INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 6, Issue 1 JAN 2017

To Building and Enhance the User Location Privacy in Geo Social Networking Applications

[1]ALLA RUPAVANI, [2]T.SUBBA REDDY

[1]M. Tech Student, Department of CS,Nalanda Institute Of Engineering &Technology, Village Kantepudi, MandalSattenapalli, District Guntur, Andhra Pradesh, India

[2]Assistant Professor, Department of CS,Nalanda Institute Of Engineering &Technology, Village Kantepudi, MandalSattenapalli, District Guntur, Andhra Pradesh, India

***Abstract*—Using geo-social applications, such as four square, lots of individuals interact with their surroundings through their friends and their recommendations. Recently privacy is very important issue in our everyday life. We tend to should get to take care of our data. However this can be impossible when, generally due to busy schedule we tend to can't beware of our data. So, we tend to planned to create an application of mobile, preserving location privacy System victimization cloud. Our system provides location data. Our application provides easy way to secure our location data. Silent options of our protective location privacy system are to provide security to location, offer primary resolution to preserve specific location data, and supply friend's locations. We tend to additionally offer privacy. This system or application is most helpful in emergency cases. With the assistance of this method friends will check location of the user and consistent with he will meet with that specific user. During this paper we tend to compare the different the various location privacy settings which will be introduced in geo social applications and different strategies that are currently adopted to provide security to the users.**

***Index Terms*--Location Based Service Area, Location Privacy, Location Based Social Applications Coordinate Transformation;**

I. INTRODUCTION

Wireless Geo social networking is a sort of social networking in that geographic services and capabilities such as geo coding (location) and geo tagging (metadata) are used to change further social dynamics. For mobile social networks , texted location information or mobile chase will change location primarily based services to enrich social networking .User submitted location data or geo location techniques, these kind of data will allow social networks to attach and coordinate users with people or events having same interest area. It is a recognized fact that the evolution of non-public communication devices results in serious issues about the location privacy problems. In response to these problems, throughout last decade several Location-Privacy Protection Mechanisms (LPPMs) have been planned. The assessment and comparison remains problematic as a result of the absence of a systematic technique to quantify the problems. Several services do not need to verify distance-based queries among random pairs of users, however solely between the chums inquisitive about every other's data and locations. Thus, partition will be done on location data primarily based on

users social groups, and then perform transformations on the situation coordinates before storing them on untrusted servers. A user should recognize the transformation keys of all users' friends, allowing transforming query into the virtual system that users friends uses. Transformations of coordinates preserve distance metrics, permitting an application server to perform each purpose and nearest -neighbor queries properly on transformed data the transformation is secure, in that transformed values cannot be simply related to real-1 world locations without a secret, that is only available to the members of the grouping.

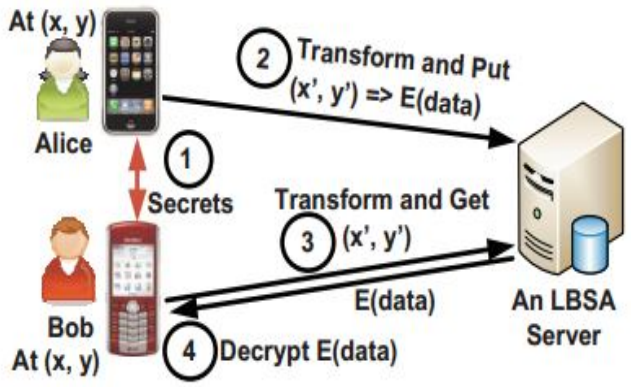

Figure 1: Architecture of Design System

Finally, transformations are efficient, and incur minimal overhead on the LBSAs. The applications built on LocX light-weight and suitable for running on today's mobile devices. Now days, the geo social applications have come terribly near a typical man. Currently these applications are being used for different functions such as social recommendations. It is terribly likely that within the future these applications are going to be the first source of data. however with the growth of technology, the risk of privacy concerning personal information has additionally enhanced. And these applications are useless while not ensuring privacy to its user as studies have indicated that users can express terribly robust concern concerning privacy to their personal information. So, would like to adopt a design method for reliable access of these applications as per the present need and demand of the user. while not adequate location protection, however, these systems will be simply exploited, In this paper, we tend to introduce, a technique that provides location secrecy without adding complexity into query results.

II. RELATED WORK

Privacy protection has recently received extended attention in location primarily based services. an oversized variety of location duration algorithms have been planned for protective the location privacy of mobile users. By considering the scenario wherever different location-based query requests are incessantly issued by mobile users whereas they are moving. The system shows that most of the existing k-anonymity location cloaking algorithms are involved with snapshots user locations only and cannot effectively prevent location dependent attacks when users' locations are continuously updated. Therefore, adopting each the location k-anonymity and cloaking granularity as privacy metrics, a new progressive clique-based cloaking algorithm, referred to as IClique Cloak, is used to defend against location-dependent attacks. The most plans is to incrementally maintain greatest cliques required for location cloaking in an undirected graph that takes into thought the result of continuous location updates. Thus, a qualified clique can be quickly recognized and used to generate the cloaked region once a replacement request comes. The efficiency and effectiveness of the planned IClique-Cloak algorithm are valid by a series of rigorously designed experiments. The experimental results additionally show that the value paid for defending against location dependent attacks is small. The second class is location transformation, that uses transformed location coordinates to preserve user location privacy. One

delicate issue in process nearest neighbor queries with this approach is to accurately notice all the real neighbors. Blind analysis using Hilbert Curves, sadly, will only notice approximate neighbors. To find real nationals, previous work either keeps the proximity of transformed locations to actual locations or incrementally processes nearest -neighbor queries, or requires trusted third parties to perform location transformation between clients and LBSA servers. metropolis a framework in that users entertain anonymous location-based services. Urban center consists of two main components; the location anonymizer that blurs the users' exact location into cloaked spatial regions and also the privacy aware query processor that is responsible on providing location-based services based on the cloaked spatial regions. whereas the location anonymizer is implemented as a complete application, the privacy-aware query processor is embedded into PLACE (a research prototype for location-based database servers).

III. FRAME WORK

To address the challenge in this paper we tend to propose Locx (short for location to index mapping), a novel approach to achieving user privacy whereas maintaining full accuracy in location based mostly social applications (LBSAs from here onwards). Our insight is that several services do not would like to resolve distance based queries between arbitrary pairs of users, however only between friends interested in every other's locations and data. so we will portion location data based on user's social teams, so perform transformations on the location coordinates before storing them on un trusted servers. A user is aware of the transformations keys of all her friends permitting her to transform her query into the virtual coordinate system that her friends use. But the transformation is secure; therein the transformed values cannot be simply related to universe locations without a secret that is only accessible to the members of the grouping. This makes the appliance built on LocX light-weight and appropriate for running on today's mobile devices. Disadvantages: wishing on heavy-weight cryptology or non-public data retrieval (PIR) techniques. Advantages: within the context of databases, recent systems projected running info queries on encrypted information (stored on untrusted servers), exploitation heavy-weight hemimorphy or uneven cryptography schemes. These approaches are appropriate for abstraction information outsourcing or information mining eventualities wherever the information are static and square measure in hand by restricted range of users The project ensuring distributed information sharing and security in automaton; cloud is to. when uploading data on cloud this project can maintain all the records regarding user who have used the data additionally bundling of the file with its information and accessing that data or location by getting that particular key & through that we will preserve our location is that the scope of the system.

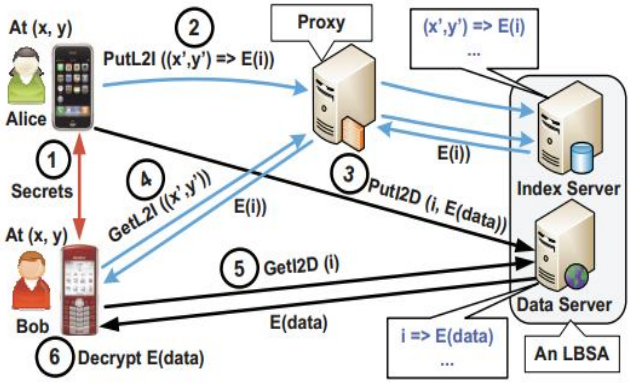

Figure 1: Architecture of Proposed System

Location coordinates refer to the line of longitude, latitude pairs related to real-world locations. A pair of coordinates is returned from a GPS, and is used to associate information with a location. Location information or location data refers to such information

related to a location. For instance, once reviews (and referral purpose details) are written for a given restaurant, the reviews are the situation information related to the restaurant's location coordinates. System and attacker Model during this paper, we tend to assume that the businesses that give LBSA services manage the servers. Users store their information on the servers to get the service. the companies are responsible for faithfully storing this information, and providing access to all or any the data a user ought to have access to. The companies will get incentives via displaying ads, or charging users some usage fees. In our offender model, we tend to assume that the attacker has access to the LBSA servers. This aggressor could be a worker of the corporate running the service or associate outsider that compromises the servers. The aggressor might even be an oppressive regime or a government that obtains information from the providers via subpoenas. As a result, in our model, the offender will access all the information hold on the servers, and may additionally monitor that user device is accessing that items of data on the servers. Our goal is to style a system that preserves the situation privacy of users during this setting. We tend to assume that the attacker does not perform any attacks on the consistency or integrity of data on the servers, however aims only to find out users' location data. Finally, like all previous social systems we tend to assume that the chums of a user are sure and do not interact with the servers in breaking the user's privacy. LocX builds on high of the essential design, and introduces two new mechanisms to overcome its limitations. First, in LocX, we tend to split the mapping between the situation and its information into two pairs: a mapping from the transformed location to an encrypted index (calledL2I), and a mapping from the index to the encrypted location information (calledI2D). This rending helps in creating our system efficient. Second, users store and retrieve the L2Is via untrusted proxies. This redirection of data via proxies, along with rending, considerably improves privacy in LocX. For efficiency, I2Ds are not proxies, yet privacy is preserved.

IV. EXPERIMENTAL RESULTS

In our experiments, network owner is register the any number of usersafter successfully registering the users and issue the keys for the registered users after keys assign to the users those keys are stored in database after that registered user login into the system registered user add the review means add the location name, longitude value add the latitude value and also we can add the review means tasty food after successfully adding the review, the location details (location name, latitude & longitude values) will be stored at index server and reviews will be stored at data server and add the review details other registered user aftersuccessfully adding the review details user can view the review to view the review user need to enter the secret key of other user to entering the secret key user can also check the nearest friends and also view the distance between the specific user. In that proposed system we are using two server's first one is Index server and second one is Data server the registered user data will be stored in this two servers to shown in below screens

We can observe thattwo data servers like Index data server and server data server the user data will be stored in this two servers based on that we can improve the performance of the system also we can maintain the user privacy and also to share the data secure way with low cost when compare to existing protocols.

V.CONCLUSION

Hence we tend to conclude that the description of paradigm implementation, design and LocX analysis that could be a system for building location-based social applications (LBSAs) whereas protective user location privacy. LocX provides location privacy for registered users while not injecting insecurity or errors into the system, and does not rely on any trusted servers or components. LocX may be a new approach to provide users location privacy whereas maintaining overall efficiency of a system, by leveraging the social data-sharing property of the target applications. In LocX, user will efficiently transform and store all their locations shared with the server and encode all location data stored on the server using affordable symmetric keys. Only friends having right keys are able to query and decode a user's data. LocX introduces many mechanisms to realize each privacy and efficiency. It additionally analyzes their privacy properties. Using analysis, based on each synthetic and real-world LBSA traces, LocX adds little computational and communication overhead to existing systems. LocX prototype runs efficiently on mobile phones.

REFERENCES

[1] M. Motani, V. Srinivasan, and P. S. Nuggehalli, "Peoplenet: engineeringa wireless virtual social network," inProc. ofMobiCom, 2005.

[2] M. Hendrickson, "The state of location-based social networking," 2008.

[3] P. Mohan, V. N. Padmanabhan, and R. Ramjee, "Nericell: rich monitoring ofroad and traffic conditions using mobile smartphones," inProc.OfSenSys, 2008.

[4] G. Ananthanarayanan, L. Ravindranath, and C. A.Thekkath, "Combine: leveraging the power of wireless peers throughcollaborative downloading," inProc. OfMobiSys, 2007.

[5] M. Siegler, "Foodspotting is a location-based game that will make yourmouth water," http://techcrunch.com/2010/03/04/foodspotting/.http: //www.scvngr.com.

[6] B. Schilit, J. Hong, and M. Gruteser, "Wireless location privacy protection," Computer, vol. 36, no. 12, pp. 135–137, 2003.

[7] F. Grace, "Stalker Victims Should Check for GPS," Feb. 2003,www.cbsnews.com.

[8] DailyNews, "How cell phone helpedcops nail key murder suspect secret'pings' that gave bouncer away," Mar. 2006.

[9] "Police: Thieves robbed homes based on facebook,social media sites," WMUR News,

September 2010,http://www.wmur.com/r/24943582/detail.html.

[10] M. Gruteser and D. Grunwald, “Anonymous usage of location-basedservices through spatial and temporal cloaking,” in Proc. of Mobisys,2003.

[11] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, “The new casper: A privacyaware location-based database server,” inICDE, 2007.

[12] B. Gedik and L. Liu, “Location privacy in mobile systems: A personalized anonymization model,” in Proc. of ICDCS, 2005.

[13] T. Jiang, H. J. Wang, and Y.-C. Hu, “Preserving location privacy inwireless lans,” inProc. ofMobiSys, 2007.

[14] P. Kalnis, K. Mouratidis, and D. Papadias, “Preventinglocation-based identity inference in anonymous spatial queries,”TKDE,2007.

[15] S. Papadopoulos, S. Bakiras, and D.Papadias, “Nearest neighbor searchwith strong location privacy,”PVLDB, 2010.