International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 7, Issue 1, No 1, 2019. ISSN: 2348-6600
Reference ID: IJCS-351 PAGE NO: 2359-2366

LOCATION BASED INFORMATION SHARING SYSTEM USING IOT

Dr.E. Punarselvam[1] , S.Gopi[2]

[1] Associate Professor, Department of Information Technology, Muthayammal Engineering College, Rasipuram, Tamilnadu, India.

[2] Assistant Professor, Department of Information Technology, Muthayammal Engineering College, Rasipuram, Tamilnadu, India.

Abstract- The mobile devices have become necessity of our lives. It use mobiles to share information to others. These mobile devices rely on the internet services provided by central ISP (internet service providers) to share information to other devices. But the services provided by internet service providers is not available in all the places and are expensive, have limited bandwidth. Information sharing between the mobile devices using the internet service requires the end device to have internet connection. To address these problems It provide a solution which enables information sharing between mobiles through inter device communication and makes use of information sharing technologies available on the mobile devices. To exhibit the advantages of our solution It are implementing interest based information sharing system in which the user interest will be expressed in small tags called strings. When two mobile devices come in contact they share the contents based on interest of each other.

Keywords: Location-based services, ISP, GPS, Wi-Fi, GPS, GSM, GPRS.

I. INTRODUCTION

Location-based services (LBSs) are one of the most important components in the mobile online social networks (MOSNs). Which provides information and entertainment service based on the geographical position of the mobile device. LBS have experienced explosive growth in recent years, particularly leveraging the fast development of mobile technology and the cloud computing. In LBS, the location of a device, representing one of the most important contextual information about the device and its owner, is exploited to develop innovative and value-added services

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 7, Issue 1, No 1, 2019. ISSN: 2348-6600
Reference ID: IJCS-351 PAGE NO: 2359-2366

to the users' personal context. Many individual, commercial, and enterprise-oriented LBSs are already available and have gained popularity. Various LBS applications have been proposed, such as location-based mobile advertising to mobile phone users. In E-health systems, LBS can also be applied to allow access to patient records outside the hospitals by doctors with location based access technology. There are also many examples of LBS including mobile check-in games like Foursquare, social networks like Loop, and location-enabled applications like Google Maps. Analysts project the revenues for LBS to grow from 2.8 billion in 2010 to hit 10.3 billion by 2015. With the increasing popularity of LBS, the privacy concerns on users' locations have been raised. Because the location tracking capability of mobile devices has been improved greatly, user's personal information such as the position and preference will be leaked and vulnerable to improper use. As a result, it violates user's privacy and impedes the development of various LBS applications.

Mobile information society is developing rapidly as mobile telecommunications moves from second to third generation technology. The Internet and its services are coming to wireless devices. The convergence of content and technology is deepening and the market is being reorganized. Different actors want to preserve their place in the mobile digital economy. Location-based services and personal navigation are parts of mobile multimedia services. Personal navigation is a service concept in which advanced mobile telecommunications allow people find out where they are, where they can find the products and services that they need and how they can get to a destination.

II OBJECTIVE

Privacy is internationally recognized as a fundamental human right. Location aware pervasive computing environments provide the ability to automatically sense, communicate, and process information about a person's location, with a high degree of spatial and temporal precision and accuracy. Location is an especially sensitive type of personal information, and so safeguarding an individual's location privacy has become a key issue for pervasive computing research. The issue of protecting sensitive information about an individual user's location,

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 7, Issue 1, No 1, 2019. ISSN: 2348-6600
Reference ID: IJCS-351 PAGE NO: 2359-2366

at the same time as providing useful location-based services to that user. Our approach focuses on negotiating a balance in the levels of privacy and utility for a location-based service. Thus, in our model an individual may deliberately degrade the quality of information about his or her location in order to protect his or her privacy, a process called obfuscation.

Another category is GPS based tracking system. Global positioning system (GPS) is the most mature and widely used technology in positioning and location tracking. GPS receivers are widely embedded in cell phones, watches, and a various kinds of embedded devices. These devices receive wireless signals from at least four GPS satellites, and calculate positioning data using a triangulation technique. Smart phone is the most popular device, and almost every smart phone equips the GPS module. Previous works have been done on using general devices to coordinate with GPS, Wi-Fi and Cell-Id to provide hybrid positioning. However, general devices are expensive, cumbersome and power consuming. A specialized positioning device should be small, cheap, and low-consumption. In addition, a tracking system should also contains a backend server for real-time data collection. A mobile app is also required for data display and interaction. Considering these requirements, it design a low-consumption IoT framework for location tracking and implement a system for walking sticks as a real-world application on the basis of the framework.

III.PROPOSED SYSTEM

The device embeds with a GPS/GSM/GPRS module, capable of receiving GPS signals, sending and receiving SMS, establishing TCP connection over GPRS. The device generates location data at a set interval.

These location data and other information i.e. device battery information and timestamps will be uploaded to the server over TCP connection. Server will collect and store these data. Server also provides a Restful API for mobile app. Command sent from mobile app to device will also be validated by the server. Mobile app acquires data from server over HTTP requests, sending SMS to control device remotely and calling API provided by server.

Control command includes changing device's frequency of uploading location data, and requesting location data via SMS, etc.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 7, Issue 1, No 1, 2019. ISSN: 2348-6600
Reference ID: IJCS-351 PAGE NO: 2359-2366

3.1 OPTIMIZE RESOURCES

GPS Fleet tracking solutions allow you to monitor your vehicles and get detailed insights on fuel usage, driver behavior, engine idling, etc. in real time.

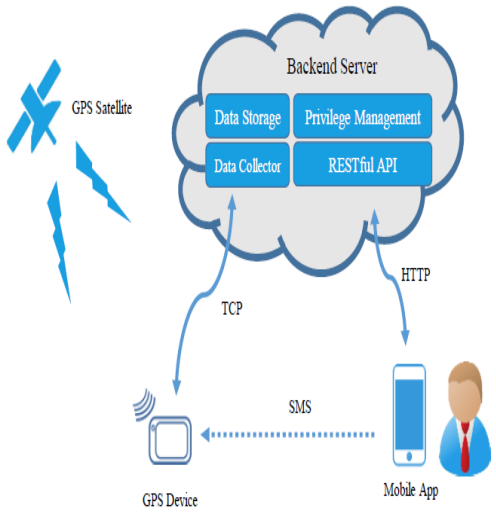
3.2 TRACK YOUR STOLEN OR MISSING PHONE

With the mobile phone GPS tracking service, you are able to find regular updates of the current location of your phone.

3.3 SUPERIOR ROUTE PLANNING

GPS tracking data is identify the routes that save both time and money. Smart route planning will reduce unproductive work and eliminate unnecessary fuel expenses.

Architecture Diagram



3.4 ENHANCED SECURITY PROVIDER MODULE

It observe that the identity of the same querying user is linkable by the location service provider in the friends' location query of previous work. Although multiple fake identities have been inserted for each user in these systems, friends' queries from the same user will be linked because of the same friend set.

The location service provider is able to finally obtain the topological structure of the social network and launch multiple attacks.

It propose a new system by introducing a new architecture with multiple location servers. More specifically, all location information will be stored in each location server. When a request of friends' locations is submitted from a user, this set will be divided into multiple subsets, and each subset will be sent to a location server, respectively.

In this way, friends' location queries from the same user will be different from the point view of each location server with enough high probability. As a result, these queries cannot be linked to the same user, and improved privacy has been achieved in this new system.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 7, Issue 1, No 1, 2019. ISSN: 2348-6600
Reference ID: IJCS-351 PAGE NO: 2359-2366

3.5 LOCATION SHARING MODULE

In the location-sharing system of MOSNs, users communicate with the location service and social network server. The user's location service is provided by LS, and the social network service is provided by SOSN. The users can submit two types of queries, nearby friends' locations and strangers' locations. In general, the location-sharing mechanism consists of three phases, which are described as follows.

(i) User registration. Two kinds of registration are required for users:

(ii) Registration at the social network server

(iii) Registration at location servers. (a) Users are required to register their personal information for the LBS at SOSN. Specifically, they need to provide the information of their profiles and individual preferences, which will be kept by the social network server. (b) Users also need to register their pseudo identity and specified access control policy at the LSs through SOSN in an anonymous way.

(iv) Location updates. Users need to update their location information at the location servers if their locations change. The new location information will be stored and updated at the location servers for location services.

(v) Location query. There are two kinds of queries supported in the system, which are the following.

a) Friends' location query. When a user wants to know his/her nearby friends' current locations, he/she queries the social network service provider and LBS providers and receives the location information of friends whose specified access control setting is satisfied by the querying user.

b) Strangers' location query. When a user wants to get nearby strangers' current locations, he/she queries the social network service provider and LBS providers and receives the location information of someone whose specified access control setting is satisfied by the user.

3.6. IOT NETWORK THREAT MODEL

Different trust assumptions will be defined over the entities involved in the system:

1) The users are assumed to be dishonest and would try to access the location information outside the scope of their access privileges.

2) The social network server is assumed to be "honest-but-curious," i.e., the social

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 7, Issue 1, No 1, 2019. ISSN: 2348-6600
Reference ID: IJCS-351 PAGE NO: 2359-2366

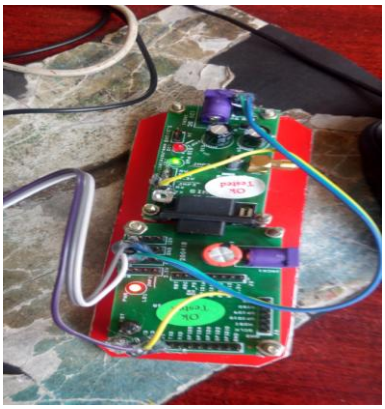
network server will follow our proposed protocol but try to find out as much sensitive information as possible. For example, it may want to extract the users' location information from the interactive communications.

3) The location server is also supposed to be "honest-but-curious." It will also honestly follow our protocols and try to get some users' sensitive information such as the friend list. In other words, the social network server and the location servers are not allowed to collude and get the information that they have not owned individually. This security assumption is also specified in past systems. This assumption is reasonable because it is unlikely that two service providers operated by independent organizations can be controlled by the same adversary.

3.6.1 HARDWARE DEVICE

3.6.2 GPS ANTENNA

3.6.3 GPS SIGNAL



3.6.4 LOCATION TRACKING SIGNAL

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 7, Issue 1, No 1, 2019. ISSN: 2348-6600
Reference ID: IJCS-351 PAGE NO: 2359-2366

4 CONCLUSION

This location based information sharing System has been designed and developed and works properly. It is very efficient; user can easily use this application. Any people can track any mobile location any time using this application. The application is free of cost and does not require any additional device. It have tested in different Android phones and different browsers it works smoothly.

FUTURE ENHANCEMENT

Mobile apps receive GPS location and store into web server database, web application is use to create user profile and location based information in mobile phone's sharing.

REFERENCES

[1] Kevin Fall, "Delay-Tolerant Network Architecture for Challenged Internets", 2003

[2] Marcelo Yannuzzi, Xavier Masip-Bruin "Open issues in Inter domain Routing: a survey", 2005

[3] Wei Gao and Guohong Cao,"User-Centric Data Dissemination in Disruption Tolerant Networks", 2011

[4] Igor Bilogrevica, Kevin Hugueninc, Berker Agirb, Murtuza Jadliwalad, Maria Gazakib, Jean-Pierre Hubauxb, "Machine-Learning Based Approach to Privacy-Aware Information-Sharing in Mobile Social Networks I", 2016

[5] Alvin Cheung, Tyrone Grandison, Christopher Johnson, "Generic Platform for Sharing on Mobile Device", 2007

[6] Igor Bilogrevic, Kevin Huguenin, Berker Agir, "Adaptive Information-Sharing for Privacy-Aware Mobile Social Networks", 2013

[7] Krishna P. N. Puttaswamy and Ben Y. Zhao,"Preserving Privacy in Location-based Mobile Social Applications", 2010

[8] Wayne Jansen, Vlad Korolev, "Location-Based Mechanism for Mobile Device Security", 2009

[9] Ichiro Satoh, "Location Model for Pervasive Computing Environments", 2005

[10] Marco Gruteser, Graham Schelle, Ashish Jain, Rick Han, and Dirk Grunwald, "Privacy-Aware Location Sensor Networks", 2003

[11] Haodong Wang , Bo Sheng, Qun Li, "Privacy-aware routing in sensor networks", 2009

[12] Jingwei Zhang, "Greedy Forwarding for Mobile Social Networks Embedded in Hyperbolic Spaces", 2013

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 7, Issue 1, No 1, 2019. ISSN: 2348-6600
Reference ID: IJCS-351 PAGE NO: 2359-2366

[13] Diego López de Ipiña1, Paulo R. S. Mendonça2, Andy Hopper,"Low-Cost Vision-Based Location System for Ubiquitous Computing", 2002