Design of Secure Location and Message Sharing System for Android Platform

Ramesh Shrestha
College of Computer Science & Technology
Harbin Engineering University
Harbin, P.R.China
helloramesh123@gmail.com

Yao Aihong
College of Computer Science & Technology
Harbin Engineering University
Harbin, P.R.China
yaoaihong@hrbeu.edu.cn

Abstract— **Present android-based location and message sharing system asks to input the personal information which fails to protect the privacy of information, has no centralized database which is causing the problem of data management and portability, and one main drawback is unable to have a secured two way communication between webserver and android based application. And this Android-based Location and Message Sharing System (ALMSS) is proposed for solving above mention problem. The proposed system uses Java programming language for android mobile user application, PHP programming language as webserver, MySQL as external database to store the data, JSON as intermediary between android platform and webserver and uses symmetric cryptography while communicating between android device and webserver which finally assures the protection of information.**

Keywords- Location Sharing, Message Sharing, Android, PHP, MySQL, Webserver

I. INTRODUCTION

Today's age is the world of technologies, where lots of inventions and discoveries have made everyone to rely on the use of latest technology. Knowingly or unknowingly we are taking the benefit of the technology. Today one can share information with others using the communication technology. One can know what is happening in different parts of the world within a click. It is possible due to the development in the internet services through which one can share the information with the rest of the world.

Internet has brought revolution in the field of communication. One can use internet for various purposes depending upon the nature of work. But the main uses of the internet in these days are sharing of information. The main application of internet is web services where internet plays an important role.

Another useful development in the technology is the mobile devices. The use of mobile devices is increasing day-by-day. Many improvements have been made, such as faster processors and better battery life, have enabled notebooks and smartphones to become powerful devices, giving us the ability to completely change the way we work. Today's mobile devices not only comes with the feature of voice communication and sending/receiving messages but also has the features of Internet, Bluetooth, Image capturing, Video recording, GPS facilities and so on. Various smart phones are available in the market, namely Samsung, HTC, Motorola, Apple iPhone, Android, Blackberry products and so on. Among them, Android has been gaining popularity and its market share in the mobile operating system market is rapidly increasing. According to Gartner (2010) [1], Android is poised to become second worldwide mobile operating system in the nearer future.

Using the technology – smart phone and internet, people are sharing information to other people but they are not sure if their information is securely transmitted or not. This paper deals with secure transmission of information with each other.

The main drawbacks with the existing android-based location and message sharing systems are as follows:

1) No centralized database due to which there is a problem in management of data, portability problem, updates as well as backup problems etc.
2) Most of the location based social network asks to input the personal information. All the messages are displayed on the screen which has failed to protect the privacy of information.
3) Lack of server centric privacy control method. No security has been maintained during transfer of information between server and device.
4) Most of the application that are based on GPS technology are storing location in their built in database and are unable to use it externally so that it is difficult to trace the current location of the people where they are.

The main objective of this paper, on the highest level, is to communicate with a PHP server that stores the information sent through the android device in encrypted form and vice-versa which finally establish a secure two way communication between android device and web server. The main highlight of our work is listed below:

1) Connect with the external database MySQL to maintain a centralized database. For achieving this goal, we will use JSON as an intermediary to send the data from android device and PHP to insert that value to the external database MySQL.
2) Interact with the webserver and maintaining security while sharing location and message. For achieving this goal, we will use two approaches, the information sent by the android application is first stored in a database in encrypted form using JSON and PHP as intermediary and decrypt data while extracting from database. And similar process is followed while sending information from webserver to device. All the data are encrypted while sending and key is needed to decrypt this data before reading from the database.

978-1-4673-0089-6/12/$26.00 ©2012 IEEE

3) To find the current location, trace the path and track the people. For achieving this goal, current location is obtained from GPS enabled android device and is sent to webserver and webserver will display location position and path on the web using the feature of Google Map.

This paper is organized as follows: section II introduces some background, including Android Platform, PHP and MySQL, JSON and some security measures taken during location and message sharing, section III describes related works, section IV illustrates the design and operation of ALMSS, experiments are performed on section V, section VI finally draws the conclusion and future works.

II. BACKGROUND

This section presents the background environment for location and message sharing system.

A. GPS Technology

The Global Positioning System (GPS) [2] is a global navigation satellite system deployed by the US Department of Defense and maintained by the US Air Force. GPS is a space based radio navigation system that provides accurate location and timing services to anyone with a GPS receiver.

B. Google Android

The Android Platform is a software stack [3] for mobile devices including an operating system, middleware and key applications. Developers can create applications for the platform using the Android SDK. Applications are written using the Java programming language and run on Dalvik, a custom virtual machine designed for embedded use, which runs on top of a Linux kernel. (Google, 2008) [4].

C. PHP and MySQL

PHP [5] (recursive acronym for *PHP: Hypertext Preprocessor*) is a widely-used open source general-purpose scripting language that is especially suited for web development and can be embedded into HTML. Instead of lots of commands to output HTML (as seen in C or Perl), PHP pages contain HTML with embedded code that does "something". The PHP code is enclosed in special start and end processing instructions <?php and ?> that allow you to jump into and out of "PHP mode."

MySQL [6] is a relational database management system that runs as a server providing multi-user access to a number of databases. It is named after developer Michael Widenius' daughter, My. The SQL phrase stands for Structured Query Language. MySQL is a key part of LAMP (Linux, Apache, MySQL, PHP / Perl / Python), the fast-growing open source enterprise software stack.

D. JSON

JSON (JavaScript Object Notation) [7] is a lightweight data-interchange format. It is easy for humans to read and write. It is easy for machines to parse and generate. It is based on a subset of the JavaScript Programming Language, Standard ECMA-262 3rd Edition - December 1999. JSON is a text format that is completely language independent but uses conventions that are familiar to programmers of the C-family of languages, including C, C++, C#, Java, JavaScript, Perl, Python, and many others.

E. AES (Symmetric Cryptography)

As described in [8], data gets produced, transferred and stored at one or more remote storage servers; it becomes vulnerable to unauthorized disclosures and modifications. So data must be prevented from an unauthorized access. Therefore, for the security issue we have used symmetric cryptography. It provides the integrity as well as the confidentiality of the data. Symmetric encryption techniques [9] works with same key i.e. we will have the same key for both encryption and decryption. Only those who know the key are able to make the message readable. Thus, it is important to make the key only available to those who should have access to the message.

III. RELATED WORKS

The various researches have been done and are going on location based project and in the same ratio various applications have been developed on location-based and message sharing system.

The various locating technology as described in [10] are summarized as follows:

1) GPS: It locates a user through a device that is in communication with a constellation of satellites.
2) Wireless Position: It locates a user using both private and public wifi access point, users can be mapped according to the location of these access point.
3) Cellular Identification: It locates using cellular data of mobile phones.
4) IP Location: It locates users using the IP address of the Internet network.

Among the various location technologies, GPS is the most and accurate way to locate user. It locates a user through a device that has GPS functionality such as mobile phone. Various location sharing applications is gaining popularity due to the growth of the GPS equipped smartphones. With the emergence of the GPS capable mobile, users started to write a small application passing location data to a central server to make their location available to other users [11, 12].

Chandra A, Jain S, Qadeer M A [13], has proposed a location sharing system based on GPS and GPRS using J2ME, PHP and MySQL which gives the user's current location, send this location using SMS and view them on google map. But the applications they have proposed has implementation problem, accuracy problem, have no centralized database as well as some security issue and have no two way communication between webserver and device.

As described in [14], the works are mainly focused on how to handle the location, how to display google map on

android devices and finally about classes and functions used for location services.

The location based service as in [15], has defined two parts: client and server. Client side is developed based on technique: Mobile SVG based JSR226 and JSR179 specification, map slicing, map layering and J2ME. Server side is developed using XML, J2EE and MySQL. This platform provides services of map segment querying, shortest path to destination query by Dijkstra algorithm, bus route query and route navigates.

As described in [16], they have proposed a GPS navigation system which will help to track the friend position, view scenic spots from smart phones and so on. They have performed this work in ASP.NET 2.0 with SQL Server 2005 as database.

Li N, Chen G [17] has compared the various location based online social network and has provided various views in privacy issue. They have also included that most of the location based online social network, ask to give the personal information due to which the privacy is the main issue in all the location based application. They have also added that mobile users have more privacy issues.

IV. DESIGN AND OPERATION

This section describes the system architecture, working principles of the system and various functions used while designing the system.

A. System Architecture

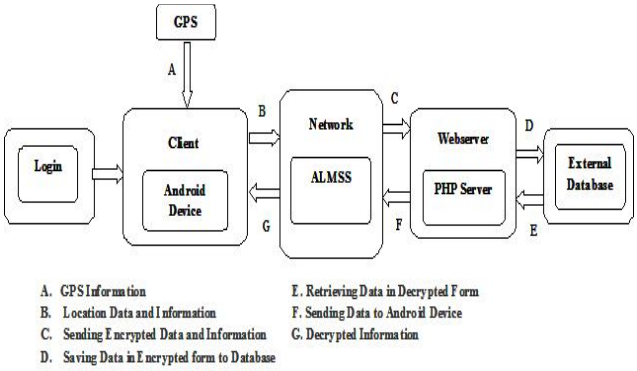

Figure 1. Architecture of the Android-based Location and Message Sharing System

Fig. 1 is a complete architecture of ALMSS. It can be further divided into two parts: User Interface (UI) and Webserver Interface (WI).

B. User Interface

User Interface consists of three modules briefly described as follows:

1) User Login Module

This module is displayed on android device when ALMSS runs. Only the registered user can login using their user id and password. If the username and password fails user will not able to enter into the main interface.

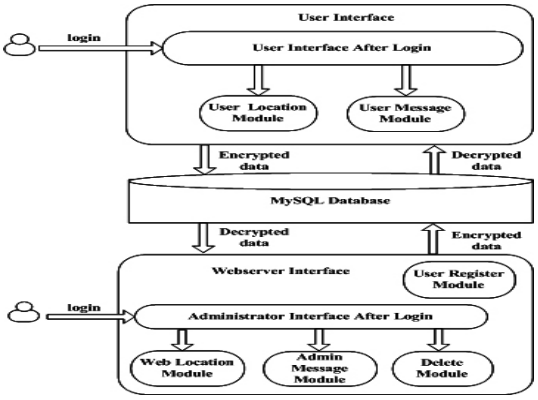

Figure 2. User and Webserver Interface of ALMSS

2) User Location Module

It is divided into two parts: First, Send Location Module to send the current location where user is, nearby historic places, scenic places, and some important places, to database in an encrypted form. When this module is clicked, a window with Google Map is displayed in Android smart phones. With the help of GPS, user location is read and finally encrypted and sent to database. Besides user's location, user can send historical places as well as some important places. A person who lost their way can send their location to the server so that administrator can view and track the location of the person. Second, View Other Location Module is used to see the location of other user. When this module is clicked, an interface to enter the user id will display and after entering it, respective user location is displayed on google map. It is also used to view other important places on device.

3) User Message Module

This module is further divided into two parts: First, Send Message Module to send the message to administrator and user. Whenever user clicks this module an interface with administrator and user option will appear. If administrator is selected then user can type the message and send it to administrator. When user click user option, then interface to select the user will come, from where user can select the user id to send the message to respective user. All the message send will be stored in database in encrypted form. Second, Receive Message Module is used to view the received messages from administrator and other users. When user clicks this module, we have two options to select, administrator and user; users have to input the decrypt key to read the received messages.

C. Webserver Interface

Webserver Interface consists of five modules briefly described as follows:

1) Admin Login Module

People with administrative privilege with username and password can used this module. If the username and password fails they will not able to enter into the webserver main interface.

2) User Register Module

This module is used to register the user information. Unless the user fails to register he/she won't be able to access any features of ALMSS. During registration user have to input preferred user id, password, name, address, email address and contact number.

3) Admin Location Module

This module is used to view the location on google map in web. Since all the location information in database are in encrypted form, administrator person have to enter the decryption key to view the location of the users on google map.

4) Admin Message Module

This module is divided into two parts: First, Send Message Module to send the message to respective user or to all users. After admin clicks this module, an interface to select user, message typing box along with date and time will appear and performing all functions message can be sent in encrypted form. Second, Receive Message Module is designed to view received messages from users. Admin have to input decryption key to read the received messages.

5) Delete Module

Using this module administrative privilege person can delete the user.

We have used Java Programming language for building UI and PHP programming language for WI. JSON is used as intermediary for information exchange between UI and WI.

D. Built in Functions

Table I lists the functions that we have used during the design of the system.

TABLE I. FUNCTIONS USED

Functions	Descriptions
LocationManager	It is a class of android to manage access to the system location services. These services allows application to obtain periodic updates of the device.
LocationProvider	It represents the technology to determine the physical location i.e. to handle GIS. A location provider provides periodic reports on the geographical location of the device.
getLongitude()	It helps of obtain the longitude of the location.
getLatitude()	It helps to obtain the latitude of the location.
HttpPost()	The POST method is used to request that the origin server accept the entity enclosed in the request as a new subordinate of the resource identified by the Request-URI in the Request-Line.
HttpClient()	Interface for an HTTP client. HTTP clients encapsulate a smorgasbord of objects required to execute HTTP requests while handling cookies, authentication, connection management, and other features. Thread safety of HTTP clients depends on the implementation and configuration of the specific client .
HttpResponse()	An Http response from server.
HttpEntity()	An entity that can be sent or received with an HTTP message.
ResponseHandler()	Handler that encapsulates the process of generating a response object from a HttpResponse().
StringEntity()	An entity whose content is retrieved from a string.
file_get_contents()	Initializing function to receive the value from android device.
json_decode()	Decode data received from the android device.
json_encode()	Encode data to send data to android device.

V. EXPERIMENTAL RESULTS

The Operating System for smart phone is Android 2.2. Programming languages are Java (version: 1.6.0_25) and PHP (version 5.2.8). MySQL (5.1.30) is used as the database. We have used Eclipse (version: Helios Service Release 2) as a Java Development Tool in Windows, Macromedia Dreamweaver (version: 8) for PHP programming.

We first used an android emulator to run client application and local server as webserver for conducting an experiment. To obtain the latitude and longitude, we use getLatitude() and getLongitude() functions respectively along with the features of LocationManager and LocationProvider classes. After obtaining the location values, these values were send to database in encrypted form. And providing the appropriate decryption key, location is displayed on google map in web. We use HttpPost() to connect to the webserver and android emulator, JSONObject() to set the value to send to webserver, HttpClient() to send information set by JSONObject(), ResponseHandler() to handle the response from the server, StringEntity() to convert JSONObject variable to string before sending to server. In server side, we use file_get_contents() to receive value from client and json_decode() to decode the receive value.

To receive the information sent from server to client, we use HttpEntity() to handle the response from the server, HttpResponse() to execute HttpPost(), JSONAray() accept encoded information from the server. In server side we use json_encode() to encode value before sending to client.

In between the process of sending and receiving data we use symmetric cryptography technique [9] in the server side to ensure the security of information. All the information in the database is stored in encrypted form. And information is decrypted while trying to read the data from database.

After the successful testing in the emulator and local server, we used real android smart phone HTC Desire G7 with Android Version 2.2 and online webserver. Fig. 3 shows some snapshots of the successful test.

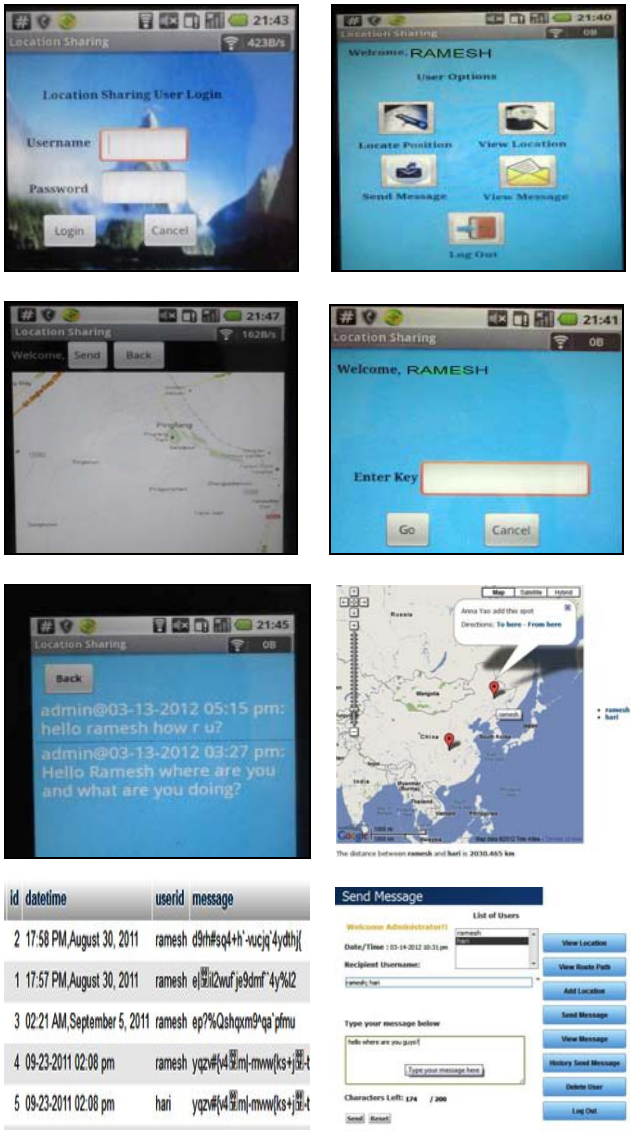

Figure 3. a) Login Interface b) Main Interface in android device c) Interface to send Message to admin d) Interface to provide decrypt key e) Decrypted messages from admin f) List of users in google map in web g) Encrypted data in database h) Interface to sent message to users from web

VI. CONCLUSION AND FUTURE WORKS

Due to the security issue of the information send by the user and lack of centralized database in the present scenario, this paper has given approach to develop a secured android-based location and message sharing system. In this paper we have used Java programming language to develop the client side, and used PHP programming language to develop server side with MySQL as external database to store information. In this case we are integrating the concept of symmetric cryptography and all the information has been encrypted before saving to the database. We have tested the system in emulator and finally tested the system successfully in the real life scenario using HTC android smart phone. With the help of GPS enabled smart phone we were able to send the longitude and latitude to the webserver, analyzing the location data from the database and displaying the location and trace path in the web which helps us to know where the client is. And finally we were able to send the message through webserver and android device and vice-versa.

ALMSS is still in the development stage. Some enhanced functions are still needed to be added continuously. In future work in this area, it plans to explore the following extensions.

1) Improvement in user interfaces in android device as well as in webserver.
2) Accuracy of information can be improved by using several algorithms.
3) Improving the security of data by using other different cryptography method.
4) Maintaining different group of users to share information within groups only.

REFERENCES

[1] Gartner (2010), http://www.betanews.com/joewilcox/article/Gartner-Android- smartphone-sales-surged-8888-in-2010/1297309933

[2] US Government, Global Positioning System, http://gps.gov/

[3] Android Developer (2011). What is Android? http://www.android.com/about/

[4] Google (2008), Documentation – Android, Available: http://code.google.com/android/documentation.html

[5] PHP, http://www.php.net/manual/en/intro-whatis.php

[6] MySQL, http://www.mysql.com/about/

[7] JSON, http://www.json.org/

[8] Lanxiang Chen, Shuming Zhou, "The comparisons between public key and symmetric key cryptography in protecting storage systems," Computer Application and System Modeling (ICCASM), 2010 International Conference on , vol.4, no., pp.V4-494-V4-502, 22-24

[9] Symmetric encryption, http://www.instantcrypt.com/how_public_key_encryption_works-ntroduction.php

[10] J. Tsai, P. Kelley, L. Cranor, and N. Sadeh, "Location-sharing technologies: Privacy risks and controls". In Research Conference on Communication, Information and Internet Policy (TPRC), 2009.

[11] Xu F, He J, Wright M, Privacy protection in location-sharing services[C] //Anon.2010 International Conference on Computer Application and System Modeling (ICCASM 2010), USA.

[12] Bellavista P, Kupper A, Helal S. Location-based services: Back to the future [J]. IEEE Pervasive Computing, 2008, 7(2): 85-89.

[13] Chandra A, Jain S, Qadeer M A. Implementation of location awareness and sharing system based on GPS and GPRS using J2ME, PHP and MYSQL[C] //Anon. 2011 3rd International Conference on Computer Research and Development, ICCRD 2011,

[14] Kumar, S.; Qadeer, M.A.; Gupta, A.; , "Location based services using android (LBSOID)," Internet Multimedia Services Architecture and Applications (IMSAA), 2009 IEEE International Conference

[15] Junhui Zhao, CaiMu Zheng, Di Zhou, "Design and Implementation of a location based service platform" , IEEE Network, 2008

[16] Yuan-Cheng Lai; Han, F.; Yi-Hsuan Yeh; Ching-Neng Lai; Yu-Chin Szu; , "A GPS navigation system with QR code decoding and friend positioning in smart phones," Education Technology and Computer (ICETC), 2010 2nd International Conference.

[17] Nan Li, Guanling Chen, "Sharing location in online social networks," Network, IEEE , vol.24, no.5, pp.20-25, September-October 2010.