Dynamic Encryption Driven over Secure IM System

V. Syamala Madhavi*  
M.Tech Student  
Department of CSE  
MIC College of Technology  
JNTUK, Andhra Pradesh, India

D. Prasad  
Associate Professor  
Department of CSE  
MIC College of Technology  
JNTUK, Andhra Pradesh, India

Abstract: With the rapid development of the mobile internet, mobile instant messaging systems are playing increasingly important roles in our life. The first IM system created by Mirabilis (a pioneer of online chatting that revolutionized communication over the internet), dubbed ICQ (I Seek You), in 1996 achieved widespread adoption among netizens. Although other instant messaging (IM) systems have surpassed ICQ in popularity, the medium of IM remains a popular form of technological communication. These IM systems still face with the issues of security and connectivity. XMPP (the extensible messaging and presence protocol) which is a cross platform and open protocol was adopted to resolve the connectivity problem of the IM system and a hybrid encryption algorithm using AES, SHA-1 and RSA algorithms was implemented to secure the system. The realization of the security algorithm was based on the bouncy castle encryption library. The main functions implemented in this mobile IM system include user login, roster, status change and display, sending and receiving of instant and encrypted messages, buddy management and so on. We propose a dynamic security encryption which implements a Spam Detection Process that encrypts only the messages that need encryption thereby reducing the unnecessary overhead of encrypting all unimportant messages sending between users.

Key words: Instant Messaging, XMPP, Hybrid Encryption, Bouncy Castle, Spam Detection.

I. INTRODUCTION

In the last couple of decades people have started using internet regularly. The need of live and sensible way of communication over internet has increased rapidly. The start of instant messaging came about in 1996. Instant Messenger is client software that allows person to person interactive communication in real-time provided both users have the same software. Such communication is called “chat”. Instant messaging (IM) is a real-time communication service which allows a user to send a message, usually based on text, to other users. Nowadays we depend more and more on information from the internet, and are increasingly not satisfied with accessing the internet using personal computers or office workstations. Hence accessing the internet by portable and wireless devices has been becoming popular.

Today in business communications IM system plays major role, such as observing the status of staff, real-time chatting, getting business opportunities and so laying more emphasis on the security of the system; therefore, existing work use the SHA-1 digest algorithm, AES symmetric encryption algorithm and RSA signature algorithm, with Bouncy Castle Crypto package, to design a security policy to secure the IM system.

II. BACKGROUND WORK

Design of the Mobile IM System:

The framework of the mobile IM system is based on the C/S architecture. This system consists of one server and several clients. The server is made up of two parts: the XMPP server and the background database. We use the open fire, which is open and based on XMPP as the server, and use the MYSQL database to store user data and system information. The client is developed in Java ME. We use wamp which is based on XMPP as client to communicate with the clients developed.

The processing flow of the IM system is as follows:

The mobile client connects to the server, then sends the user’s requests to the server after the XML packaging program transforms the messages, input by the user into the XML format defined by XMPP.

The open fire server receives the XML message, analyzes the requests, manipulates the database, and then sends the message to the receiver that is specified by the sender.

The mobile receiver client receives the XML message and calls the XML parsing program to transform the XML format to the data format that the Java ME program could process and finally, Java ME displays results on the screen.

The XMPP protocol and the open fire server:

XMPP is an open XML protocol, which is designed for providing real-time messaging, presence information and request-response service. XMPP has been approved by IETF as a standard. XMPP is the unity of IM protocols and resolved the connectivity problems between different IM platforms. XMPP protocol is the XML stream protocol which...
contains the XML elements that two entities exchange through the internet. In the XMPP stream there are three top-level XML stanzas.

- `<message/>` it can be seen as a push mechanism whereby one entity pushes information to another entity.
- `<presence/>` it can be seen as a basic broadcast mechanism where multiple entities receive information about an entity to which they have subscribed.
- `<iq/>` it is a request-response mechanism that enables an entity to make a request of and receive response from another entity.

Open fire is a real time server based on the open XMPP protocol and any IM client that supports XMPP could login to this server.

**Design of the Mobile Client:**

The design of the mobile client is based on Java ME platform. We divide the mobile IM client into four modules:

- Design of the interface
- XML packaging
- XML parsing
- Event response

**Design of the user interface:**

The design of the interface should be easy to use, clear and friendly. The branching process of the user interface is as follows.

**XML packaging:**

When we input some information to the interface and send requests to the server, we have to transform the byte stream information that the user input into the XML character stream that the XMPP server could identify.

For example, when we want to login, request the buddy list, request adding or deleting the buddies, the xml packaging program packages the requested information into the XML format defined by the XMPP protocol.

**XML Parsing:**

The message returned from the server is in XML format. When the mobile client receives the xml message, XML parsing program pickup the data in it according to the XMPP rules. The parsing program distinguishes the stanzas and picks up the sub elements and attributes for making sure what to be displayed or what to be executed in the next step. The parsing program is mainly used for displaying the roster, monitoring the status change and the requests for adding or deleting the buddies, etc.

**Response of events:**

The response program is responsible for displaying the content that the parsing program has picked up so as to prompt users what they should do next.

**Drawbacks of IM:**

Insecure communication is the main drawback of IM. Businesses are required to protect information related to their customers, vendors and their own trade secrets. Some of the issues that come up with insecure communication are as follows:

- Identity Theft – In identity theft an individual’s identity is stolen and is used by an identity thief to conduct various monetary transactions. By the time an individual becomes aware of such theft bad record in the system...
is already established. Confidential information such as your bank account number, social security number, and credit card information should not be shared during IM session.

- Cyber stalking - In this case stalker stalks a victim on Internet. Use of E-mail or other forms of electronic communication is used by stalker as means of stalking. Presence is the most popular feature of IM. IM gives away the presence of user. This makes it easier to stalk the person online.

### III. EXISTING SYSTEM

In the existing system when a user sends a message that message will be encrypted regardless of it is important or not. In case of unimportant messages it unnecessarily increases the time taken for encryption.

**CASE A:** when user sends a message which requires encryption is shown below.

The above message is encrypted and the encrypted code and time taken for encryption and user key generation is shown below.

**CASE B:** when a user sends a message that does not require encryption
The above message "this product is very cheap, buying this at cheaper prices" is not a important message and it does not requires encryption but it is also encrypted. Thereby increases the encryption time.

IV. PROPOSED SYSTEM

In the proposed system the important messages will be encrypted but the unnecessary messages are not encrypted. Thereby reduces the unnecessary overhead of encrypting all messages.

CASE A: when a user sends a important message it encrypts the message.

The above message is encrypted and encryption details are shown below.
CASE B: when user sends an unimportant message that message will not be encrypted to reduce the burden of encrypting unnecessary messages.

The above is not encrypted that’s why the message encryption status is shown below as “no”

Security of the system:

Security is an important aspect for both mobile users and wireless developers. A hybrid security method using AES, SHA-1 and RSA algorithms which is realized using bouncy castle is implemented. AES symmetric encryption algorithm is used to encrypt the data in communication and RSA asymmetric encryption algorithm is used to negotiate the AES key between the sender and receiver. RSA signature generation and verification algorithm is used to verify the user’s identity.

Comparison between the existing work and proposed work:

In the existing work, all messages are encrypted as it does not differentiate the messages which requires encryption and which does not requires encryption where as in the proposed work only the important messages will be encrypted thereby reduces the time for unnecessary encryption of all messages. The proposed work uses a dynamic security facility which implements a spam detection process which is helpful in processing the messages and recognizing the messages that does not require encryption.

Spam Detection Process:

The spam detection process processes the messages and recognises the unimportant messages based on the calculation of spam count. Spam count can be calculated as follows:

\[ \text{Final score} = \left( \frac{\text{spw} \times 100}{\text{tow}} \right) \]

\( \text{Spw} = \) no of spam words present in the message
\( \text{Tow} = \) total no of words present in the message

Spam words will be maintained in the database according to the requirements of the user.

Explanation:

if final score < prescribed spam count limit then
    Perform encryption // performs encryption as it is important message
else
    Do not perform encryption // do not performs encryption

Spam count limit = the limit specified based on the requirement of the user.
V. CONCLUSION

With the development of the mobile internet, mobile instant messaging systems are playing progressively more vital roles in our life. These IM systems are facing the issues of security and connectivity. XMPP which is a cross platform and open protocol was adopted to resolve the connectivity problem and a hybrid encryption algorithm using AES,SHA-1 and RSA algorithms is used to provide the security to the IM system .In the existing work all messages that send and receive between the users will be encrypted which increases the unnecessary overhead of encrypting all messages whereas in the proposed system the spam detection process processes the messages and recognises the messages which does not requires encryption and sends them to the receiver without encryption thereby reduces the unnecessary overhead of encryption. If we compare the time taken for encryption of important messages, the time taken by the proposed system is less than the time taken by the existing system. Thus in proposed work we are not compromising in providing security and added advantage in lessening the encryption time.

REFERENCES