Short Message Service using SMS Gateway

Veena K.Katankar
M.E.-4th Sem
(Wireless Communication & Computing)
G.H. Raisoni College Of Engg, Nagpur

Dr.V.M.Thakare
Professor & H.O.D.
Dept. Of Computer Science & Engg
SGB Amravati University, Amravati

Abstract — **Short message service (SMS) will play a very vital role in the future business areas whose are popularly known as mobile banking, organizational marketing system etc. For this future, SMS could make a mobile device in a business tool as it has the availability and the effectiveness. This thesis is about software development that is based on short messaging service (SMS) system for delivering messages through SMS gateway. Main goal of proposed system is to provide multi level local authentication to the SMS gateway service. This service can be implemented in any multi departmental organization where SMS service is used for notification system and marketing purpose. Proposed system has web interface and the encryption method for providing service**

Keywords—SMS, SMS gateway, SMPP (Short Message Peer-Peer) Protocol, SS7

I. INTRODUCTION

Short Message Service is a mechanism of delivery of short messages over the mobile networks [1]. It is a store and forward way of transmitting messages to and from mobiles. The message from the sending mobile is stored in a central short message centre (SMS) which then forwards it to the destination mobile. This means that in the case that the recipient is not available; the short message is stored and can be sent later. Each short message can be no longer than 160 characters, while these characters can be text (alphanumeric) or binary Non-Text Short messages.

SMS gateway is a device or service offering SMS transit; transforming messages to mobile network traffic from other media, or vice versa, allowing transmission or receipt of SMS messages with or without the use of a mobile phone. Typical use of a gateway would be to forward simple e-mail to a mobile phone recipient. SMS gateway is most fast and reliable way for mass / bulk SMS sending. It deals with mobile service provider and sends SMS with sender identity as textual sender ID and authentication. This system is developed for improving gateway user security.

Some SMS gateway providers can be classified as aggregators or Signaling system No.7 (SS7) providers. The aggregator model is based on multiple agreements with mobile carriers to exchange 2-way SMS traffic into and out of the operator's Short Message Service Centre (SMS-C), also known as 'local termination model. Aggregators lack direct access into the Signaling system No.7 (SS7) protocol, which is the protocol where the SMS messages are exchanged. These providers have no visibility and control over the message delivery, being unable to offer delivery guarantees. SMS messages are delivered in the operator's Short Message Service Centre (SMS-C), but not the subscriber's handset.

II. SMS NETWORK ARCHITECTURE

SMS messages are transmitted over the Common Channel Signalling System 7 (SS7). SS7 is a global standard that defines the procedures and protocols for exchanging information among network elements of wire line and wireless telephone carriers. These network elements use the SS7 standard to exchange control information for call setup, routing, mobility management, etc. Figure 1 shows the typical network architecture for SMS communication. Conceptually, the network architecture consists of two segments that are central to the SMS model of operation: the Mobile Originating (MO) part, which includes the mobile handset of the sender, a base station that provides the radio infrastructure for wireless communications, and the originating Mobile Switching Centre (MSC) that routes and switches all traffic into and out of the cellular system on behalf of the sender. The other segment, the Mobile Terminating (MT) part, includes a base station and the terminating MSC for the receiver, as well as a centralized store-and-forward server known as SMS Centre (SMSC). The SMSC is responsible for accepting and storing messages, retrieving account status, and forwarding messages to the intended recipients.

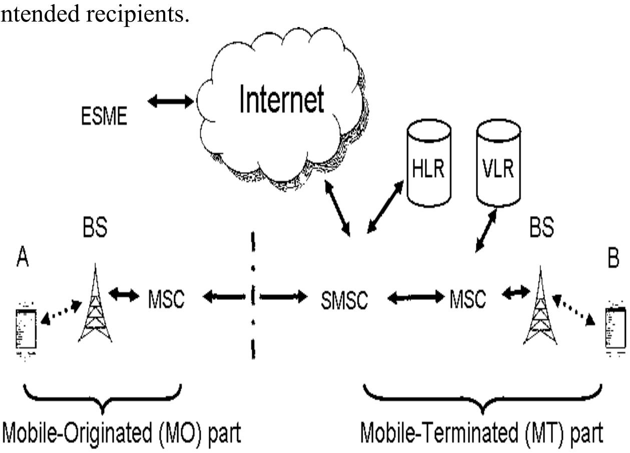


Fig. 1.1. Typical network architecture for SMS

It is assisted by two databases: the Home Location Registrar (HLR) and the Visitor Location Registrar (VLR). The two databases contain respectively permanent and temporary mobile subscriber information, e.g., the address of the MSC the device is associated with. Though the Short Message Service has been popularized by the exchange of text messages among cell phone users, it has been increasingly used by businesses as a low-cost bearer to deliver various types of content such as ringbones, news, stock price, quizzes, and casting of votes. Such content providers, also known as External Short Message Entities (ESMEs), initiate or receive text messages through gateways which bridge the SMS interface to the internet .

III. REASON FOR SELECTION

A Direct To Short Message Service Centre (SMSC) Gateway is a device which allows SMS text messages to be sent and/or received by email, from web pages or from other software applications. The Gateway connects directly to a Mobile Operator's Short Message Service Centre (SMSC) via the Internet or direct leased line connections. It converts the message format into a format understood by the SMSC, typically this is the Short Message Peer-to-Peer **(**SMPP) protocol. Direct To Short Message Service Centre (SMSC) Gateways are used by SMS Aggregators to provide SMS services to their clients. Typically Direct To Short Message Service Centre (SMSC) Gateways are used for high volume messaging and require a contact directly with the Mobile Operator.

IV. PROPOSED SYSTEM

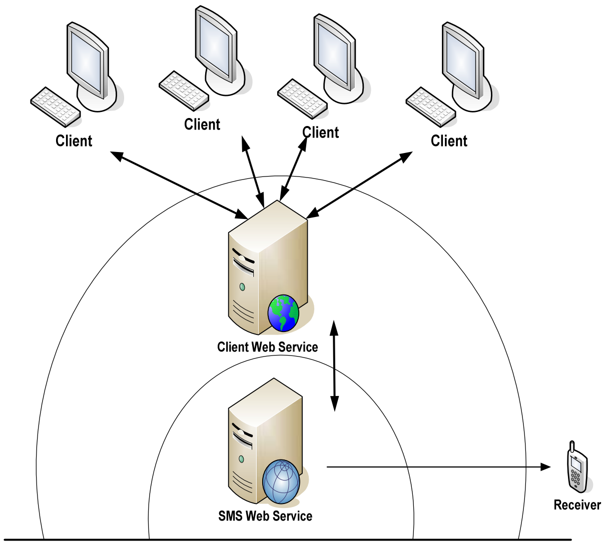


Fig.1.2. Overall Structure

Figure 1 describe the overall structure of the project it has three main level of execution. First level where user will access web based application and assemble SMS with basic header like receiver mobile number and message to send to the receiver. This message has been send to second level that is at web server level where it will modify message by applying some security header to SMS and pass it to the SMS gateway now SMS gateway will send this message to receiver mobile phone. Here whenever user send message he don't need to give security header [4] which protect password from user. Major advantage of this system is protection of security header and providing service to the clients along with this service will let the administrator track the service utilization of every user if the service is free to client [5].

V. RESEARCH METHODOLOGY

SMS Client User Interface: This module is web page based user interface where user need to login using user specific authentication details. After successful login user can manage SMS sent, saved by that specific user and can compose new SMS using web user interface. Now this interface ask user receivers mobile number and message to send it won't require SMS gateway authentication security headers those are applied at last level of execution. Once user press sent option system will first encrypt the user message using some encryption algorithm [6] and then generate web POST data and transfer it to web application. Web application then process further [7].

SMS Verification & Management: This is first level of verification. As proposed system giving free access to SMS gateway resource to the user then it's systems responsibility to manage local user with their resource usage. This level will manage all transactions by local user [8].

Web Application: web application is mainly divided in to different sub module from decryption to authentic SMS generation.

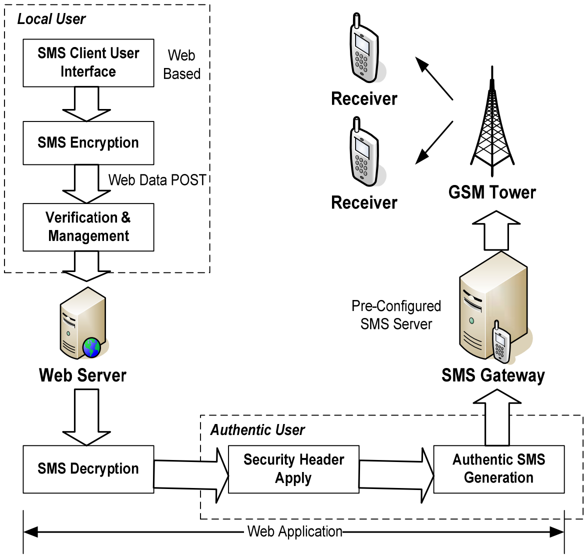


Fig.1.3. Software Level Execution Flow

POST Data Decryption: As client web interface send data using web POST method and encrypted then web application will first read web data from POST method using server request object then it will decrypt SMS in to text because SMS gateway cant understand encrypted message it need ASCII code SMS.

Security Header Adder: This module will simply add security header to the decrypted message. These headers are provided by the SMS gateway service. To local user system is providing it's own password for client security [9, 10, 11].

Authentic SMS Generation: This module will generate authentic message this is for SMS gateway. After message generation it will transfer message to SMS gateway web service this is implemented by some mobile service operator they also provide some unique sender ID to each client [12,13].

VI. DATA POSTING

First is user interface i.e. input need to login using user specific authentication detail. After successful login, web user interface ask two parameters such as receiver mobile number and message to send it. Once the user press sent option the system will first encrypt the message using session hijacking method and then transfer to the local web service.

This local web service read the message and providing its own id and password given by SMS gateway when this service registers with them. Then the SMS gateway has given the sender id GHMTech. This service will require five parameters. The parameters are receiver mobile number, message, user id password and sender id. It will also manage database.

Then message will transfer to the remote web service using internet and finally this remote web service send message to the mobile number.

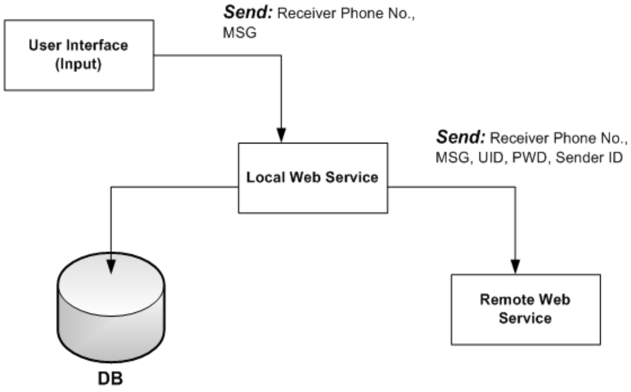

Send: Receiver Phone No., MSG
User Interface (Input)
Send: Receiver Phone No., MSG, UID, PWD, Sender ID
Local Web Service
Remote Web Service
DB

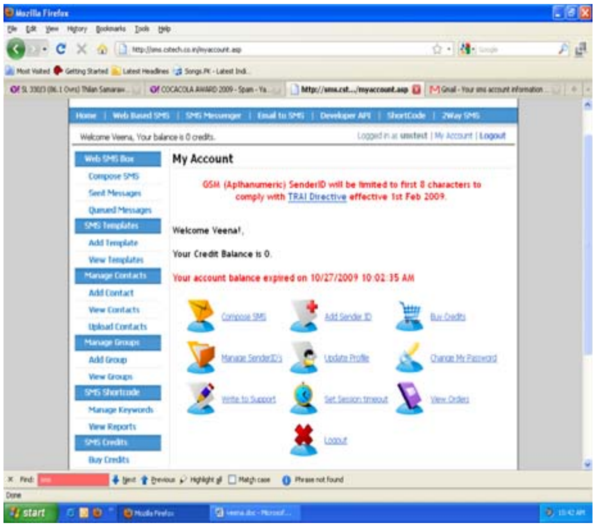
Fig.1.4.Data Posting

VII. SMS GATEWAY USER INTERFACE

Our proposed system connects to SMS gateway internally. When a user use Messaging System, the Authentication is important. Without this Authentication users are not able to send the message. This Authentication is a Subscriber ID and Subscriber Password given by SMS gateway when the users register with them. The SMS gateway have given the sender ID GHMTech.

First we have got sender ID. Using this sender ID, this SMS gateway is used for sending SMS to different mobile. In this ,SMS can be compose. Here we can see sent messages on what time and on what date messages have to be sent. .We can see queued messages.

We can add new contacts, edit contacts..We can add templates, view templates. We can manage group. We can upload contacts.



Welcome Veena, Your balance is 0 credits.

My Account

GSM (Aplhanumeric) SenderID will be limited to first 8 characters to comply with TRAI Directive effective 1st Feb 2009.

Welcome Veena!,

Your Credit Balance is 0.

Your account balance expired on 10/27/2009 10:02:35 AM

Fig.1.5. SMS gateway user interface

VIII. SMS GATEWAY ARCHITECTURE

SMS gateway is a powerful, flexible SMS Gateway application that enables the applications to send/receive SMS messages to mobile devices with your computer. It has an easy to use user interface, and an excellent internal architecture. The application can use a GSM mobile phone attached to the PC with a phone-to-PC data cable or IP SMS technology to transmit and receive the messages. Message Server works on Microsoft Windows XP, 2000, 2003 operating systems.

Office users can use Microsoft Outlook, Microsoft Outlook Express and Microsoft Excel to send hundreds of messages to their clients. The messages and the phone numbers are stored in Excel files and an Excel Macro initiates the sending process. (The excel macro is included in the software package.)

Software developers can integrate SMS messaging functionality into their applications very easily. For example if an SMS message needs to be sent, it can be inserted into a database table used for outgoing messages. The Message Server monitors this table and delivers the message. The Message Server puts all received SMS in another database table used for incoming messages. Of course many other APIs are available in the software to support software development

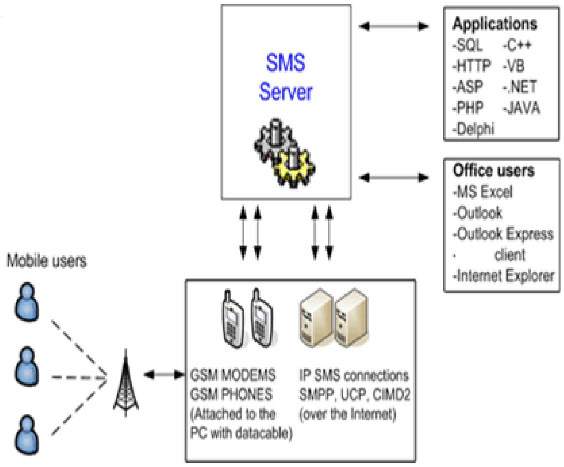


Fig. 1.6. SMS gateway system architecture

IX. SMPP PROTOCOL

The SMPP('Short Message Peer-to-Peer')protocol is an open industry Layer-7 TCP/IP protocol for exchanging SMS messages between SMS peer entities such as short message service centres. It is often used to allow third parties(e.g. content suppliers like news organisations)to submit SMS messages ,often in bulk. It is a standard messaging protocol designed to simplify integration of data applications with wireless mobile networks such as GSM, TDMA, CDMA etc. The application and mobile carriers are connected via TCP/IP. SMPP is secure and sustain greater message volumes 10,000/min.

X. SOFTWARE DESIGN

This software was designed in Visual Basic 2005.The database connection was written using Query based on SQL. SQL was used to store the record and also to retrieve the record.

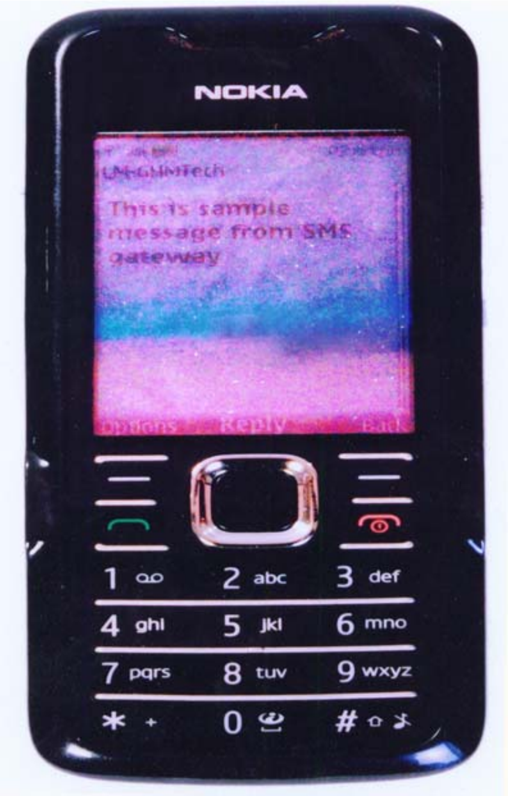
In order to make this software more realistic for college application, the design was added with application related to students. The login page was designed so that, it should be link with other options. Through this user friendly login page one can easily choose and use the option.

This software application starts with login page. Then the login page will be displayed. Two level of accessing to this software are possible. These are Administration and User.

All the required information of the users will be loaded into the message form .The main purpose of this software is to send message. Users can send the message to the selected person in their record.

User can set their site using set internet links and by clicked on the address. The page will automatically open using internet explorer.

XI. RESULT



LM-GHMTech

This is sample message from SMS gateway

Fig.1.7. Software Output

XII. CONCLUSION

The short message service unifies Internet and mobile network is on a rapid development stage, and every short message business emerged one after another. This software development that is based on short messaging service (SMS) system for delivering messages through SMS gateway. This system is most useful and uses SMS gateway which is emerging technology used by different marketing and notification provider organization like super market, colleges, weather forecasting centers.

This software was designed based on typical practical applications. From the various tests carried out, the designed software was found to be reliable and practical. More functions can be added from the prototype design. Specifically, the database had also been tested using some sets of data and it had been found to be successful. However, it has been tested using a real phone.

XIII. FUTURE SCOPE

In the future, for security of SMS various kinds of latest encryption algorithms and the hash functions are yet to be analyzed. We will try to integrate the channel coding and the encryption procedure so that it will give errorless secures fastest SMS transmission.

The application could also provide multiple senders ID implementation. The other desktop application could also port to different programming platform. There could also provide various mobile applications.

IV. REFERENCES

[1] M.A. Mohammad and A. Norhayati," A Short Message Service for Campus Wide Information Delivery", 4& National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia,2003,pp216-221.

[2] Benting Wan,2008,"Business-Based SMS Mobile Search",22nd International Conference on Advanced Information Networking and Applications – Workshops,pp. 692-695.

[3] M. Hassan Shirali-Shahreza, Mohammad Shirali-Shahreza ,2008,"An Anti-SMS-Spam Using CAPTCHA", 2008 ISECS International Colloquium on Computing, Communication, Control, and Management,pp. 318-321.

[4] Quratulain Aziz,13-14 November 2006,Payments through Mobile Phone", IEEEICET 2006, 2nd International Conference on Emerging Technologies, Peshawar, Pakistan 13-14 November 2006,,pp. 50-53.

[5] Ningning Wu, Ming guang Wu, Siguo Chen, 2008,"Real-time Monitoring and Filtering System for Mobile SMS,"pp. 1319-1324.

[6] David Lisoněk,Martin Drahanský, 2008,"SMS Encryption for Mobile Communication" 2008 International Conference on Security Technology,pp. 198-201.

[7]]Peizhou He, Xiangming Wen, Wei Zheng, 2008,"A Novel Method for Filtering Group Sending Short Message Spam", International Conference on Convergence and Hybrid Information Technology 2008,pp. 60-65.

[8] Siti Dianah Abdul Bujang , Ali Selamat,2008,"Verification of Mobile SMS Application with Model Checking Agent",Eighth International Conference on Intelligent Systems Design and Applications,pp. 217-222.

[9] Juan Jos´e Garza-Salda˜na, Arturo D´ıaz-P´erez, 2008, "State of Security for SMS on Mobile Devices", Electronics, Robotics and Automotive Mechanics Conference 2008,pp. 110-115.

[10] Hany Harb, Hassan Farahat, Mohamed Ezz ,2008,"SecureSMSPay: Secure SMS Mobile Payment Model".

[11] MD. Asif Hossain1, Sarwar Jahan, M. M. Hussain, M.R. Amin, S. H. Shah Newaz,2008,"A Proposal for Enhancing The Security System of Short Message Service in GSM", pp235-240.

[12] Shushan Zhao, Akshai Aggarwal, 2008, "Building Secure User-to-user Messaging in Mobile Telecommunication Networks",pp 151-157.

[13] Webpage:http://www.smsspoofing.com/