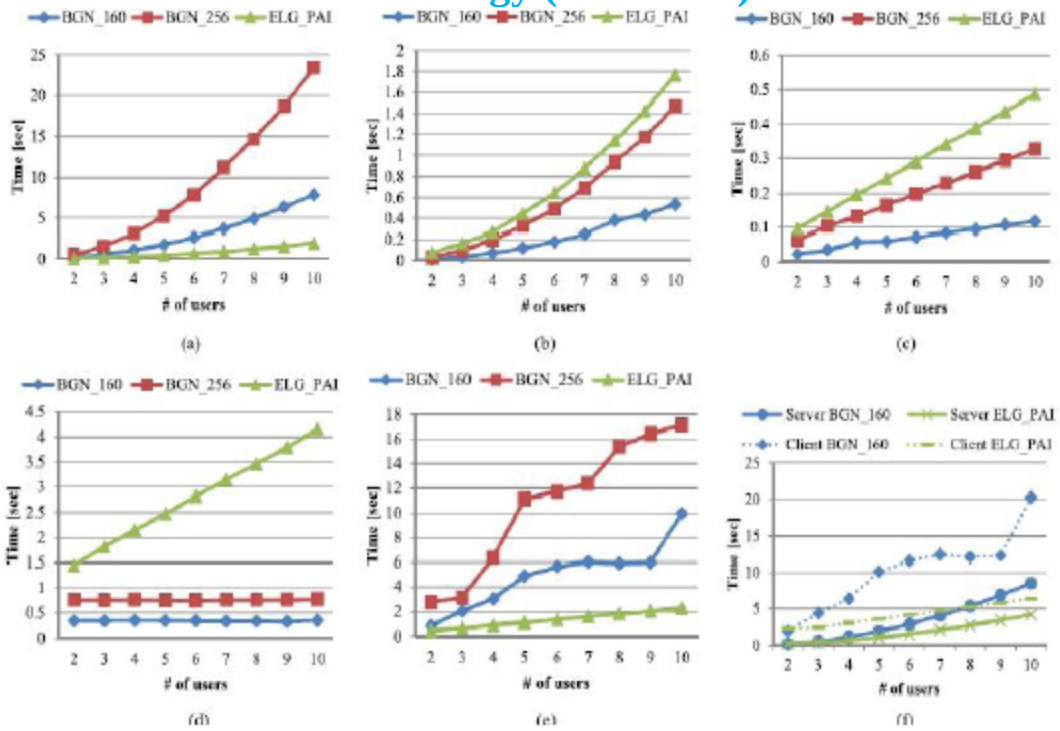


Fig.4.Performance measurements. (a) LDS distance computations. (b) LDS maximum computations. (c) LDS minimum computations. (d) Client distance computations. (e) Client max/argmin computations. (d) Total client and LDS run times.

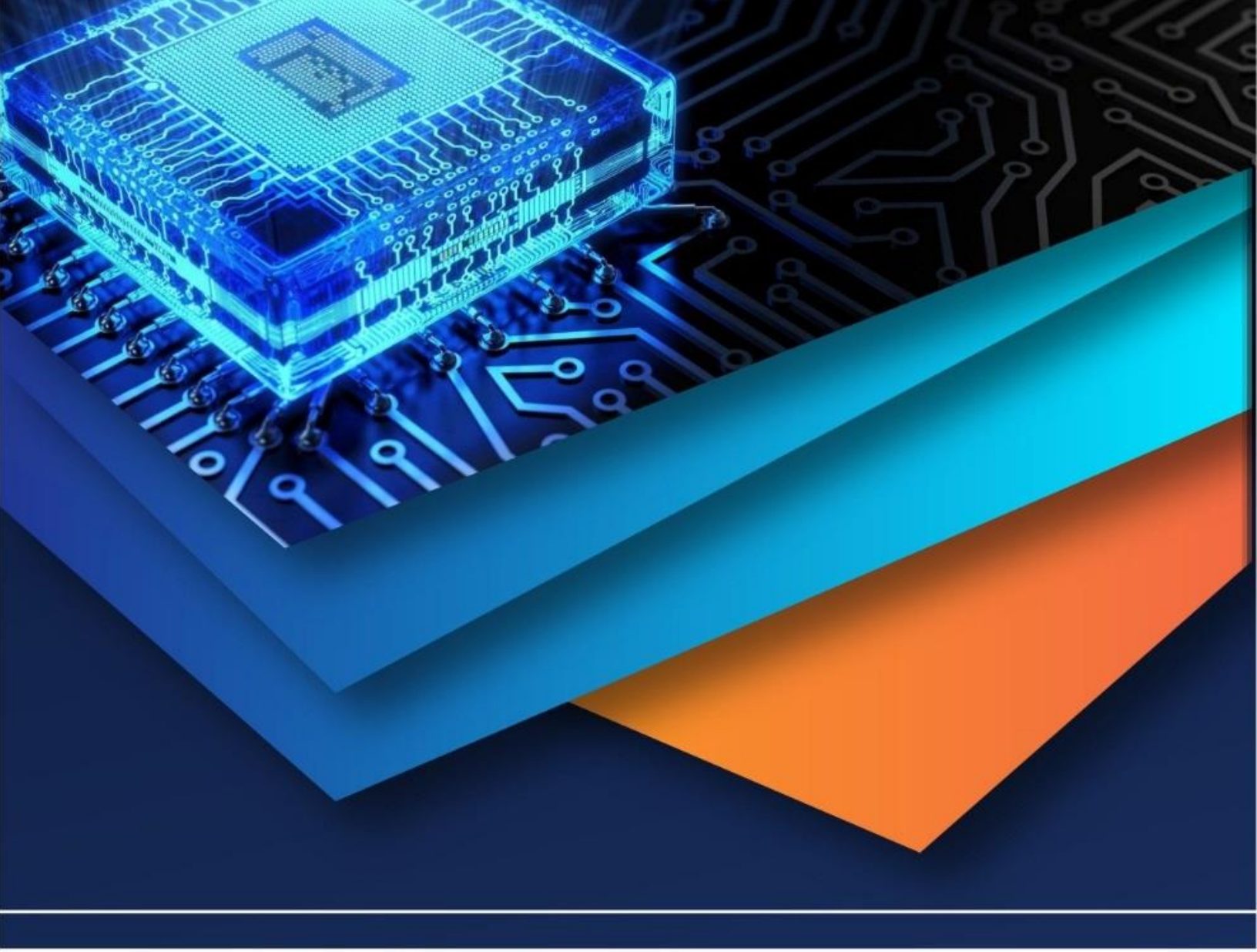
V. CONCLUSION AND FUTURE WORK

We proposed the conservation of security of versatile clients by finding so as to gather the favored areas of the clients the ideal area in FRVP (i.e. Reasonable Rendez-Vous issue). Arrangement of this work depends on the homomorphism elements of cryptosystems which are surely understood. We have executed calculation and execution is assessed on cell phones. We have demonstrated that the execution assessed continuously is acknowledged generally in view of powerful conservation of security. Finally, we demonstrated that the security safeguarding is the critical point in while utilizing the cell phone applications.

REFERENCES

[1] 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 pp. 263–270, (Oct. 2003)
[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,” PersonalUbiquitous Comput., vol. 13, no. 6, pp. 391–399, (2009).
[6] V. Vazirani, Approximation Algorithms. New York, NY, USA: Springer-Verlag, (2001).
[7] I. Bilogrevic, M. Jadliwala, K. Kalkan, J. Hubaux, and I. Aad, “Privacy in mobile computing for location-sharing-based services,” in Proc. 11thInt. Conf. PETS,2011, pp. 77–96.
[8] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K. Tan, “Private queries in location based services: Anonymizers are not necessary,” in Proc. ACMSIGMOD, , pp. 121–132, (2008)
[9] 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)
[10] C.-H. O. Chen et al., “GAnGS: Gather, authenticate ’n group securely,” in Proc. 14th ACM Int. Conf. Mobile Computing Networking, pp. 92–103, (2008)
[11] Y.-H. Lin et al., “SPATE: Small-group PKI-less authenticated trust establishment,” in Proc. 7th Int. Conf. MobiSys, pp. 1–14, (2009)
[12] 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)
[13] O. Goldreich, Foundations of Cryptography:Basic Applications. Cambridge, U.K.: Cambridge Univ. Press, (2004).
[14] K. B. Frikken and M. J. Atallah, “Privacy preserving route planning,” in Proc. ACM WPES, 2004, pp. 8–15.
[15] S.-D. Li and Y.-Q. Dai, “Secure two-party computational geometry,” J. Comput. Sci. Technol., vol. 20, no. 2, pp. 258–263, (2005).

[16] A. Solanas and A. Martínez-Ballesté, "Privacy protection in location based services through a public-key privacy homomorphism," in Proc.4th European Conf.Public Key Infrastructure, Theory and Practice, pp. 362–368, (2007)
[17] 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)
[18] S. Jaiswal and A. Nandi, "Trust no one: A decentralized matching service".
[19] 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)
[20] Facebook Statistics [Online]. Available:http://www.facebook.com/press/info.php?statistics (Nov. 2011).
[21] Facebook Deals [Online]. Available: http://www.facebook.com/deals/ (Nov. 2011)
[22] Let's Meet There [Online]. Available:http://www.letsmeetthere.net/ (2011).
[23] Please Rob Me [Online]. Available: http://pleaserobme.com/ [11] (Nov. 2011)
[24] Microsoft Survey on LBS [Online]. Available: http://go.microsoft.com/?linkid= 9758039, (2011).
[25] Orange Taxi Sharing App [Online]. Available: http://event.orange.com/default/EN/ all/ mondial (Nov. 2011).
[26] UTM Coordinate System [Online]. Available: https://www.education.psu.edu/natureofgeoinfo/c2_p21.html (Nov. 2011)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY