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. 4, April 2015, pg.200 – 202

SURVEY ARTICLE

A Survey To Safeguard Privacy And Security On Mobile Devices Through Optimal Algorithms

Ruhi Dubey[1], Prof. Garima Singh[2]

[1]Department of Computer Science and Engineering, WCEM, Nagpur, India

[2]Department of Computer Science and Engineering, WCEM, Nagpur, India

[1] ruhidubey30@gmail.com; [2] garima11makhija21@gmail.com

Abstract— The rapid proliferation of smart phone technology in urban communities has enabled mobile users to utilize context aware-services on their devices. Today's highly interconnected urban population is increasingly dependent on these gadgets to organize and plan their daily lives. They often rely on the preferred locations according to their demands thus lacking security. In this paper we propose algorithms which provide privacy and security to user contents and requirements. Users may not want to reveal their actual locations to a third party which are not trustworthy. We perform a thorough privacy estimation and optimization for determining an optimal meeting location for a group of users. Our solutions are based on the homomorphic properties of well-known cryptosystems.

Keywords— location based services, security, control plane locating, self-reported positioning, mobile devices

I. INTRODUCTION

Today's highly interconnected urban population is increasingly dependent on gadgets to organize and plan their daily lives. People buy mobile devices for various purposes.

One such issue is to find an appropriate meeting location between groups of users. This issue is vulnerable to online threats. In this paper, we safeguard the privacy and security of end users through optimal solutions. We perform a thorough privacy evaluation by formally quantifying privacy-loss of the proposed approaches. By means of a targeted user-study, we attempt to get an insight into the privacy-awareness of users in location based services and the usability of the proposed solutions. Location-based Services (LBS), for example, are used by millions of mobile subscribers every day to obtain location-specific information.

Location-based services (LBS) are a general class of computer program-level services that use location data to control features. As such LBS is an information service and has a number of uses in social networking today as an entertainment service, which is accessible with mobile devices through the mobile network and which uses information on the geographical position of the mobile device. This has become more and more important with the expansion of the smart phone and tablet markets as well. LBS are used in a variety of contexts, such as health, indoor object search, entertainment, work, personal life, etc.LBS include services to identify a location of a person or object, such as discovering the nearest banking cash machine (*a.k.a.* ATM) or the whereabouts of a friend or employee. LBS include parcel tracking and vehicle tracking services. LBS can include mobile commerce when taking the form of coupons or advertising directed at customers based on their current location. They include personalized weather services and even location-based games. They are an example of telecommunication convergence.

II. EXISTING TECHNIQUES

Igor Bilogrevic, Murtuza Jadliwala proposed privacy-preserving algorithms for determining an optimal meeting location for a group of users. They perform a thorough privacy evaluation by formally quantifying privacy-loss of the proposed approaches.

Wei Xin presented a LocSafe method, a "missed-connections" service is used which grantees based on RFID technology, in order to prove an encounter sharing among users in the past. LocSafe is comprised of three parts: RFID Tags, LE Collectors, and social service provider. We use RFID technology to detect encounters, and use attribute-based encryption and broadcast encryption to establish trust and protect users, privacy. We evaluate LocSafe by an study of "missed-connections "problems and analysis of system implementation.

As per the author Wei Li, Wei Jiao, in this paper, Location-Based Service(LBS) combined with mobile devices and internet become more and more popular, and are widely used in traffic navigation, intelligent logistics and the point of interest query. However, most users worry about their privacy when using the LBS because they should provide their accurate location and query content to the untrustworthy server. This paper analyses the query association attack model for the continuous query in mobile LBS.

As prescribed by Ramaiah Y.G, Kumari G.V, this paper covers an encryption scheme "homomorphic" used for the data security. In order to prevent the leakage of information from IT companies, this paper uses homomorphism algorithm which has data encryption technique.

As per the author P. Golle and K. Partridge, existing fully homomorphic schemes are not truly practical due to their high computational complexities and huge message expansions. Targeting the construction of a homomorphic encryption scheme that is implementable for at least certain class of applications, this paper proposes a Somewhat Homomorphic public key encryption scheme, which can be viewed as a variant of the scheme devised by Van Dijk et.al, extended to larger message space. The proposed scheme is compact, semantically secure with significantly smaller public key, and is capable of encrypting integer plaintexts rather than single bits, with comparatively lower message expansion and computational complexities.

III. PROPOSED WORK

We perform a thorough privacy evaluation by formally quantifying privacy-loss of the proposed approaches. By means of a targeted user-study, we attempt to get an insight into the privacy-awareness of users in location based services and the usability of the proposed solutions. Proposed system will employee following methodologies for successful completion of system:

1. Finding the distance between multiple geo-points,
2. Finding the centroid of virtually created geo-polygon,
3. Finding the preferred location from mapping server,
4. Stealth Geo-Synchronization.

Google launched the Google Maps API in June 2005 to allow developers to integrate Google Maps into their websites. It is a free service, and currently does not contain ads, but Google states in their terms of use that they reserve the right to display ads in the future. By using the Google Maps API, it is possible to embed Google Maps site into an external website, on to which site specific data can be overlaid.

Proposed system aims at finding the preferred and central location for user group using geo-point calculation and mapping technology. In near future the system can be implemented over different mobile device and mobile platform and it can be developed as plug in for group chat applications like what's App and Hike messenger.

IV. CONCLUSION

Thus in this survey paper we explain various optimal techniques to provide security and privacy to a group of users trying to meet at a specific location. In a recent report on location-based data, we analyze the opportunities emerging from this new local-mobile paradigm, examine how location-enabled mobile ads have generated excitement, look at how location-based feature have boosted engagement for apps, explain how local data can connect hundreds of thousands of small and medium-sized businesses to the mobile economy, and demystify some of the underlying technologies and privacy issues. Location-based features: have turned out to be great for boosting engagement on apps. Facebook, Google, Yelp, Instagram, Groupon, Twitter and dozens of other popular apps offer location-enabled features. These mobile properties, and many others, have moved beyond the "check-in" concept, which in any case never really caught on with users. They may still offer the ability to "check-in," but are also trying to be more imaginative with location-based notifications and location-aware services. By the means of implementing the proposed system we are trying to assist user groups in different ways.

REFERENCES

[1] Igor Bilogrevic, MurtuzaJadliwala, VishakJoneja, kubra Kalka, Jean-Pierre Hubaux and ImadAad, " Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices". IEEE Transaction on Information Forensics and Security, Vol. 9,No.7,JULY 2014.
[2] Wei Xin, Cong Tang, TaoYang, Huiping Sun, Zhong Chen, "Towards Privacy-Preserving RFID-Based Location–Based Services". International Conference on Fuzzy Systems and Knowledge Discovery.
[3] Wei Li, Wei Jiao, Guangye Li, "A Location Privacy Preserving Algorithm for Mobile LBS. IEEE CCIS 2012. from mobile sources," in *Proc. IEEE/WIC Int. Conf. WI*, Oct. 2003,pp. 263–270.
[4] Ramaiah Y.G, Kumari G.V, "Efficient public key Homomorphic Encryption over integer plaintexts".
[5] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in *Proc. 7th Int. Conf. Pervasive Computing*, 2009, pp. 390–397.

