Cloud Based Location and Message Sharing System

Anita Gaikwad
IT Department
Jspm's Rajarshi Shahu College Of Engg
Pune,India
anitagaikwads25@gmail.com

Kajal Bhise
IT Department
Jspm's Rajarshi Shahu College Of Engg
Pune,India
kajal.bhise21@gmail.com

Prof. Dipmala Salunkhe
IT Department
Jspm's Rajarshi Shahu College Of Engg
Pune,India
Dipmala.salunke@gmail.com

Shraddha Kalbhor
IT Department
Jspm's Rajarshi Shahu College Of Engg.
Pune,India
Shraddha.kalbhor000@gmail.com

Varsha Bangar
IT Department
Jspm's Rajarshi Shahu College Of Engg.
Pune,India
Varshabangar94@gmail.com

Abstract **-** It has been observed in the last few years that android technology is emerging very rapidly. Because of the android technology the smart phones have come into boom. There are various applications developed using the android technology like games, music, shopping, maps etc. One of the most used applications is the chatting application. Chatting application is the most convenient medium to chat or communicate with each other. There are many chat applications developed earlier, but they have some or the other drawbacks. In previous papers there was a major problem related to the security of the messages. But this drawback has been overcome in this paper. Now-a-days most of the communication is preferred to do on mobile, this communication may contain normal talks, personal information or any other sensitive data. For this purpose the security implementation is very necessary. Security can be implemented in many ways like encryption and decryption of the messages, stegnography, hashing etc. In the face of widespread Internet surveillance, we need a secure and practical means of talking to each other from our phones and computers. Many companies offer "secure messaging" products—but are these systems actually secure? Is your communication encrypted in transit? Is your communication encrypted with a key the provider doesn't have access to? Can you independently verify your correspondent's identity? Are past communications secured if your keys are stolen? Is the previous database centralized? And many such questions arise when you use the chatting application. This paper provides solution to the above questions in a more prominent manner.

Keywords:- *Stegnography ,Secure messaging , PHP , Android ,Cloud*

*****

I. Introduction

Today's world is filled with evolution of various technologies, where everyone relies on its inventions and discoveries. Knowingly or unknowingly all are addicted to these technologies. Using communication technology one can share information very easily. And this has happened because of the rigorous and fast development in the internet services, which allows us to know what is happening in the world within a click of a button. A very interesting and important technology that has been a boon to mankind is the invention of the mobile devices. As the mobile phones came into existence the technology used in the mobile were different operating systems but the most common mobile operating systems are: Android from Google, iOS from Apple, Blackberry and Windows Phone from Microsoft.In recent years, with the development of mobile communication and Mobile terminal, especially the release of Android smart phone platform has injected new vitality to the mobile space. Android is an open sourcing mobile operating system based on Linux which is a completely open and integrated platform for mobile devices. Android platform consists of the operating system, middleware and user interface and application software. It is a key applications, software stack and middleware for mobile devices. Various developers can create different applications using android SDK, all these applications can be written using the java programming language and they are run on Dalvik, which is a custom virtual machine that is created for embedded use, that runs on top of Linux kernel.

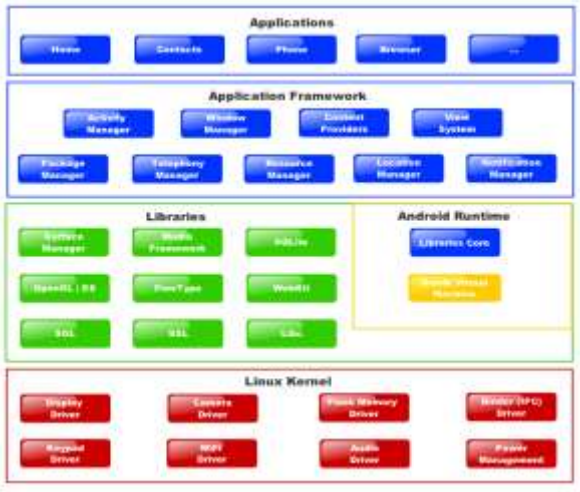

Figure.1.Android Levels

The above diagram shows the different levels used in the android operating system. Android has been gaining its popularity very rapidly and its market share is also increasing. Using this communication technology people are sharing the information with each other whether it be private information or in general, but the question arises is the information securely transmitted or not. This paper deals with secure message sharing based on android smart phone using cloud computing.

Cloud computing: -

The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.Cloud computing can be thought of as ―time-sharing or the ability to share computing resources among many different users. In the early days of computing, many companies actually shared a single computer that was located in a remote data center. The computer was able to allocate and manage resources for each user and each application, and users could request more computing time, or less, adjusting the amount of time they used the timesharing service.

So, what does modern cloud computing offer that is new to enterprise IT? First is the ability to leverage components from different cloud resources and mix and match the solutions you are seeking. You can leverage storage as-a-service from one provider, database-as-a-service from another, and even a complete application development and deployment platform from athird. This ability to leverage just the resources you need from the solutions you want to drive, as well as in just the right amounts, is a clear value of modern cloud computing. Second is the commoditization of bandwidth, which allows enterprises to leverage cloud computing resources as if they are local. Thus, you can leverage storage and runtime resources as if they existed within your data center, something that was difficult just a few years ago.

Finally, there is the availability of very innovative cloud computing providers. While the architecture and model of cloud computing is nothing new, the cloud computing players who provide the services are, including infrastructure- as-a-service players such as Amazon's EC2 and platform-as-a-service players such as Google's App Engine. With cloud computing growing by leaps and bounds, better and more innovative cloud computing services are being built and released continuously. Cloud computing has many benefits such as

- Cost
- network
- innovative
- expandability
- speed to implementation.

II. Literature Survey

Nowadays the message sharing communication is widely used. In this communication various secret and confidential information may be transmitted. So security is the major issue in the message sharing system. This communication also involves the voucher-less electronic recharge system , balance transfer or message banking like financial transactions. In these value added services (VAS) there is a major issue of security and integrity .For this purpose message encryption and authentication is very much important at network layer and at application layer as well. It prevents the internal fraud in between the communication. [2]

For authenticating a message over an insecure network , secret key is shared between sender and receiver .But in this method the data can be hacked if anyone gets the key .So authentication can be done without using secret key as well, for example by speaker identification over the phone. By using such techniques only small messages can be authenticated. For larger one the message is subdivided in parts and then authenticated .In this synchronization must be maintained [3]

Group communication is also the important aspect of communication. Group communication also requires privacy and security when transferring the confidential data. For this purpose one time session key is shared among all the group members in secured way. Authentication can be provided by using authenticated key transfer protocol. [8] Access control mechanism is also important in the group communication. In the peer to peer network adding or revoking a group member without changing secret key of other group members. So unauthorized members cannot access the data in the group communication. Also the massive message transferring as avoided. [10]

Cloud computing is widely used in the communication. In cloud computing set of resources and services are provided on internet throughout the world. It also provides virtual resources via internet so as large amount of data is to be maintained. So the concept of cloud computing is raised .to manage data cloud computing is very important, as it shares hardware and software. There is not any risk of losing data in the cloud. So the use of cloud is increasing day by day but there is the issue of security is raised. Securing data on

 ISSN: 2321-8169
1630 - 1636

cloud is very important aspect for preventing the hackers from hacking the confidential data. Some techniques use ECC based PKI for certificate procedure as it provides security with 1024 bit key size. Secured Cloud Storage Framework (SCSF) is used in technique [4] to store and access data in cloud in insecure channel as well in secure way [4].

Cryptography is used to prevent access of intruders for hacking the information. Hybrid Vigenere Ceaser Cipher Encryption (HVCCE) is used in scheme [5]. It prevents cloud in three places that is in client location, in network and in server location. In this scheme the time for decrypting the cipher text for hackers will be more than single cryptographic system [5].

In the technique [9] new environment that is trusted cloud environment being used previously that is controlled by both client and the cloud admin. It is more secured one because both the admin and client cannot make any updation in the data without permission of each other. This leads to maintain the privacy of the user. This provides a two way security protocol. Users upload the data on the cloud in an encrypted format. If admin wants to update the data, it asks the user for the secret key and the user sends a key in a message digest tag. It uses MD5 algorithm for the message digest tag. If any intruder changes the key then the tag also changes. So it indicates that the key is not correct. [9]

To improve the security of hidden information steganography is used with visual encryption [7]. For securing data hiding and transmission over networks steganography is used on the large scale. It makes the encryption and hides the data in Least Significant Bits (LSB) of original image. It involves both Genetic algorithm and visual cryptography for making data more secure. Genetic algorithm modifies the pixel location of image and to detect the message is very difficult task. Visual cryptography is the encryption of the visual information. [6]In the value added services and mobile commerce security of a communication is needed to be maintained. For this purpose encryption is one of the important methods and is used for the many security issues. Along with encryption and decryption, Hash function is also playing an important role in security. These are the function used for maintaining the integrity. They are the error detecting code or the checksum for checking whether the integrity is maintained or not. Hash function are better than MAC function because these are less complex and are not more time consuming.[1]

So considering the advantages and disadvantages of the above techniques the proposed system contains the cloud as a server which stores all the data in an encrypted form. Here the privacy of the user is also maintained on the cloud. Digital signature is also used for the authentication, in the form of message digest using MD5 algorithm. Steganography is also used for hiding the confidential data. For storing the password on cloud hashing function is used so that even admin of the cloud cannot hack the password.

III. Proposed System

A. System Architecture

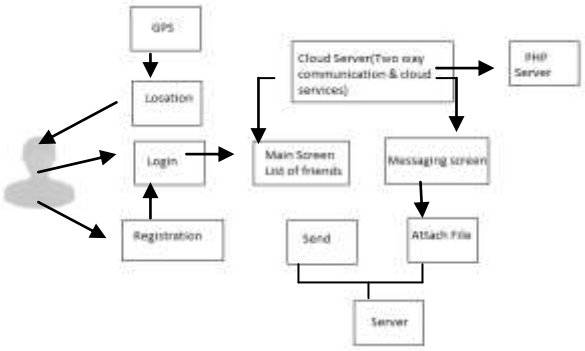

Figure 2. Architecture of the Cloud-based Based Location And Message Sharing System

This system architecture consists of two operations. Which are as follows:

1) Message sending operation.
2) Message receiving operation.

1) Message sending operation:

In message sending operation user need to register on this system. When the registration process is completed then user will get login. User need to add friends then list of friends is shown. User can send message or attach file to his or her friends. All this information is stored on cloud server in an encrypted format.

2) Message receiving operation:

In message receiving operation user have to input the decrypt key to read the received message.

B. User and cloud server interface of cloud based location and message sharing system.

 ISSN: 2321-8169
1630 - 1636

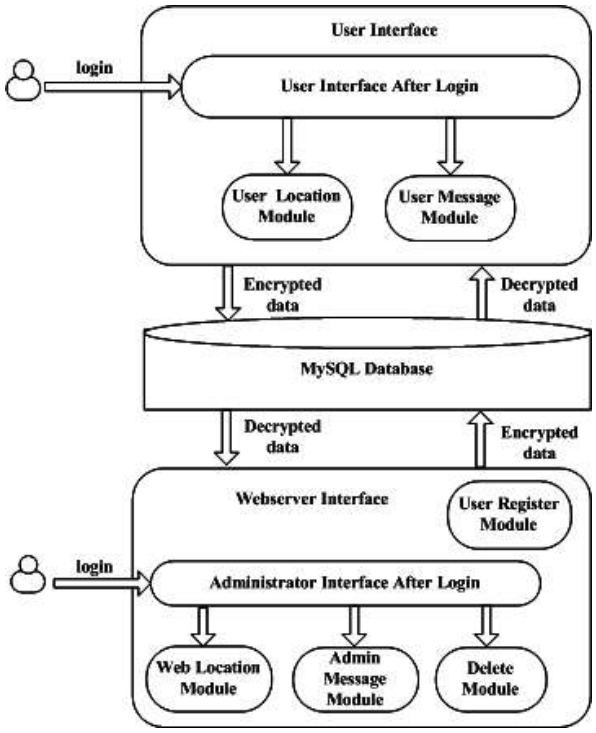

Figure 3. User and cloud server interface of cloud based location and message sharing system.

This user and webserver interfaces can be further divided in

Server Interface (CI).

1. User interface

User interfaces consists of following three modules

which are explained as follows:

a) User Login Module

This This module is displayed on android device when Cloud based location and message sharing system 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.

b) User location Module

It is divided into two parts: First, Send Location Module to send the current location where user is and some nearby important places, to database in an encrypted form. When this module is clicked, a window with some nearby important places 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 some nearby important places. 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. It is also used to view other important places on device.

c) User Message Module

This module is further divided into two parts: First, Send Message Module to send the message to administrator or 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 selects 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 get two options to select, administrator and user; users need to input the decrypt key to read the received messages.

2. Cloud Server interface

a) Admin Login Module

People having username and password can use this module. If the username and password fails they will not able to enter into the cloud server main interface.

b) 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 cloud based location and message sharing system. During registration user have to input preferred username, password, email address.

c) Admin Location Module

This module is used to view the location. 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.

d) Admin Message Module

This module is divided into two parts: First, Send Message Module to send the message or file to respective user or to all users. After admin clicks this module, an interface to select user, message typing box along with attach file 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 or to see any file.

e) 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 cloud server. JSON is used

as intermediary for information exchange between UI and cloud server interfaces.

C. Built in function

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

Functions	Descriptions
Location Manager	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.
Location Provider	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.

IV. Experimental Result

The operating system for smart phone is Android keplar. We have used Eclipse (version :Helios service Release 2)as a Java Development Tool in Windows. Programming language as a java(version 1.8) and PHP(version 5.8.2). MySQL (version 5.1.30) is used for database.

To run client application we used android emulator and for conducting experiment we can used local server as web server. we first use the Google place API level, In this level various places are include. Firstly to obtain the longitude and latitude used getLongitude() and getLatitude functions respectively along with feature of LocationProvider and LocationManager classes. firstly we concentrate LocationProvider, In LocationProvider first obtain the location space for encryption these place it send to the database and decryption is take places. Through in this application we can finding up to 10 kilometre hospital, Shop, Mall, Airport, Bank, Bus Station , Movie theatre various location displaying on Google map in web. For connecting web server and android emulator used HttpPost(), To set the message and send the web server used JSONObject(), HttpClient() used to send message set by JSONObject(), To handle the response used ResponseHandler, for converting JSONObject() variable to string before sending to server used StringEntity(). In server side receive message from the client used File_get_contents() and for decoding the receiving message used JSON_decode().

To receive the message send from server to client used HttpEntity(). The HttpEntity() also used for handle response from the server. For execution of HttpPost() used HttpResponse(). Before sending message to the client first the message is encoded, In server side JSON_encode() to encode the message before sending.

The symmetric cryptography technique use for between the process of sending and receiving data. The message security check in server side . All the messages in the database stored in encrypted form and message is decrypted when trying to read the data from database.

Fig. Show some snapshots of successful test.

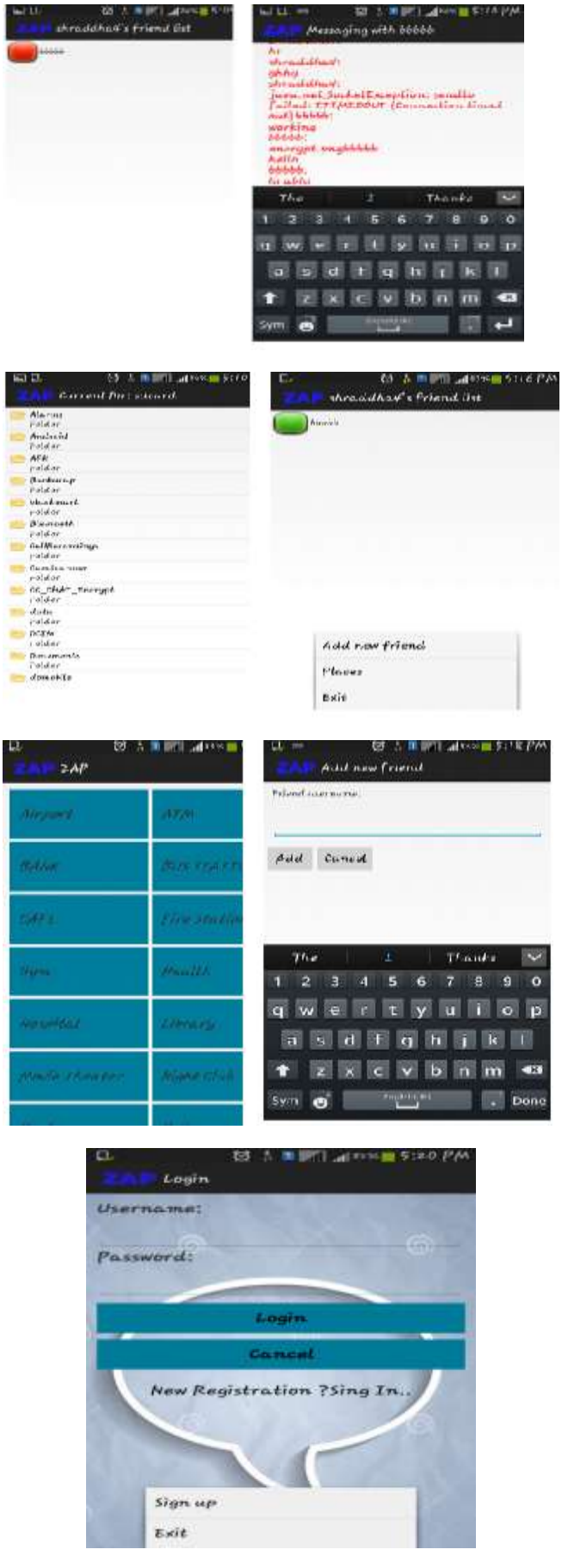

Fig. a) Login Interface b) Main Interface sign up c) Show friend list in this list those friend is added they can show d) Messaging encryption and decryption is takes places e) Current Sdcard f)Location g)Add new friend through email id h)Exit

V. Conclusion

Today's android based system does have security issues about the information send by the user. Also today's android based system doesn't have centralized database. This project gives emphasis on to develop a secured connection between android devices and hence supports message sharing system. This project uses JAVA programming to develop client and uses PHP to develop server side with MySQL as external database to log the information. All the information is being encrypted before sending to the database and hence database stores data in encrypted format. For encryption, symmetric cryptography has been used. Testing has been done in two ways to ensure project is working correctly. Unit testing has been performed on emulator. Also, to ensure correctness of the program, it is tested on HTC android smart phone to ensure that it is working in real life world. We can track the location client using following mechanism: with the help of GPS enabled smart phone, we are able to send longitude and latitude to the web server, and then analyzed the location data from the database and displayed the location and traced path in the web. Once location of client has been traced, we are able to send the message through web server and android device and vice-versa.

VI. Future Direction

This project is in development stage and opens for extensions. In future, following amendments could be made.

1) User interfaces of android and web server can be improved and can be made simpler.
2) Correctness and accuracy of information can be improved.
3) Security can be improved by using more robust encryption algorithm.
4) Maintaining different group of users to share information within groups only.

References

[1] Saxena, N. ; Chaudhari, N.S. ; Prajapati, G.L. "**An extended approach for SMS security using authentication functions"** Industrial Electronics and Applications (ICIEA), 2012 7th IEEE Conference on DOI: 10.1109/ICIEA.2012.6360809 Publication Year: 2012 , Page(s): 663 - 668

[2] Al Bashar Abul Ulayee, H. ; Mesbah-Ul-Awal, M. ; Newaj, S. "Simplified Approach Towards Securing Privacy and Confidentiality of Mobile Short Messages" Advanced Computing & Communication Technologies (ACCT), 2014 Fourth International Conference on DOI: 10.1109/ACCT.2014.23 Publication Year: 2014 , Page(s): 403 - 408

[3] Maurer, U." Authentication amplification by synchronization" Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on DOI:

10.1109/ISIT.2013.6620719
Publication Year: 2013 , Page(s): 2711 - 2714

[4] Xiao Chun Yin ; Zeng Guang Liu ; Hoon Jae Lee "An efficient and secured data storage scheme in cloud computing using ECC-based PKI" Advanced Communication Technology (ICACT), 2014 16th International Conference on
DOI: 10.1109/ICACT.2014.6779015
Publication Year: 2014 , Page(s): 523 - 527

[5] Sengupta, N. ; Holmes, J. "Designing of Cryptography Based Security System for Cloud Computing" Cloud & Ubiquitous Computing & Emerging Technologies (CUBE), 2013 International Conference on
DOI: 10.1109/CUBE.2013.20
Publication Year: 2013 , Page(s): 52 - 57

[6] Prema, G. ; Natarajan, S. "Steganography using Genetic Algorithm along with Visual Cryptography for wireless network application" Information Communication and Embedded Systems (ICICES), 2013 International Conference on
DOI: 10.1109/ICICES.2013.6508373
Publication Year: 2013 , Page(s): 727 - 730

[7] Mostaghim, M. ; Boostani, R. "CVC: Chaotic visual cryptography to enhance steganography" Information Security and Cryptology (ISCISC), 2014 11th International ISC Conference on
DOI: 10.1109/ISCISC.2014.6994020
Publication Year: 2014 , Page(s): 44 - 48

[8] Yining Liu ; Chi Cheng ; Jianyu Cao ; Tao Jiang "An Improved Authenticated Group Key Transfer Protocol Based on Secret Sharing" Computers, IEEE Transactions on
Volume: 62 , Issue: 11
DOI: 10.1109/TC.2012.216
Publication Year: 2013 , Page(s): 2335 - 2336

[9] Dubey, A.K. ; Dubey, A.K. ; Namdev, M. ; Shrivastava, S.S. "Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment" Software Engineering (CONSEG), 2012 CSI Sixth International Conference on
DOI: 10.1109/CONSEG.2012.6349503
Publication Year: 2012 , Page(s): 1 - 8

[10] Xiaoming Wang ; Shuaiwen Xu "A secure access control scheme based on group for peer to peer network" Systems and Informatics (ICSAI), 2012 International Conference on
DOI: 10.1109/ICSAI.2012.6223323
Publication Year: 2012 , Page(s): 1507 - 1511

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

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

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

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

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

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

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

[18] 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

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

[20] 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.