Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 3, March 2015, pg.188 – 200

RESEARCH ARTICLE

SAFE GUARDING SPOT PRIVACY WITH GEO-SOCIAL APPLICATIONS

[1]Prudhvi V, [2]Mahendra Reddy Y

[1]M.Tech Student, Department of Computer Science & Engineering, Gokula Krishna College of Engineering, Sullurpet under JNT University , Ananthapur, Andhra Pradesh, India

[2]Associate Professor, Department of Computer Science & Engineering, Gokula Krishna college of Engineering, Sullurpet under JNT University, Ananthapur, Andhra Pradesh,, India

1st prudv410@gmail.com, 2nd mahe.yella@gmail.com

Abstract: Using geo-social applications, like FourSquare, millions of people connect to their own surroundings via their own pals along with their own referrals. Without adequate privateness safeguard, nevertheless, these techniques might be easily abused, at the. gary the gadget guy., for you to course users as well as targeted them with regard to residence breach. On this paper, we bring in LocX, any fresh alternative that provides significantly-improved position privateness with no adding doubt directly into problem outcomes as well as relying on robust assumptions regarding server protection. The critical perception is usually to use protected user-specific, distance-preserving organize transformations to all or any position information distributed to the actual server. Your pals of the individual reveal this particular user's secrets and techniques to allow them to use identical change for better. This will give most position

inquiries to become evaluated appropriately from the server, although our privateness systems promise that will computers are unable to notice as well as infer your position information from the transformed information as well as from the information gain access to. Most of us display that will LocX supplies privateness actually next to a strong foe style, along with we employ prototype measurements showing it supplies privateness along with almost no functionality cost, making it made for today's mobile devices.

Index Terms—Spot privacy, security, Android Mobile, location-based social applications, location transformation, efficiency, Effectiveness.

1. INTRODUCTION

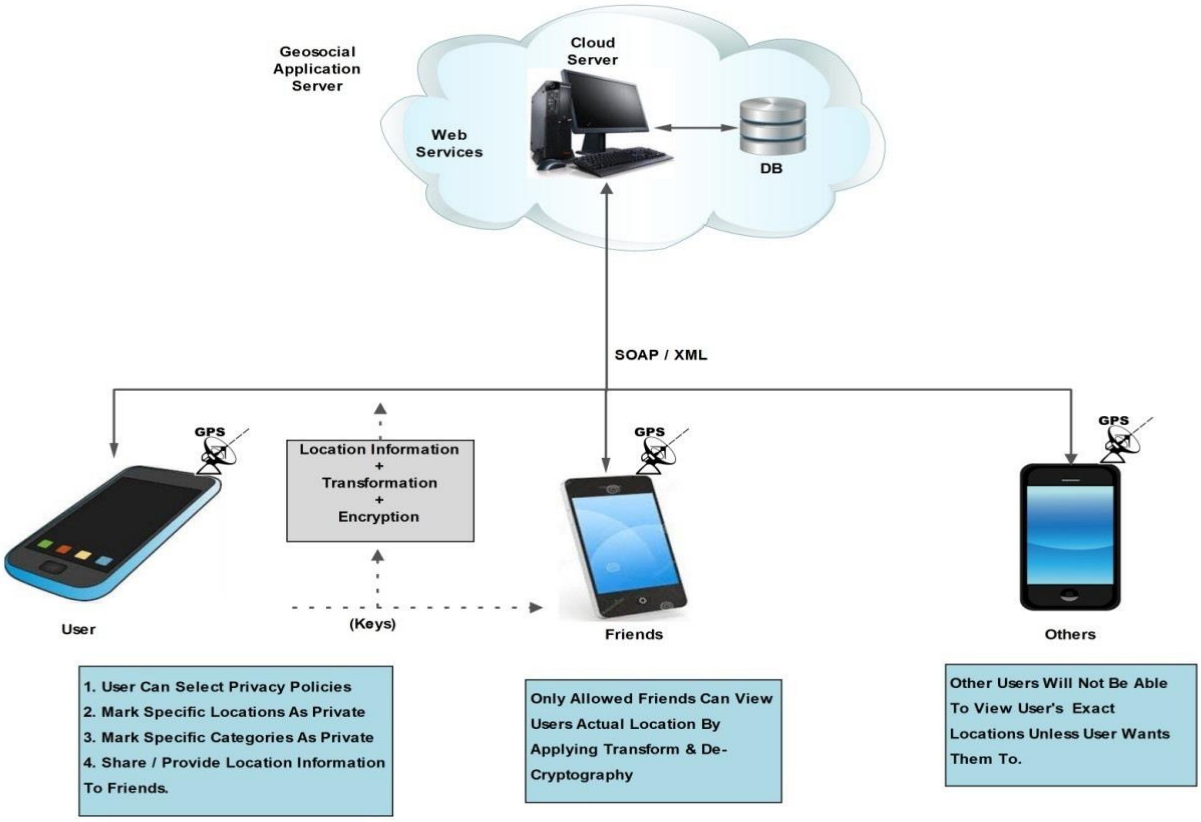
WITH billions in downloads and annual revenue, smartphone applications offered by Apple iTunes and Android are quickly becoming the dominant computing platform for today's user applications. Within these markets, a new wave of geo-social applications is fully exploiting GPS location services to provide a "social" interface to the physical world. Examples of popular social applications include social rendezvous, local friend recommendations for dining and shopping , as well as collaborative network services and games. The explosive popularity of mobile social networks such as SCVNGR and FourSquare (3 million new users in 1 year) likely indicate that in the future, social recommendations will be our primary source of information about our surroundings.

Unfortunately, this new functionality comes with significantly increased risks to personal privacy. Geosocial applications operate on fine-grain, time-stamped location information. For current services with minimal privacy mechanisms, these data can be used to infer a user's detailed activities, or to track and predict the user's daily movements. In fact, there are numerous real-world examples where the unauthorized use of location information has been misused for economic gain , physical stalking , and to gather legal evidence. Even more disturbing, it seems that less than a week after Facebook turned on their popular "Places" feature for tracking users' locations, such location data were already used by thieves to plan home invasions. Clearly,

mobile social networks of tomorrow require stronger privacy properties than the open-to-all policies available today.

Existing systems have mainly taken three approaches to improving user privacy in geosocial systems: 1) introducing uncertainty or error into location data, 2) relying on trusted servers or intermediaries to apply anonymization to user identities and private data , and 3) relying on heavy-weight cryptographic or private information retrieval (PIR) techniques. None of them, however, have proven successful on current application platforms. Techniques using the first approach fall short because they require both users and application providers to introduce uncertainty into their data, which degrades the quality of application results returned to the user. In this approach, there is a fundamental tradeoff between the amount of error introduced into the time or location domain, and the amount of privacy granted to the user. Users dislike the loss of accuracy in results, and application providers have a natural disincentive to hide user data from themselves, which reduces their ability to monetize the data. The second approach relies on the trusted proxies or servers in the system to protect user privacy. This is a risky assumption, since private data can be exposed by either software bugs and configuration errors at the trusted servers or by malicious administrators. Finally, relying on heavy-weight cryptographic mechanisms to obtain provable privacy guarantees are too expensive to deploy on mobile devices , and even on the servers in answering ueries such as nearestneighbor and range queries.

2. ARCHITECTURE:



3. RELATED WORK

Preceding work on privateness generally location-based solutions (LBS). You will discover generally 3 families of proposals about offering area privateness generally LBSs that do definitely not especially goal sociable applications. 1st is spatial in addition to temporary cloaking when rough area in addition to time is provided for the actual server instead of the particular prices. The pure intuition here is that this stops correct detection on the destinations on the customers, or maybe skins the user between ok different customers (called k-anonymity , thereby boosts privateness. This approach, nonetheless, affects the actual exactness in addition to timeliness on the tendencies through the server, in addition to most importantly, there are several basic attacks about these things that will still bust end user privateness. Pseudonyms in addition to hushed occasions are usually different things to attain cloaking, in which with system identifiers are usually changed generally, in addition to files just isn't transported regarding very

long times with typical time intervals. This, nonetheless, significantly affects operation in addition to disconnects customers. The main element distinction among these solutions in addition to our own work is they depend upon dependable intermediaries, or maybe dependable machines, in addition to show rough realworld area towards machines with plain-text. Inside LocX, we all don't trust any intermediaries or maybe machines. For the beneficial aspect, these solutions are more normal in addition to, for this reason, can apply at many location-based solutions, even though LocX centers generally on the appearing geo-social applications. Your second group is area alteration, which usually utilizes developed area coordinates in order to preserve end user area privateness. Just one simple difficulty with finalizing nearest-neighbor queries using this type of approach is to effectively uncover each of the genuine neighbors. Shades assessment utilizing Hilbert Shape , however, can simply uncover rough neighbors. In order to find genuine neighbors, prior work either will keep the actual proximity connected with developed destinations in order to precise destinations in addition to incrementally operations nearest-neighbor queries or maybe demands dependable finally celebrations to do area alteration among customers in addition to LBSA machines. In contrast, LocX will not trust any finally get together and also the developed destinations aren't linked to precise destinations. Nonetheless, our bodies continues to be ready to look for the precise neighbors, and is particularly resistant in opposition to attacks depending on checking constant queries .

The next class of work relies upon Private information Collection (PIR) to deliver sturdy area privateness. The performance, even though much better by employing specific hardwares , continues to be very much more painful than the rest of the solutions, so it is unclear currently when this method might be employed with genuine LBSs.

Preceding work on privateness with geo-social solutions For sure kinds of geo-social solutions, including good friend checking solutions to find out if the good friend is neighborhood, a few current proposals accomplish provable area privateness utilizing high-priced cryptographic methods including safe two get together calculation. Inside form a contrast, LocX simply utilizes low-priced symmetric encryption in addition to pseudorandom quantity machines. The closest work in order to LocX is Longitude , which usually additionally transforms destinations coordinates in order to avoid disclosure towards machines. Nonetheless, with Longitude, the actual techniques regarding alteration are usually managed among each set of pals to be able to make it possible for customers in order to selectively disclose destinations in order to pals. Just

as, Longitude can let a new end user show your ex area in order to only a subset connected with your ex pals. Inside form a contrast, LocX has a simpler danger type in which all pals can entry a new user's facts and therefore the number of techniques of which customers ought to preserve is just 1 every end user. LocX can still accomplish area in addition to end user unlinkability. In addition, LocX provide far more flexible geo-social solutions, including area centered sociable recommendations, pointers, while others, than just good friend checking as with the above mentioned before work. Confidential conversation systems. These types of systems, as well as Tor , offer anonymity in order to customers through community pastime. Just one may consult, then, the reason why utilizing Tor in order to anonymously way files in order to LBSA machines just isn't ample? This approach usually offer privateness because the server simply views area files and not the actual personality on the end user powering of which files. Nonetheless, current analysis has revealed of which covering the actual personality on the customers on it's own just isn't ample to guard area privateness. Perhaps when Tor is used, it is possible on an attacker using entry towards area files in order to violate our own privateness in addition to unlinkability demands. As an example, utilizing anonymized GPS UNIT footprints collected through the machines, it's been shown of which users' property in addition to workplace destinations, and in some cases end user personality might be taken. LocX protects in opposition to this sort of attacks in addition to complies with all our own demands. Programs about untrusted machines. Within the context connected with listings, current systems suggested operating databases queries about encrypted files (stored about untrusted servers), utilizing heavy-weight homomorphic or maybe asymmetric encryption schemes.

These types of solutions are usually suited to spatial files entrusting or maybe files exploration cases where the files is static and is particularly held by simply minimal amount of customers. Nonetheless they are usually a lesser amount of suited to LBSAs, where the files is active in addition to particular, thereby cannot be encrypted underneath 1 solution key. Within the context connected with area in addition to sociable applications, Persona in addition to Adeona additionally counted about encrypting all files located about untrusted machines to guard end user privateness. Persona aimed at privateness with social networks, in addition to Adeona aimed at privateness with system checking systems in which there is zero files sharing between customers. Making use of Persona's things in order to LBSAs specifically would encrypt all area coordinates, generating LBSAs unable to process nearest-neighbor queries.

Yet when area just isn't encrypted, attacks utilizing anonymized GPS UNIT footprints, mentioned previously, can realize success, generating Persona lack of to guard area privateness. Similarly, Adeona is helpful for a new end user in order to get back her own files, and not the results from your ex pals. Our own additions enhance these systems. Some methods with these documents will help LocX too, e. grams. Persona's method of partition files distributed to pals in to fine-grained groups, in addition to Adeona's hardware-assisted solutions in order to accelerate crypto finalizing.

4. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

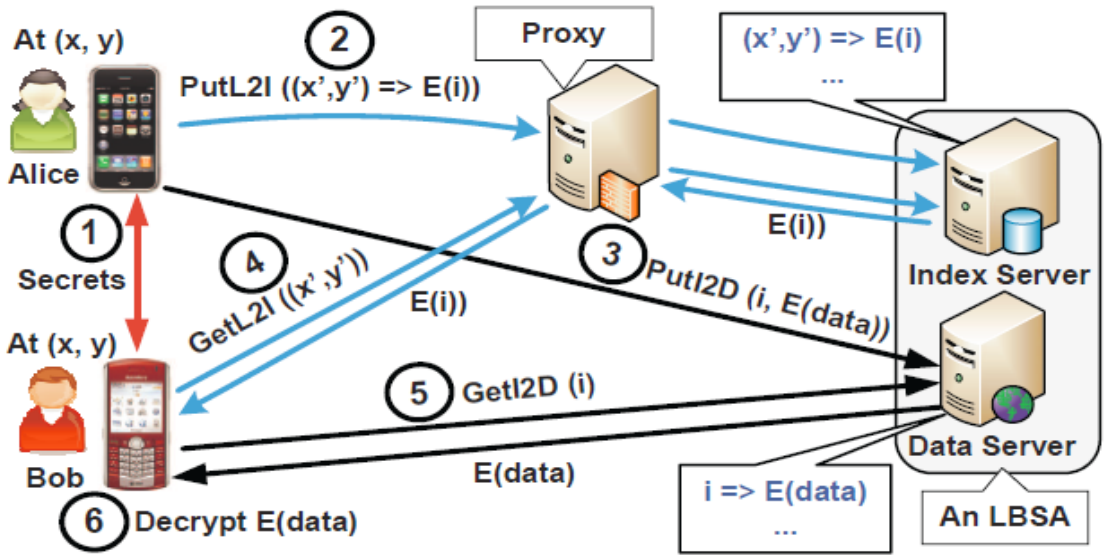
The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Algorithm:

Filtering-and-Verification Algorithm:

This motivates us to follow the *filtering-and-verification* paradigm for the uncertain aggregate query computation. Particularly, in the *filtering phase*, effective and efficient filtering techniques will be applied to *prune* or *validate* the points. The algorithm consists of two phases. In the *filtering* phase for each entry e of RS to be processed, we do not need to further process e if it is *pruned* or *validated* by the filter F. We say an entry e is *pruned* (*validated*) if the filter can claim $P_{fall}(p, \gamma) < \theta$ ($P_{fall}(p, \gamma) \geq \theta$) for any point p within e_{mbb}. The counter cn is increased by |e| if e is *validated* where |e| denotes the aggregate value of e (i.e., the number of data points in e). Otherwise, the point p associated with e is a candidate point if e corresponds to a data entry and all child entries of e are put into the queue for further processing if e is an intermediate entry. The *filtering phase* terminates when the queue is empty. In the *verification* phase candidate points are *verified* by the integral calculations.

4.1. LOCX: Loc X builds on top of the basic design, and introduces two new mechanisms to overcome its limitations. First, in Loc X, we split the mapping between the location and its data into two pairs: a mapping from the transformed *location to anencrypted index* (called **L2I**), and a mapping from the *index to the encrypted location data* (called **I2D**). This splitting helps in making our system efficient. Second, users store and retrieve the L2Is via *untrusted proxies*. This redirection of data via proxies, together with splitting, significantly improves privacy in LocX. For efficiency, I2Ds are not proxied, yet privacy is preserved.



4.2.Proxying L2Is for location privacy:

Users store their L2Ison the index server via *untrusted proxies*. These proxies can be any of the following: Planet Lab nodes, corporate NAT sand email servers in a user's work places, a user's home and office desktops or laptops, or Tor [34] nodes. We only need a one-hop indirection between the user and the index server. These diverse types of proxies provide tremendous flexibility in proxying L2Is, thus a user can store her L2Is via different proxies without restricting herself to a single proxy. Furthermore, compromising these proxies by an attacker does not break users' location privacy, as (a) the proxies also only see transformed location coordinates and hence do not learn the users' real locations, and (b) due to the noise added toL2Is (described later). To simplify the description, for now, we assume that the proxies

are non-malicious and do not collude with the index server. But we will later describe our solution in detail to even defend against colluding, malicious proxies. With this high-level overview, we now describe our solution to store and query data on the servers in detail. We also explain the challenges we faced, and the tradeoffs we made in makingour solution secure and efficient.

4.3. Storing L2I on the index server:

First consider storing L2I on the index server. This transformation preserves the distances between points1, so circular range and nearest neighbor queries for a friend's location data can be processed in the same way on transformed coordinates as on real-world coordinates. Then the user generates a random index (i) using her random number generator and encrypts it with her symmetric key to obtain at the transformed coordinate on the index server via a proxy. The L2I is small in size and is application independent, as it always contains the coordinates and an encrypted random index. Thus the over head due to proxying is very small.

4.3.Storing I2Ds on the data server:

The user can directly storeI2Ds (location data) on the data server. This is both secure and efficient.

1) This is secure because the data server only sees the index stored by the user and the corresponding encrypted blob of data. In the worst case, the data server can link all the different indices to the same user device, and then link these indices to the retrieving user's device. But this only reveals that one user is interested in another user's data, but not any information about the location of the users, or the content of the I2Ds, or the real-world sites to which the data in the encrypted blob corresponds to.

2) The content of I2Dis application dependent. For example, a location-based video or photo sharing service might share multiple MBs of data at each location. Since this data is not proxied, LocX still maintains the efficiency of today's systems.

5. INPUT DESIGN AND OUTPUT DESIGN

5.1.INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:'

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

5.2. OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2. Select methods for presenting information.

3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

6. FUTURE ENHANCEMENT

The project ensuring distributed data sharing and security in android & cloud is to. After uploading data on cloud this project will maintain all the records about user who have used the data. Also bundling of the file with its information and accessing that data or location by getting that particular key & through that we can preserve our location is the scope of the system.

Using evaluation based on both synthetic and real-world LBSA traces, we find that LocX adds little computational and communication overhead to existing systems. Our LocX prototype runs efficiently even on resource constrained mobile phones. Overall, we believe that LocX takes a big step toward making location privacy practical for a large class of emerging geosocial applications.

7. CONCLUSION:

This paper describes the design, prototype implementation, and evaluation of LocX, a system for building locationbased social applications (LBSAs) while preserving user location privacy. LocX provides location privacy for users without injecting uncertainty or errors into the system, and does not rely on any trusted servers or components

locx takes a novel approach to provide location privacy while maintaining overall system efficiency, by leveraging puttaswamy et al.: preserving location privacy in geosocial applications. ideal amount of noise necessary to protect users in brightkite, with increase in the number of malicious proxies. the social data-sharing property of the target applications. In LocX, users efficiently transform all their locations shared with the server and encrypt all location data stored on the server using inexpensive symmetric keys. Only friends with the right keys can query and decrypt a user's data. We introduce several mechanisms to achieve both privacy and efficiency in this process, and analyze their privacy properties.

REFERENCES:

1. Beginning ASP.NET 4: in C# and VB by *Imar Spaanjaars*.
2. ASP.NET 4 Unleashed by *Stephen Walther*.
3. Programming ASP.NET 3.5 *by Jesse Liberty, Dan Maharry, Dan Hurwitz.*
4. Beginning ASP.NET 3.5 in C# 2008: From Novice to Professional, Second Edition by *Matthew MacDonald.*
5. Amazon Web Services (AWS), Online at http://aws. amazon.com.
6. Google App Engine, Online at http://code.google.com/appengine/.
7. Microsoft Azure, http://www.microsoft.com/azure/.
8. A. Agrawal et al. Ws-bpel extension for people (bpel4people), version 1.0., 2007.
9. M. Amend et al. Web services human task (ws-humantask), version 1.0., 2007.
10. D. Brabham. Crowdsourcing as a model for problem solving: An introduction and cases.
11. P. K. Agarwal, S.-W. Cheng, Y. Tao, and K. Yi. Indexing uncertain data. In *Proc. Symp. Principles of Database Systems (PODS)*, 2009.
12. C. Aggarwal and P. Yu. On high dimensional indexing of uncertain data. In *Proc. Intl Conf. Data Eng. (ICDE)*, 2008.
13. C. Bohm, M. Gruber, P. Kunath, A. Pryakhin, and M. Schubert. Prover: Probabilistic video retrieval using the gauss-tree. In *Proc. Intl Conf. Data Eng. (ICDE)*, 2007.
14. C. Bohm, A. Pryakhin, and M. Schubert. Probabilistic ranking queries on gaussians. In *Proc. Intl Conf. Scientific and Statistical Database Management (SSDBM)*, 2006.
15. V. Bryant. *Metric Spaces: Iteration and Application*. Cambridge University Press, 1996.

Sites Referred:

http://www.asp.net.com

http://www.dotnetspider.com/

http://www.almaden.ibm.com/software/quest/Resources/

http://www.computer.org/publications/dlib

http://www.developerfusion.com/

