ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

NOVEL TECHNIQUES TO SAFEGUARD PRIVACY AND SECURITY ON MOBILE DEVICES THROUGH OPTIMAL ALGORITHMS

Ruhi Dubey*, Prof. Garima Singh
* Department of Computer Science and Engineering, WCEM, Nagpur, India
Department of Computer Science and Engineering, WCEM, Nagpur, India

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: privacy, LBS, preferred location, optimal solutions, geopoint.

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. LBS privacy issues arise in that context, and are documented below:

Control plane locating

Sometimes referred to as positioning, with control plane locating the service provider gets the location based on the radio signal delay of the closest cell-phone towers (for phones without GPS features) which can be quite slow as it uses the 'voice control' channel. In the UK, networks do not use trilateration; LBS services use a single base station, with a "radius" of inaccuracy, to determine a phone's location. This technique was the basis of the E-911 mandate and is still used to locate cellphones as a safety measure. Newer phones and PDAs typically have an integrated A-GPS chip.

GSM localization
GSM localization is the second option. Finding the location of a mobile device in relation to its cell site is another way to find out the location of an object or a person. It relies on various means of multilateration of the signal from cell sites serving a mobile phone. The geographical position of the device is found out through various techniques like time difference of arrival (TDOA) or Enhanced Observed Time Difference (E-OTD).

Self-reported positioning
A low cost alternative to using location technology to track the player, is to not track at all. This has been referred to as "self-reported positioning". It was used in the mixed reality game called Uncle Roy All Around You in 2003 and considered for use in the Augmented reality games in 2006. Instead of tracking technologies, players were given a map which they could pan around and subsequently mark their location upon. With the rise of location-based networking, this is more commonly known as a user "check-in".

LITERATURE SURVEY

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. . They address the privacy issue in LSBSs by focusing on a perticuler problem called Fair Rendez-Vous Point (FRVP) problem. It given a set of user location preferences, the FRVP problem help to determine a location among the proposed ones such that the greatest distance between this location and all other users' locations is minimized.

Rinku Dewri and Ramakrishna Thurimella proposed a user-centric location based service architecture where a user can observe the impact of location inaccuracy on the service before deciding the geo coordinates to use in a query. They construct a search application based on user-centric location-based service architecture where a user can observe the impact of location inaccuracy on the service accuracy.

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.

RESEARCH METHODOLOGY

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

Great Circle Algorithm
The greatcircle or orthodromic distance is the shortest distance between two points on the surface of a sphere, measured along the surface of the sphere (as opposed to a straight line through the sphere's interior). The distance between two points in Euclidean space is the length of a straight line between them, but on the sphere there are no straight lines. In non-Euclidean geometry, straight lines are replaced with geodesics. Geodesics on the sphere are the great circles (circles on the sphere whose centers coincide with the center of the sphere).

Through any two points on a sphere which are not directly opposite each other, there is a unique great circle. The two points separate the great circle into two arcs. The length of the shorter arc is the great-circle distance between the points. A great circle endowed with such a distance is the Riemannian circle.

Between two points which are directly opposite each other, called antipodal points, there are infinitely many great circles, but all great circle arcs between antipodal points have the same length, i.e. half the circumference of the circle, or , where r is the radius of the sphere.

Polygon Mid-Point Formulae
In geometry, the midpoint polygon of a polygon P is the polygon whose verrtices are the midpoints of the edges of P. It is sometimes called the Kasner polygon after Edward, who termed it the inscribed polygon "for brevity".

Triangle
The midpoint polygon of a triangle is called the medial triangle. It shares the same centroid and medians with triangle. The perimeter of the medial triangle equals the semiperimeter of the original triangle, and the area is one quarter of the area of the original triangle. Theorthocenter of the medial triangle coincides with the circumcenter of the original triangle.

Quadrilateral
The midpoint polygon of a quadrilateral is a parallelogram called its Varignon parallelogram. If the quadrilateral is simple, the area of the parallelogram is one half the area of the original quadrilateral. The perimeter of the parallelogram equals the sum of the diagonals of the original quadrilateral.

Google Map API
After the success of reverse-engineered mashups such as chicagocrime.org and housingmaps.com, 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. Although initially only a JavaScriptAPI, the Maps API was expanded to include an API for Adobe Flash applications (but this has been deprecated), a service for retrieving static map images, and web services for performing geocoding, generating driving directions, and obtaining elevation profiles. Over 1,000,000] web sites use the Google Maps API, making it the most heavily used web application development API.

The Google Maps API is free for commercial use, provided that the site on which it is being used is publicly accessible and does not charge for access, and is not generating more than 25 000 map accesses a day.Sites that do not meet these requirements can purchase the Google Maps API for Business. The success of the Google Maps API has spawned a number of competing alternatives, including the Yahoo! Maps API, Bing Maps Platform, MapQuest Development Platform, and OpenLayers. Each design decision will be presented and rationalized, and sufficient detail will be given to allow the reader to examine each element in its entirety.

Summary: The geographic midpoint is calculated by finding the center of gravity for the locations in the 'Your Places' list. The latitude and longitude for each location is converted into Cartesian (x,y,z) coordinates. The x, y, and z coordinates are then multiplied by the weighting factor and added together. A line can be drawn from the center of the

earth out to this new x, y, z coordinate, and the point where the line intersects the surface of the earth is the geographic midpoint. This surface point is converted into the latitude and longitude for the midpoint.

RESULTS

The experimental results are presented to show that the proposed methods can achieve promising performance in background subtraction and foreground object extraction. This system detects and tracks the moving objects exactly and removed the shadow efficiently. In this approach, the background scene is modeled using a set of background image frames.

Getting maps from geopoint

Fig. 4.1:Getting map from Geo-Point

Showing map by loction

Fig. 4.2:Showing map by location

Showing route between cities

Fig. 4.3: Showing route between cities

Showing route between areas

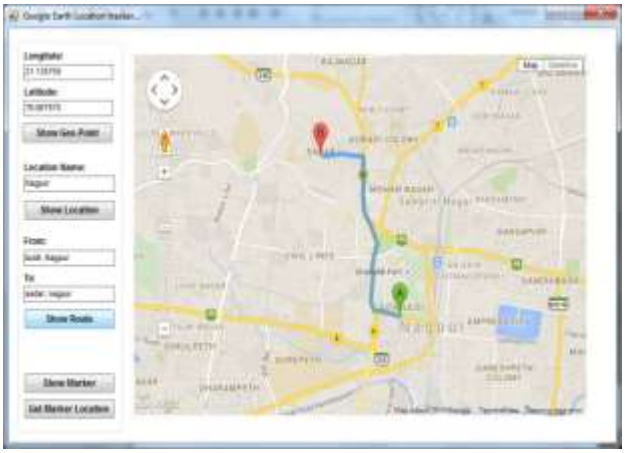

Fig. 4.4: Showing route between areas

Placing and showing the markers

Fig. 4.5: Placing & showing the markers

In this way we fetch the address of each location for the person who want to take the meeting in unknown place.

Fetching address of location

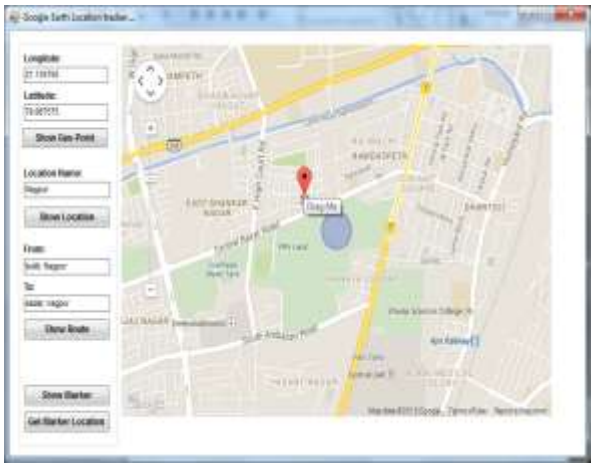

Fig. 4.6: Fetching address of location

Drawing polygon

Fig 4.7: Drawing a Polygon

Getting centroid

Fig. 4.8: Getting Centroid of Polygon

After finding the centroid location one user will select preferred location and that location will send to all another user with route calculation.

CONCLUSION

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 rather user group in different way.

REFRENCES

[1] (2011, Nov.). Facebook Statistics [Online]. Available: http://www.facebook.com/press/info.php?statistics
[2] (2011, Nov.). Facebook Deals [Online]. Available: http://www.facebook.com/deals/
[3] E. 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, Oct. 2003, pp. 263–270.
[4] (2011). Microsoft Survey on LBS [Online]. Available: http://go.microsoft.com/?linkid=9758039
[5] (2011, Nov.). Orange Taxi Sharing App [Online]. Available: http://event.orange.com/default/EN/all/mondial

[6] (2011). Let's Meet There [Online]. Available: http://www.letsmeetthere.net/
[7] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in Proc. 7th Int. Conf. Pervasive Computing, 2009, pp. 390–397.