ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Privacy-Preserving Location Sharing Services for Social Networks

K. Saranya[1], S. Sri Harishma[2]

Assistant Professor, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Erode District, India

B.E Student, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Erode District, India

ABSTRACT: The major objective of location based applications involving over online services include location sharing between groups or friends circle, which allows the people to share their locations between entities. The major issues needs to be concentrate with this service is privacy-preserving, because the medium used here to share the location is web, so anyone can easily attack the server and hack the data without the knowledge of the respective individual. The past systems, believe in secured third-party-service-providers, the service providers handle these issues and provide the successful solutions for the Privacy-Preserving Location Sharing Services (PPLSS). However, the user's believeness is again raising an issue, like third-party is again an intermediator to share the location data to recipient; hence the privacy is misleading over here. Several approaches are designed to solve these privacy issues over location sharing between users, all are coming under certain limitations in certain cases. So, a new mechanism is required to solve these issues, called Order-Retrievable Encryption (ORE), which encrypts the transferred or shared location details and pass the hidden text into the recipient. If any attacker or hacker tries to mislead the data they can get only encrypted format location details, which will be securely decrypted in recipient end with proper keys. For all the proposed approach provides more safe and accurate location sharing services between users without any privacy issues.

KEYWORDS: Privacy Preserving, Location Sharing, Privacy-Preserving Location Sharing Services, PPLSS, Order-Retrievable Encryption, ORE.

I. INTRODUCTION

Numerous location based service providers today furnish clients with services identified with their locations by making utilization of GPS empowered cell phones, remote correspondence and spatial database service frameworks. A prevalent kind of such services is for a client to look for purposes of enthusiasm for the region (for instance feasting and shopping). As of late, location based services have been joined with online interpersonal organizations, where client produced, geo-labeled data is shared among individuals who are a piece of an informal organization. A typical usefulness of many existing location based informal communication frameworks is location sharing services that enable clients to find the present location of their companions and tell the clients when a companion is in the region or inside a specific separation, for example Facebook's Places, Foursquare, Google Plus and Loopt. Existing location based long range informal communication frameworks with lo-cation sharing services depend on a focal server which gets location data from all clients in the framework.

The issue with this approach is that the focal server can produce a point by point development profile of every client and that raises security concerns. Existi ng security saving location sharing plans mean to ensure the client location protection against the focal server, however despite everything they enable the server to give the client the vital services. In any case, in some current plans, the focal server still knows the client's inexact location. Different plans require a few messages to be traded not just between the client and the focal server yet additionally specifically between the client and the client's companions, expanding the correspondence cost and making those plans less handy. Different plans just return inexact outcomes, making them less helpful. Distributed frameworks, where clients' gadgets would straight-forwardly impart without a moderate server are naturally hard to realize in cell phone arranges as they regularly influence utilization of NAT (to organize address interpretation), confining direct correspondence between gadgets all the while.

In this system, we propose another encryption thought, called Order-Retrievable Encryption(ORE); another cryptographic protocol that understands our Privacy-Preserving Location Sharing Services (PPLSS) for long range interpersonal communication frameworks. Specifically, our ORE conspire empowers clients to peruse their companions' correct locations inside a specific separation without uncovering any data about their locations to some other clients or an informal communication specialist co-op. The structure of our PPLSS comprises of a database server (which is kept up by the informal communication specialist co-op) and clients. The clients send their location data in scrambled shape to the database server as indicated by our ORE plot.

At the point when a client needs to find his/her companions in the region, the client sign onto the interpersonal interaction framework, sends an location inquiry to the database server, and acquires the asked for location data in scrambled shape in view of our ORE conspire. The client at that point recoups the real location of his/her companions from the scrambled data returned by the database server.

II. PROPOSED APPROACH ATTRIBUTES - A SUMMARY

The key recognizing attributes of the proposed PPLSS-ORE plot are:

(i) Secure Location Protection: PPLSS does not uncover any location data of its clients to a focal server or a busybody, not even a rough location, and does not require any outsider.
(ii) Low Computational and Communication Cost: It enables a client to get the correct location information of his/her companions without requiring direct correspondence between clients or different rounds of correspondence between a client and a server.
(iii) Index Structure: We plan a list structure for our ORE plan to list scrambled locations of a gathering of companions to enhance the productivity of location inquiry preparing.
(iv) Efficient Information Refreshes: Our plan bolsters profoundly powerful location refreshes from singular clients proficiently.

(v) Personalized Protection Inside a Gathering of Companions: Every client can determine a most extreme separation characterizing a customized protection location so t cap just those companions who are inside the locale can find the client.

The basis behind such customized security is that clients might not have any desire to impart their locations to far-away companions as it will not be down to earth or important to impart their location to companions everywhere removes. As to prerequisites, we view the database server as genuine yet inquisitive, to be specific, the database server handles questions, stores information got from clients and sends information to clients who are making inquiries without altering the information. In any case, the database server additionally endeavors to discover the location of clients in the framework. Note that the expression 'privacy preserving' alludes to the location security of clients instead of keeping their characters private. Notwithstanding the security examination of proposed PPLSS, we likewise contrast the execution of our plan with that of the cutting edge cryptography-based plan through analyses. The outcomes demonstrate that proposed PPLSS beats the work regarding both correspondence cost and question accessing execution.

III. PROBLEM SUMMARY

The problem with this approach is that the central server can generate a user (e.g., the location, time and frequency of each place which has been visited by each user). In the existing privacy-preserving location sharing schemes aim to protect the user location, but failed in several circumstances such as third-party server usages, service requirements from service provider, data sharing needs and many more. For that a new encryption and decryption based secured privacy efficient location sharing scheme is required to process further. So, a new crypto based location sharing methodology is introduced called "Order-Retrievable Encryption (ORE)", which realizes the Privacy-Preserving Location Sharing Services (PPLSS) for social networking and web involved systems.

Proposed System Model

PPLSS system comprises of a database server and an arrangement of (versatile) clients. The database server is kept up by an interpersonal interaction specialist co-op. Fig. 1 represents the PPLSS system, in which every client sends his/her location in scrambled shape as per our ORE plan to the database server. At the point when a client needs to question the correct location of his/her companions who are inside a separation determined by the client, the client sends an location inquiry as a private location based range inquiry to the database server.

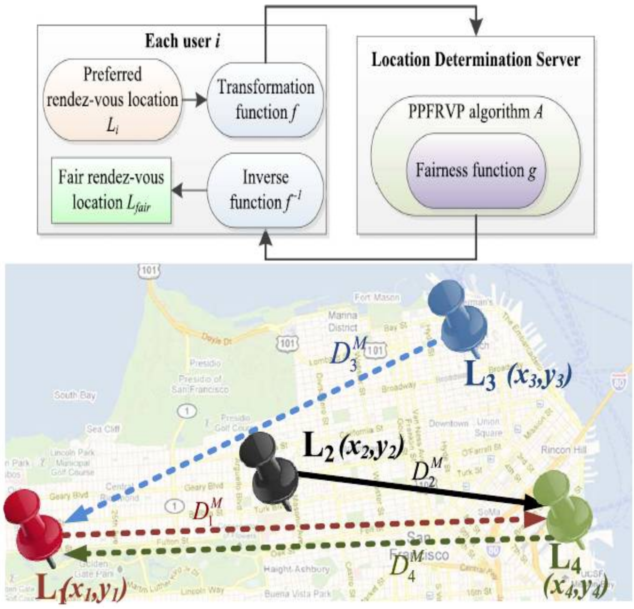

Each user i
Preferred rendez-vous location L_i
Transformation function f
Fair rendez-vous location L_{fair}
Inverse function f^{-1}
Location Determination Server
PPFRVP algorithm A
Fairness function g
D_3^M
L_3 (x_3,y_3)
L_2 (x_2,y_2)
D_2^M
D_1^M
D_4^M
L_4 (x_4,y_4)
$L_1(x_1,y_1)$

Fig.1 Proposed System Model

The database server is outfitted with a protection mindful inquiry processor that can give a correct question reply to the client in view of the client's encoded location and his/her companions' scrambled locations without knowing any location data about the question and the clients. At long last, the client unscrambles the inquiry answer and peruses his/her companions' locations shown on a guide. Note that all client locations and location inquiries are scrambled utilizing our ORE conspire before they are sent to the database server. In PPLSS, we expect that the database server is straightforward yet inquisitive, that is, it takes after our planned convention, yet it endeavors to surmise the client's location. Then again, the client puts stock in his/her companions. The client develops a trusted gathering in which they share their locations through private location questions as per our ORE plot.

IV. LITERATURE SURVEY

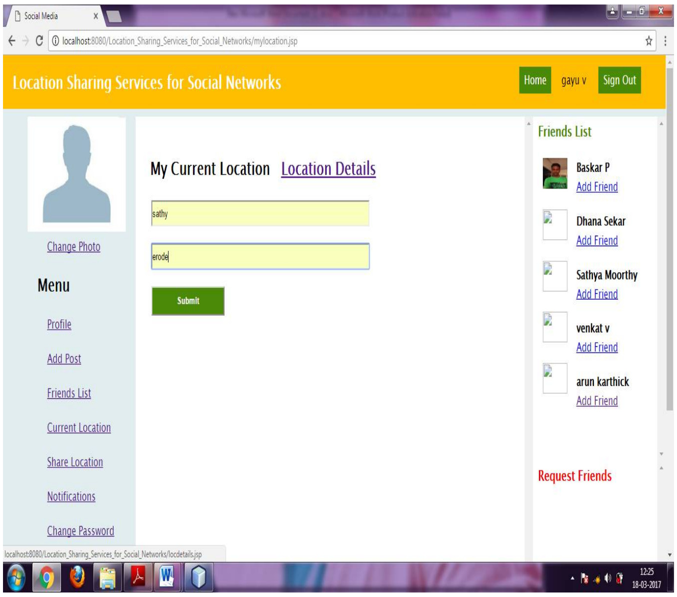
In the year of 2010, the author "E. Toch" proposed a paper titled "Empirical models of privacy in location sharing", in that he described such as: the fast reception of location following and versatile person to person communication innovations raises critical protection challenges. Today our comprehension of individuals' location sharing protection inclinations stays extremely restricted, including how these inclinations are affected by the kind of location GPS beacon or the idea of the locations went by. To address this hole, we sent Locaccino, a portable location sharing framework, in a four week long field think about, where we analyzed the conduct of study members (n=28) who imparted their location to their associates (n=373.) Our outcomes demonstrate that clients seem more open to sharing their essence at locations went to by an extensive and various arrangement of individuals. Our examination likewise shows that individuals who visit a more extensive number of spots have a tendency to likewise be the subject of a more prominent number of solicitations for their locations. After some time these same individuals have a tendency to likewise develop more modern protection inclinations, reflected by an expansion in time-and location based limitations. We finish up by examining the suggestions our discoveries.

In the year of 2010, the authors "L. Siksnys, J. R. Thomsen, S. Saltenis, and M. L. Yiu" proposed a paper titled "Private and flexible proximity detection in mobile social networks", in that they described such as: a security mindful vicinity discovery benefit decides whether two versatile clients are near each other without expecting them to uncover their correct locations. Existing proposition for such administrations give frail security, give low precision ensures, acquire high correspondence expenses, or need adaptability in client inclinations. We address these inadequacies with a customer server answer for nearness recognition, in light of scrambled, multi-level segments of the spatial location. Our administration advises a client if any companion clients enter the client's predetermined territory of intrigue, called the region district. This location, as opposed to related work, can be of any shape and can be adaptably changed on the fly. Encryption and visually impaired assessment on the server guarantees solid protection, while low correspondence costs are accomplished by a versatile location refresh approach. Trial comes about demonstrate that the adaptable usefulness of the proposed arrangement is furnished with low correspondence cost.

In the year of 2012, the authors "S. Triukose, S. Ardon, A. Mahanti, and A. Seth" proposed a paper titled "Geoloca ting ip addresses in cellular data networks", in that they described such as: Cell phones associated with cell systems are progressively being utilized to get to Internet-based administrations. Utilizing information gathered from cell phones running a famous location based application, we look at IP address assignment in cell information systems, with accentuation on understanding the pertinence of IP-based geolocation methods. Our dataset has GPS-based location information for around 29,000 cell organize appointed IP addresses in 50 distinct nations. Utilizing this dataset, we give bits of knowledge into the worldwide sending of cell systems. For example, we find that Network Address Translation (NAT) is ordinary in cell systems. We additionally discover a few occasions of administration separation with administrators appointing open IP delivers to a few gadgets and private IP delivers to different gadgets. We likewise assess the blunder of geolocation databases while deciding the position of the cell phones, and find that the mistake is at least 100km for around 70% of our estimations. Further, there is potential for mistakes at the size of between nation and between mainland separations.

V. EXPERIMENTAL RESULTS

The following figure illustrates the current location detail creation of the proposed system.



localhost:8080/Location_Sharing_Services_for_Social_Networks/mylocation.jsp

My Current Location

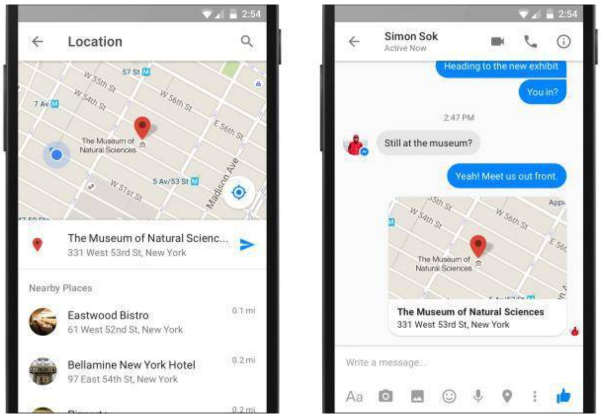
sathy

erode

localhost:8080/Location_Sharing_Services_for_Social_Networks/locdetails.jsp

Fig.2 Location Details Creation

The following figure illustrates the location details sharing scenario.



The Museum of Natural Scienc...
331 West 53rd St, New York

Nearby Places

Eastwood Bistro 0.1 mi
61 West 52nd St, New York

Bellamine New York Hotel 0.2 mi
97 East 54th St, New York

Simon Sok
Active Now

Heading to the new exhibit

You in?

2:47 PM

Still at the museum?

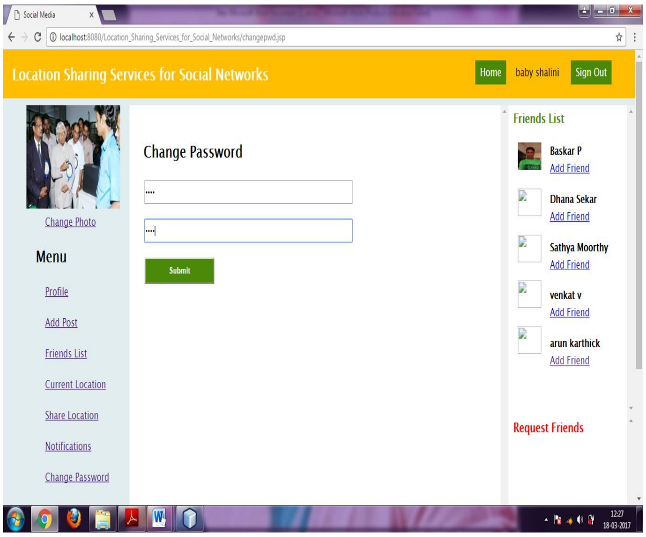
Yeah! Meet us out front.

The Museum of Natural Sciences
331 West 53rd St, New York

Write a message...

Fig.3 Location Sharing Scenario

The following figure illustrates the password changing facility of the proposed system.



localhost:8080/Location_Sharing_Services_for_Social_Networks/changepwd.jsp

Location Sharing Services for Social Networks

Change Password

....

....

Baskar P
Dhana Sekar
Sathya Moorthy
venkat v
arun karthick

Fig.4 Change Password

VI. CONCLUSION

In this system, we present an Order-Retrievable Encryption (ORE) plot; another encryption idea for Privacy-Preserving Location Sharing Services (PPLSS) in long range interpersonal communication applications. Metal is intended to answer location questions that enable a client to see the correct location of his/her companions inside a client indicated remove without uncovering any location data about the client and his/her companions to the database server and some other clients in the framework. The recognizing qualities of ORE contrasted with existing calculations are that ORE gives secure location protection, accomplishes low correspondence and computational cost, and backings dynamic location refreshes. To enhance inquiry handling efficiency, we propose a tree-like file structure for our ORE conspire (ORE-Index) to encourage go seeks over the encoded locations of a gathering of companions. What's more, a customized protection location plot is proposed to additionally enhance client security inside a gathering of companions by empowering a client to indicate a greatest separation up to which his/her companions are permitted to find the client. We additionally perform investigations to assess ORE and ORE-Index and demonstrate that their execution is greatly improved contrasted with the cutting edge cryptography-based method intended for spatial questions.

REFERENCES

[1] S. Consolvo et al., “Location disclosure to social relat ions: Why, when, & what people want to share,” in Proceedings of the ACM Conference on Human Factors in Computing Systems, 2005.

[2] C.-Y. Chow, M. F. Mokbel, and W. G. Aref, “Casper*: Query p rocessing for location services without compromising privacy,” ACM Transactions on Database Systems, vol. 34, no. 4, pp. 1–48, 2009.

[3] M. Gruteser and D. Grunwald, “Anonymous usage of locatio n-based services through spatial and temporal cloaking,” in Proceedings of the ACM International Conference on Mobile Systems, Applications, and Services, 2003.

[4] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, “The new casper: Query processing for location services withoutcompromising privacy,” in Proceedings of the International Conference on Very Large Data Bases, 2006.

[5] T. Wang and L. Liu, “Privacy-aware mobile services over road networks,” in Proceedings of the International Conference on Very Large Data Bases, 2009.

[6] L. Siksnys, J. R. Thomsen, S. Saltenis, and M. L. Yiu, “Pr ivate and flexible proximity detection in mobile social networks,” in Proceedings of the International Conference on Mobile Data Management, 2010.

[7] L. Siksnys, J. R. Thomsen, S. Saltenis, M. L. Yiu, and O. Andersen, “A location privacy aware friend locator,” in Proceedings of the International Symposium on Spatial and Temporal Databases, 2009.

[8] S. Mascetti, C. Bettini, and D. Freni, “Longitude: Cent ralized privacy-preserving computation of users' proximity,” in the International Workshop on Secure Data Management, 2009.

[9] S. Triukose, S. Ardon, A. Mahanti, and A. Seth, “Geoloca ting ip addresses in cellular data networks,” in Passive and Active Measurement, ser. Lecture Notes in Computer Science, 2012, vol. 7192, pp. 158–167.

[10] M. L. Yiu, G. Ghinita, C. S. Jensen, and P. Kalnis, “Enabl ing search services on outsourced private spatial data,” The International Journal on Very Large Data Bases, vol. 19, no. 3, pp. 363–384, 2010.

[11] O. Goldreich, Foundations of Cryptography, volume I, Basic Tools. Cambridge University Press, 2007.

[12] B. Kaliski, “TWIRL and RSA key size,” 2003, CryptoBytes Technical Newsletter, http://www.rsa.com/rsalabs/node.asp?id=2004.

[13] W. K. Wong, D. W.-L. Cheung, B. Kao, and N. Mamoulis, “Sec ure kNN computation on encrypted databases,” in Proceedings of the ACM International Conference on Management of Data, 2009.

[14] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Order-pr eserving en-cryption for numeric data,” in Proceedings of the ACM International Conference on Management of Data, 2004.

[15] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, “Orde r-preserving symmetric encryption,” in Eurocrypt, 2009.

[16] “Specification for the advanced encryption standard (A ES),” Federal Information Processing Standards Publication 197, 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[17] C. Boyd and A. Mathuria, Protocols for Authentication and Key Estab-lishment. Springer-Verlag, 2003.

[18] IEEE, P1363 - 2000: Standard Specifications For Public Key Cryptog ra-phy, 2000.