Integrating a Instant Messenger into the Institution Website

Saugat Poudel[1] **Vinod L.B[2]** **Olorunmo Taiwa Samuel[3]**

Abstract— Instant messaging (IM) application provides a real time media and text transmission over a network. IM can be used for real time communication between the individuals when both are connected over a network. Through IM not only text but other media files like audio, video and image files also can be shared. There are a lot of IM applications that are being used by millions of user. Because of different preferences of the user they prefer different type of IM giving a high market for IM application developer to develop new application of user preferences. Some IM application focuses on faster communication, while some on reliable communication, while some may provide more secured communication then others. Integrated IM in an institution can be used securely and for more reliable information sharing by people affiliated to the institution.

Keywords—*Instant Messaging(IM), JIT, Transport Layer Sceurity(TLS), Self-Signed Certificate(SSC), Secured Socket Layer(SSL)*

I. INTRODUCTION

Instant messaging (IM) and Internet chat communication have seen enormous growth over the last several years. IM is the private network communication between two users, whereas a chat session is the network communication between two or more users. Chat sessions can either be private, where each user is invited to join the session, or public, where anyone can join the session. Although Instant Messaging (IM) services are quite mature and very popular as an instant way of communication over the Internet, they have become less secured over the period of time.

Android Operating System

Open Handset Alliance which is led by Google is the one which developed Android Operating system. It includes a large set of features for supporting mobile applications. It is basically used for running mobile applications. It consists of a kernel based on the Linux kernel, with middleware, libraries and APIs written in C and application software running on an Application Framework which includes Java compatible libraries based on Apache Harmony. To run compiled Java code, Android takes use of the Dalvik virtual machine with just-in-time(JIT) compilation. The Android development environment includes a device emulator, tools for debugging, memory and performance profiling, and a plug-in for the Eclipse IDE.

- *Saugat Poudel[1] , Olorunmo Taiwa Samuel[3] is currently pursuing bachelor degree program in ISE DEPT., at RRIT.*
- Vinod L.B[2] *is an Assistant Professor in ISE Dept at RRIT, Bengaluru- 90*

The programming language is Java. The emulator available in the Android SDK is a tool that allows developers to easily test applications without having to install it to a real device. With the proper configuration for an emulator, it is also possible to test situations which are hard to reproduce on a physical device.

II. LITERATURE SURVEY

With the increasing use of instant messaging as a communication tool, research have recently produced a lot of studies aimed at better understanding the impact of this communication interface on daily working tasks. IM appears as a communicative process aimed at maintaining a sense of connection, negotiating availability, and sustaining social interactions. Furthermore, in spite of the possibility for direct communication, several studies have found out that one of the primary goals for IM was the initiation of communication bridges to other media: IM is used to start a conversation after checking the recipient's availability, then the users switch to another media, like telephone, or real face-to-face conversation. Through the survey we can find that the number of user for instant messaging is increasing every day.

MOTIVATION OF INSTANT MESSAGING

Instant messaging now a day is being used by millions of user worldwide. According to the preferences people use different kind of IM. IM can be used for various purposes. It has a lot of advantages and disadvantages. Because of its disadvantages IM can be banned from some of the institutions. So a IM which is integrated in the institution over a Local Area Network

(LAN) can be used by students of those institution for study and other knowledge sharing purposes.

III. Analysis

A. Problem Definition

Although, Instant Messenger provides various services like phone call, video call, file transfer, they do not provide more secure way of doing so. Without proper security there is always risk of information leaking.

B. Aim

The aim of this project is to provide more secure way of Instant Messaging services to the student by linking it with the college website through a local area network connection.

C. Proposed System

We propose a system that uses a structured client server architecture as a mechanism for resource location and presence, but uses a store and forward mechanism to exchange the actual text messages, or whatever other sort of media is to be exchanged (voice, video, etc.). We wish to leverage to as great an extent as possible existing technology and protocols for both the client server and IM portion of the application.

IV. Design

A. Design constraints

The following characteristics constrain the design space of the IM system:

- Real time communication.
- An IM conversation between two people and allowing a person to be involved in multiple conversations at the same time.
- Messages are text based. File transfer is layered on top of that (more on this later)
- Connection over a network. The parties involved maybe in physically remote locations, but connected over a *network.

B. Design specifications

As a result of the listed constraints, the system would have the following properties:

1) Architectural pattern / style: Client-Server Architecture

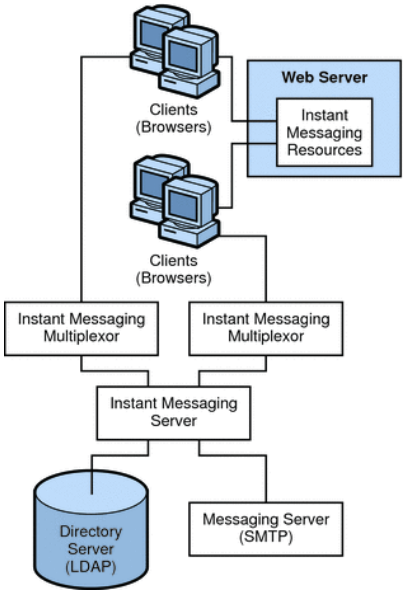

Fig4: Client Server Architecture

- This system will include a server component that handles the transfer of messages and other data, and a client component with a graphical user interface.
- The client is a program that opens a network connection with the IM server at a specified IP address and port number.
- The server is a program that accepts connections from clients. A server should be able to maintain an *unlimited number of open clients connections and clients should be able to connect and disconnect as they please.

2) Conversation

- An interactive data exchange session between two clients, a conversation, is the ultimate purpose of the system.

3) Client/Server Interaction

- A client and the server interact by making requests and responding using a custom communication protocol over another custom transport protocol. With this communication protocol, the user interface presented by the client should
- Provide a facility for joining the IM user s network.
- Provide a feature for starting a conversation.

- Provide a way to add other users to the contact list.
- Provide a facility for requesting info of other users.

4) Security

- Every user first creates an account; requiring a unique username (which cannot later be changed) and a password.
- The whole client/server interaction occurs over the Transport Layer Security (TLS) protocol.
- TLS is a cryptographic protocol designed to provide communication security over the Internet. It uses X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom it is communicating, and to exchange a symmetric key. This session key is then used to encrypt data flowing between the parties. This allows for data/message confidentiality and message authentication codes for message integrity and as a by-product, message authentication.
- As a result of choosing X.509 certificates, certificate authorities and a public key infrastructure are necessary to make sure the relationship between a certificate and its owner, as well as to create, sign, and manage and responsible for checking the validity of certificates.
- Since we are only trying to validate a connection to the server and not trying to establish trust to others we should not care about signing with a real CA.

We then have an option of using a form of certificate pinning i.e. Generate a self-signed certificate (SSC), install SSC into the root keystore on the client and setup the server to use certificate SSC.

5) Real time communication

- To achieve real time communication, the server must have a PUSH capability.
- The IM system will use a request-respond communication protocol over TCP/IP with SSL. This means a client can make requests and the server replies but not the other way around.
- How then does the server notify a client of a new message? Here are two different solutions. However, the second is selected.
- Polling

  The client repeatedly sends a request to fetch new messages. This is resource intensive and wasteful of CPU cycle.
- Notification Packets

When the server receives a message to be sent out to another client, it first sends out a UDP (user datagram protocol) packet to the client. UDP is an unreliable protocol and may not reach the client. This problem is solved by intermittently sending a notification packet until the new message is fetched. The sending of notification packets are designed to be idempotent.

V. PROTOCOL

Figv: Protocol used in IM

A. Communication Format

The communication format defines the syntax of requests and response between the server and a client. The client submits a request to the server. The server, which performs an operation specified in the request, returns a response message to the client.

Operations that the server supports are given identification numbers. A client then refers to an operation by its identification number to indicate the desired action to be performed on the supplied argument(s).

<Operation Request Code><argument list>

The server must reply with a response code, the identification number of the requested operation, and results of the operation if applicable.

<Response Code><Operation Request Code><result list>

For example, a server that supports an opera-

tion DIVIDE gives it identification number, e.g.109, and also expects two operands as arguments. A client can invoke a DIVIDE operation like

109 12 3

Which means divide 12 by3.The server's reply would be

0 109 4

0 indicates a success, 109 – the request code, and 4 –the result of the operation.

B. Wire Protocol

The communication format only defines how requests are formulated but does not specify how they are transferred.
A wire protocol refers to a way of getting data from point to point. It is needed if more than one application has to interoperate. In contrast to protocols at the transport level, the term 'wire protocol' describes a common way to represent information at the application level.

For this IM system, a byte based data transfer protocol is used. It defines a self-describing encoding scheme allowing interoperable representation of a wide range of commonly used types. The protocol was designed to facilitate cross-platform data exchange.

The wire protocol recognizes only primitive data types: byte, integer, long, double, Strings and binary large objects in the form of byte arrays. It also defines String to be encoded in UTF-8 and floating point numbers to use the IEEE 754 (IEC 60559) standard.

It can be regarded as a form of binary serialization where a group of data elements are encoded as a unit. Each data element is converted to its byte representation. For numeric values, Big-endian is defined as the standard byte ordering.

VI IMPLEMENTATION

A) SSL Certidicate

The SSL Certificate was generated using the Open SSL toolkit with the following command: The cert.crt file is converted to cert.bks (the format Android uses) using portecle-1.7 toolkit.

: If you installed OpenSSL in non-default directory, you MUST change paths in commands.
@echo off
set
OPENSSL_CONF=C:\OpenSSL\bin\openssl.cfg

B) Server Implementation

Requirements

Component	Requirements
.Net Framework	Version 4.0 and above
Operating System	Windows NT 6.0(Vista) and above
SQL server	Microsoft SQL Server 2008 R2 and subsequent versions

The server was implemented using the C# programming language. The functionality was broken down so as to be handled by different modules.
The modules include:

- Database module
- Network module
- User Interface module
- Worker Thread module

c) Client Implementation

Requirements

Component	Requirement
Android Framework	API level 14 (Ice Cream Sandwich) and above

The Android Client was implemented using the Java programming language. The main functionality was broken down so as to be handled by different components.
These include:

- TalkService
- Communicator
- Activities
- DatabaseHelper

VII REFERENCES

[1] R. Katz-Haas, "Ten guidelines for user-centered Web design," Usability Interface, vol. 5, no. 1, Jul. 1998. [Online]. Available: http:// www.stcsig.org/usability/newsletter/9807-webguide.html

[2] O. H. Juarez-Espinosa, "Development of user centered environmental software systems," Ph.D. Dissertation, Carnegie Mellon Univ., Pittsburgh, PA, 1999.

[3] X. Wu, "User-centered agents for structured information location on the Web," in Proc. 10th IEEE Int. Enterprise Distrib. Object Comput. Conf., 2006, p. 19.

[4] C. Xiong, Y. Fan, and M. Zhou, "QoS-aware Web service configuration," IEEE Trans. Syst., Man, Cybern. A, Syst., Humans, vol. 38, no. 4, pp. 888–895, Jul. 2008.[5] Christopher Brewster, Fabio

[5] Ciravegna, Yorick Wilks, " Background and Foreground Knowledge in Dynamic Ontology Construction : Viewing Text as Knowledge Maintenance,": Available http://eprints.aston.ac.uk/78/

[6] Ignazio Palmisano , Valentina Tamma , Luigi Iannone , Terry Payne paul , " Dynamic Ontology Evolution in Open Environments," : Available at http://ceurws.org/Vol401/iswc2008pd_submission_41.pdf

[7]Q. A. Liang, H. Lam, L. Narupiyakul, and P. C. K. Hung, "A rule- based approach for availability of Web service," in Proc. IEEE Int. Conf. Web Serv., 2008, pp. 153–160.

[8] Ibrahim M.Al-Nedhami, Pradeep K. Sinha, "A Privacy Framework for Composite Wed services,": Available at www.hpl.hp.com/india/senopt08/papers/senopt08101.pdf

[9] Christopher Brewster, Fabio Ciravegna, Yorick Wilks, " Background and Foreground Knowledge in Dynamic Ontology Construction : Viewing Text as Knowledge Maintenance,": Available http://eprints.aston.ac.uk/78/

[10] Baron, Naomi S., et al. 2003. "Tethered or Mobile? Use of Away Messages in Instant Messaging by American College Students." Forthcoming in Rich Ling and Per Pedersen, eds. Front Stage – Back Stage: Mobile Communication and the Renegotiation of the Social Sphere.Springer-Verlag.

[11] Tyson, Jeff. "How Instant Messaging Works." How Stuff Works. Electronic Document,http://computer.howstuffworks.com/instant-messaging.htm/.,2004