Retrieving Password through SEESMS system

Hardik B. Nadiyana
G.H.Raisoni College of Engg,
Nagpur, India
hardikbn@rediffmail.com

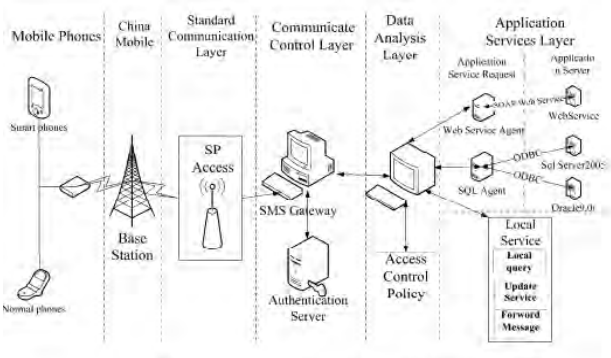
V.P. Balpande
G.H.Raisoni College of Engg,
Nagpur, India
vpbhute@gmail.com

Abstract: **In current scenario, the SMS is used world wide with wide usage of more than three trillions sent across the globe. Due to such huge usage and easy as well as efficient work, it provides wide coverage to people globally. This paper proposes the system in which we can easily create passwords with the help of website name. With the help of this system, it also plays significant role of recalling SMS from the server stored in database in encrypted format. This also helps to eavesdropping, frauding and non-repudiation of SMS.**

Keywords: ***SMS, SEESMS, Query generating algorithm, password generation, cryptosystem***

I. INTRODUCTION

SMS has shown significant resilience in market that is bombarded with media that all add to the clutter of daily communications. SMS is a form of highly personal, immediate communication with high reach capability, low cost and high retention levels. With communications media converging, SMS is now accessible in many ways as a business tool. Consumers have been first in adopting SMS as a means of communication, popularizing the protocol with a specific language and creating the playing fields that are now being entered by businesses[1]. This article tries to bring an innovative, cheap, and easy approach to mobile application user interface personalization for mobile devices, based on SMS (Short Message Service) technology. This service aims to provide poor and developing countries with the same kind of possibilities that the rich ones have: access to updated information with low cost. The success of SMS communication [2] may be upon to 3 main reasons: it is ubiquitous, it has a near real time delivery and it follows the "store and forward" mechanism, with later retransmission in case of failure. Other important SMS characteristic for this system is to be asynchronous, so it's able to send data for device without mobile device request, and it's possible to send, for example, an user interface updating without mobile application in question being started or requested it. Although SMS protocol is a well designed communication protocol that uses GSM networks to information traffic, SMS messages have little security to protect the data being transferred, which can be catch by an unauthorized monitoring agent, besides then, SMS does not guarantee confidentiality and integrity of the message content [3] This paper proposes a method for making a generic application which dynamically communicates with databases and extracts information based on the contents of SMS.



The typical network topology of SMS framework

This application can be used to provide information to users through SMS. The system administrator can add additional functionalities by simply providing the information of new features without making any change in the source code. Section 3 describes a detailed method of how our new SMS messaging service can be added by the system administrator. In order to get specific information, a user will send an SMS to mobile Gateway which will forward it to the desktop application for necessary query execution.

After collecting required information from a specific database, a prompt reply will be forwarded to the user in reverse order. Since it is difficult to memorize formats of SMS to get different information, user can send a query SMS asking for exact format. A prompt reply will occur showing the format of SMS.

II. WORKING OF SMS

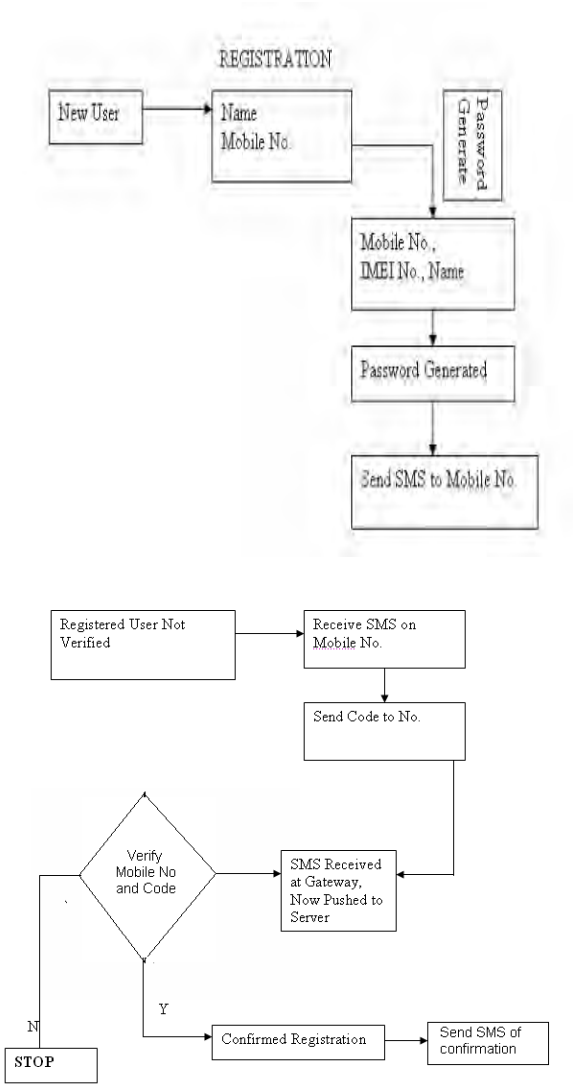
In this section, we introduce our generic SMS information system. The communication scenario of the system is divided into five steps, as shown in Figure 1 The user sends an SMS message to the SMS Gateway application having a specific starting identifier (@ in our case). Format of the SMS is automatically generated when administrator adds some new messaging service to the system.

2. The SMS Gateway application receives the message from the user and forwards it to the server application along with the phone number.

3. Server application then processes the SMS and makes a dynamic link with concerned database for information

retrieval. The server application then executes a dynamic query on the database and then generates a prompt reply containing that record which comes as a result of the required query execution.
4. The result of the query execution is sent back to the SMS gateway along with the user number.
5. The SMS gateway then forwards the message to the user.

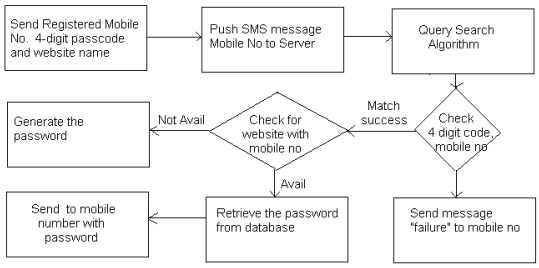
III. Project Implementation



In this project, user has to register himself with name, mobile number, city, address, IMEI number. With successful registration, it will display the screen for verification of mobile number for which again user need to enter the values and on the basis of mobile number and IMEI number as well as name, it will generate the password 4 digit code for the user and will send sms to the user mobile number and password will be displayed on the screen. After getting sms user has to enter the code, 4 digit passcode for verification and so it will give validation after the user will get transferred from SMSC gateway. Now user is ready to use this system

IV: Review Of The Project

We have implemented this proejct on various mobile numbers with various operators. The conclusion was that number registered with DND as "Do Not Disturb" with TRAI will not be able to access this service in India. The reason is we need to use SMSC gateway which will not send sms to those users who are registered with DND. The DND is facility available in India which hangs such users from telemarketers and so these SMSC gateway block those numbers from sending sms. But these users can send sms to the gateway but since they are not getting verified from the user, they won't be able to receive sms.



Once that user give the confirmation to the server with prescribed message, then it will store that username and password in encrypted format with the website name into the database. If next time same user want to retrieve the password then he will have to send the website name and the user id of the system's server. If this is giving proper verification to the user then server will automatically transfer the username and password to the user in SEESMS format with the help of which the sms will be in encrypted format. This sms will again be decrypted at the user side and then will give display to the user in actual format. The following diagram displays the flowchart of the project.

V. Encrypting SMS With Seesms

Sending or receiving SMS messages is a common habit for most of the people using a cellular phone. The general expectations are that mobile equipment should be able to promptly send and receive a message with almost no delay. The way of sending and receiving secure SMS messages could change

this habit since it involves processing incoming/ out coming secure messages which may be of several seconds. Thus, the efficiency of these systems is almost as important as the security they guarantee. Moreover, the efficiency of a system for guaranteeing secure SMS messages is heavily influenced by the same ingredients which govern its own security: in other words, the cryptosystems and the security parameters it uses. The user should be given the possibility to choose to trade part of the security of a system with shorter response times, and vice-versa. Moreover, such a customization should be allowed on a per-message basis, because the same user might need to send messages, even to the same recipient, with different levels of security. As a matter of fact, all the systems for sending secure SMS messages presented so far in literature are bound to a particular cryptosystem. While this choice simplifies their development, it may have a negative effect on their ability to meet the requirements of the users, as we said above.

By keeping this in mind, SEESMS, a Java based framework for exchanging secure SMS that aims to be efficient by supporting several cryptosystems through a modular architecture. This choice offers the advantage to easily experiment and assess the performance of several cryptosystems using several security parameters. The same advantage holds also for the final users, as they may choose which combination of cryptosystem/security parameters better suit their needs. SEESMS works at the application level and can be used for exchanging secure SMS in the P2P and in the CS scenarios. It can be seen as a tool that uses an SMS based communication channel as bearer service to exchange encrypted and tamperproof messages.

The SSMC is in charge of handling the provisioning process, used to deliver to new users a customized copy of the SEESMS client application, and the key-distribution process, used to send the public-keys of registered users following a client request. The entire communication with clients is done by using signed SMS messages. The application includes the following modules:

Registration Service (RS): The RS is used to register new users, to provide them a copy of the SEESMS client application and to run key-exchange protocols with them

Server Message Handler (SMH): The SMH is a module that can be used to exchange messages with another peer by means of SMS messages. It also includes the code needed to serialize/deserialize SMS messages and send/receive them through a GSM modem.

Secure Storage (SS): The SS implements a secure local storage area used to encrypt and to maintain sensitive data about the users that are registered to the service, such as their public-keys or their registration information. Data is encrypted using the AES symmetric cipher and stored in a relational database.

Cryptosystem Engines (CE): The CE are the modules that take care of securing the messages exchanged with a remote user. Each CE carries the implementation of a cryptosystem and offers up to three standard set of functions: Key Generation, Message Encryption/Decryption and Message Signature/Verification. These engines are used by the SSMC to implement the user registration phase and the key-exchange protocol. The current version of SEESMS includes the engines implementing ECC (ECDSA and ECIES), RSA and DSA.

VI. SEESMS CLIENT

The SEESMS client application can be used by two parties to exchange encrypted and digitally signed SMS messages. It includes the following modules:

Message Handler (MH). The MH is responsible for sending and receiving secure SMS messages. It is a trimmed version of the SMH, not including the code needed to handle communication over a GSM modem.

Secure Storage (SS). The SS implements a secure local storage area used to hold sensitive data such as the cryptographic keys of a user.

Cryptosystem Engines. Similarly to the SSMC case, these modules are used to implement the registration phase and the key-exchange protocol and, moreover, all the functions related to secure communications with another user.

Keys Communicator. This module implements the client-side key-exchange, which is used to communicate to the SSMC the cryptographic keys generated by the client.

VII. PROJECT SCENARIO

In today's world recalling passwords and usernames for each websites has become very difficult. And it has become more difficult to consider strong passwords as well as remember them. For this reason, we are developing the project in which the system will itself generate the password and so it will transfer the same to user's mobile number. The user has to download the requisite package which will decrypt the password onto the mobile handset. This will help to the user to have very unique identity for that user. Whenever the server sends the message, it will be in encrypted format with private key of IMEI number and mobile number of the user which are unique items to that user. Since, this numbers are

very unique to that user therefore these numbers are to be used. In case, handset are stolen then that user has to change the IMEI number from online form with the help of that code which is given to the user at time of verification. If user doesn't want to generate the password but want to just store them into the database that too can be possible with this system. In this system, the user will request for the password with the help of website name and so server will generate the password for that user and if user want to generate the username that too our system can generate. But this newly generated password and username will be stored in the temporary table.

Once that user give the confirmation to the server with prescribed message, then it will store that username and password in encrypted format with the website name into the database. If next time same user want to retrieve the password then he will have to send the website name and the user id of the system's server. If this is giving proper verification to the user then server will automatically transfer the username and password to the user in SEESMS format with the help of which the sms will be in encrypted format. This sms will again be decrypted at the user side and then will give display to the user in actual format.

VII. Result

The project gives innovative application to the user in modest way to comfort him to maintain the passwords of all the websites. We have taken into consideration fifty users with different MSP(mobile service providers) and tried the system. It was magnificent that all the users provide same output but many of users were not able to take SMS from the server i.e. SMSC gateway. The reason was that the users were registered with DND (DO NOT DISTURB). This service is provided by the TRAI(Telecom Regulatory Act of India) to provide comfort to the users from unwanted calls. This has to be registered as SMS DND to 1909 which is activated within 45 working days. And if we want to unregister ourselves from this service, then NDND to 1909 which again takes 45 days.

VIII. Conclusion

According to the given system we have implemented highly secured SMS which is developed with the help of SEESMS technology for password generation and also to retrieve the password for the particular website. With the help of this technology, user doesn't need to remember the password every time and don't have to take trouble for password generation for every website. The new password is needed because it might happen the user might be sharing some passwords with the some close friends and realtives. But the password for net-banking and for such financial transaction the password should be only unique and known to that individual user. Indeed, the user has to remember the password for the website and also has to use the same handset to retrieve the password which is send in the encrypted format from the server.

References

[1]. http://www.palowireless.com/sms/resources.asp.

[2]. Mauro Teófilo Alexandre Martini Paolo Cruz "Ulmo: A system to Enable Mobile Applications Personalization by Binary SMS" 2009 Fourth International Multi-Conference on Computing in the Global Information Technology DOI 0.1109/ICCGI .2009.40

[3]. Aziz J. L. Lo, J. Bishop, J. H. P. Eloff, "SMSSec: An end-to-end protocol for secure SMS", Computers & Security, Volume 27, Issues 5-6, October 2008, Pages 154-167

[4]. Md. Subrun Jamil, Fouzia Ashraf Mousumi1 "Short Messaging Service (SMS) Based m-Banking System in context of bangladesh" 11th International Conference on Computer and Information Technology (ICCIT 2008), 24-27 Dec. 2008 Page(s):599 – 604

[5]. Generic Information System Using SMS Gateway, 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology