Map-Blogs Using Secure Parallel Communication through Internet on Real-Time Operations

A SUMMER INTERN PROJECT REPORT

Submitted By

A Vikramkumar	**B092633**
T Chittibabu	**R092478**
M Sravani	**N091869**

in partial fulfilment of Summer Internship for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

Computer Science and Engineering

Under the guidance of

Mr. P V Vinod,

Scientist/Engineer,

RRSC-S, ISRO

RAJIV GANDHI UNIVERSITY OF KNOWLEDGE TECHNOLOGIES

TELANGANA & ANDHRAPRADESH

July 2014

ABSTRACT

In an Internet environment, the risks to valuable and sensitive data are greater than ever before. And with the Internet continually growing, the threat to data travelling over the network increases exponentially. Network security threats may come externally from the Internet, or internally, where high numbers of attacks can actually originate. Intrusion detection systems (IDS) monitor networks and raises alarm when there is an attempt at an unauthorized entry into the network.

Mapblogs is an efficient method to deliver multimedia content from a sender to a group of receivers and is gaining popular applications such as real time stock quotes, interactive games, video conference, live video broadcast, or video on demand . Authentication is one of the critical topics in securing Map blogs in an environment attractive to malicious attacks.

In this project a asymmetric cryptography technique i.e., Digital Signature Algorithm(DSA) to provide the services like Data Integrity, Authenticity and Data Availability which helps in transferring data over network in our project through Internet . Mapblogs also provides live blogging system where there will be communication between clients using parallel computing were the queries of other clients can be posted and can be replied by group of clients through Internet access. Blogging system helps in the exchange information and converse with friends and family, to participate in group discussions through public news bulletin board. The live chatting application is integrated with a canvas board to exchange the drawings lively.

Another application is to send the files by dividing it into packets and signing the packets using DSA. To reduce the signature verification overheads in the secure MapBlogs, block-based authentication schemes have been proposed .Unfortunately, most previous schemes like RSA have many problems such as vulnerability to packet loss and lack of resilience to denial of service (DoS) attack which have been overcome in Mapblogs using DSA.

ACKNOWLEDGEMENT

It gives us utmost pleasure to have completed our Internship successfully. It is our duty and privilege to place on record our sincere gratitude to these people.

we would like to express our esteemed sense of gratitude and sincere thanks to our guide **Mr. P V Vinod, Scientist/Engineer, Regional Remote Sensing Centre - South, ISRO, Bangalore**, for his exemplary guidance and monitoring throughout the course of the Internship.

We are thankful to **Mr. Hebbar, Scientist/Engineer, RRSC-South, ISRO, Bangalore** for his immense encouragement, guidance during our internship period.

We would also like to take the opportunity to express our sincere gratitude and thanks to **Prof. R V Raj Kumar, Vice-chancellor of RGUKT** and **Dr. Uday Raj, General Manager, Regional Remote Sensing Centre – South**, **Bangalore**, for giving us an opportunity to work at this organization and we are obliged to all the staff of **RRSC-S/ISRO, Bangalore** for their cooperation during our internship.

We are extremely grateful to our **Faculty** for providing excellent academics and their invaluable guidance and suggestions all the time during undergraduate programs.

Lastly, we thank the almighty, our parents and friends for their firm support and encouragement without which this task would not have been achieved.

Vikramkumar Allakonda,

Chittibabu Tirupathi,

Sravani Murakonda.

Contents

TABLE OF FIGURES

Chapter 1

INTRODUCTION

Mapblogs is an efficient method to deliver text and multimedia content from a sender to a group of receivers and is gaining popular applications such as real time stock quotes, interactive games, video conferences, live video broadcast, or video on demand. Authentication is one of the critical topics in securing Mapblogs in an environment attractive to malicious attacks.

Mapblogs authentication may provide three security services such as data integrity, data origin authentication and Non repudiation. The sender generates a signature for each packet with its private key, which is called signing, and each receiver checks the validity of the signature with sender's public key, which is called verifying .If the verification succeeds, then the receiver knows the packet is authenticated .There are following issues in real world challenging the design .First, efficiency needs to be considered, especially for receivers. Compared with the Mapblogs sender, which could be a powerful server, receivers can have different capabilities and resources .Second, packet loss is inevitable. In the Internet, Constant service interruptions may be caused due to packet loss congestion at routers is a major reason causing packet loss. For messages sent through a non-secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by a claimed sender .Digital signatures are equivalent to traditional hand written signatures in many respects; properly implements digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret, so that even if the private key is exposed, the signature is valid .Efficiency and packet loss resilience can hardly be supported simultaneously by conventional Mapblogs schemes.

1.1 About Main Domain

Authentication is one of the critical topics in securing Mapblogs in an environment attractive to malicious attacks for securing the data through transmission in the internet. Basically, Mapblogs authentication may provide the following security services.

- ✓ **Data Integrity:** Data integrity means that data is protected from deletion and corruption, both while it resides within the database, and while it is being transmitted over the network and the assurance that data received are exactly as sent by an authorized entity.

- ✓ **Data origin Authentication:** Provides for the corroboration of the source of a data unit i.e., each user should be able to assure that each received packet comes from the real sender as it claims.
- ✓ **Non-repudiation:** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. All the three services can be supported by an asymmetric encryption technique called Digital signature. In an ideal case, the sender generates a signature for each packet with its private key which is called signing, and each receiver checks the validity of the signature with the sender's public key, which is called verifying .If the verification succeeds, the receiver knows the packet is authentic .
- ✓ **Live Blogging System:** Live blogging is basically posting regular updates to your blog as the event is taking place, rather than blogging about it after the fact. There will a communication between clients using parallel computing were the queries of other clients can be posted and can be replied by group of users within the network .Only clients who are already connected to the server can take part in blogging **.**Live blogging requires a bit of preparation that isn't necessary for regular blogging. The most important thing, of course, is internet access from the event. In this whenever the user completed to give one byte(8 bits) of input in the chatting room the data is transferred to all the other users , whoever logged into that room . Once if the sender selects the send button the message will be stored finally. If haven't selected send button while typing the message, then the sender can change the previously typed message and the changes will be done in other users accounts also in that chat room .The chat rooms are also provided with canvas board. If the user wants maintain a private chat room, then user can create his/her own room. Only the user who knows the room password can enter into the room to participate in discussion. If it is a public chat room anyone can participate in the discussion and can post messages to the chat room.
- ✓ **CANVAS:** There will be a drawing space or the canvas in other terms which lets clients draw real time figures .It also gives option to change colors, selecting different shapes and thickness and is even capable of drawing text .Using send file option, we can share any files with other users securely. Only clients who are already logged in with the server can take part in blogging.

1.2 Advantages and Limitations

1.2.1 Advantages

The advantages of using digital signatures include:

- ✓ **Imposter prevention :** By using digital signatures you are eliminating the possibility of committing fraud by an imposter signing the document .Since the digital signature cannot be altered .Digital signatures serves the purpose of authenticity in the communication network .Using digital signature frauds can be prevented and security issues can be resolved .
- ✓ **Message Integrity:** By having the digital signature you are in fact proving the documents to be valid. You are assuring the recipient that the document is free from forgery or false information.
- ✓ **Legal Requirements:** Using a digital signature satisfies some type of legal requirement for the document in question. A digital signature takes care of any formal legal aspect of executing the document.

WWW is called the World Wide Web.WWW supports many kinds of texts, pictures, video and audio formats. WWW resources through a web browser which basically a program that runs on the internet.

There are two kinds of browsers 1) text only browsers and 2) graphical browsers. Graphical browsers like Netscape Navigator and Internet Explorer are popular. These browsers provide you access a WWW server. The document is transferred to your computer and then the connection is terminated.

The World Wide Web is a network of information, accessible via an easy-to-use interface. The information is often presented in hypertext multimedia and provided by servers located around the world .The usability of the web depends on the performance of these servers.

This application is Java client/server combination, which can be used to chat over the Internet or local networks .With these features and with the advent of WWW, Web browsers and with “BLOGGING”, Internet has become the media of applications.

We can use “Blogging System” for the following activities:

- ✓ To exchange information and converse with friends and family.
- ✓ To participate in group discussions through public news bulletin board.
- ✓ For entertainment.
- ✓ Leisure activities.
- ✓ Access business while at home.
- ✓ Communicate and collaborate through pictures and messages.

- ✓ At any given point of time, up-to-date information is provided.

1.2.2 Limitations

- ✓ **Cost :** Digital signatures, even some of the simpler ones, come at a cost .You must have a necessary software to encode the signatures, and if you are using hardware so that customers can sign physically, then the cost goes up even further .Digital signatures are an additional cost that should be weighed against their potential security benefits .
- ✓ **Training and Troubleshooting:** If your employees aren't tech savvy or simply aren't sure how to use a digital signature, then you will have to spend time training them about how the signature process works. This will take them away from their jobs, costing you money .Additionally, as with all computer-related applications, sooner or later there will be a hiccough in the system and you will need someone to troubleshoot. If none of your employees can find and fix the problem, you will have to hire someone else to do it.
- ✓ **The correlation among packets** makes them vulnerable to packet loss, which is inherent in the internet and wireless networks. Moreover, the lack of denial of Service (DoS) resilience renders most of them vulnerable to packet injection in hostile environments.

1.3 Application Areas

1.3.1 Multimedia

It comes in many different formats. It can be almost anything you can hear or see like text, pictures, music, sound, video, records, films, animations and more. Multimedia elements also have their recorded and played, displayed or accessed by information content processing devices. Multimedia authentication deals with confirming the genuineness or truth of truth of the structure and/or content of multimedia.

Multimedia signal can be easily reproduced and manipulated .Although we cannot perceive the change, what we are seeing or listening to may have been changed maliciously for whatever reasons .Multimedia authentication is to confirm the genuineness or truth of the structure and/or content of multimedia .The first approach to multimedia authentication is cryptograph; while the second approach is the digital watermarking. In addition, cryptograph can be integrated into digital digital watermarking to provide more desirable authentication. It is worth mentioning that multimedia authentication is different from user authentication.

1.3.2 Video Conferencing

It is the conduct of a videoconference by a set of telecommunication technologies which allow two or more locations to communicate by simultaneous two-way video and audio transmissions. It has also been called ‘visual collaboration’ and is type of groupware.

Videoconferencing differs from videophone calls in that it’s designed to serve a conference or multiple locations rather than individuals. It is now possible to share your organization’s valuable and sensitive information with more people than ever before. The internet is a forum for public information exchange. Extranets provide suppliers and customers access to data that enhances their productivity. Remote workers have come to expect the same level of resources as if they were in the office. Innovations such as TRDDING’s firewall traversal solution are making it possible to communicate across boundaries.

But, with open communication comes risk. Network administrator’s site security as one of their highest concerns in managing communication tools. Financial institutions are constantly sharing information that must be restricted. The health care industry is overwhelmingly concerned with patient confidentiality. The fact is that any organization needs to protect its information as well as its resources. TANDBERG is a pioneer solution to resolve security concerns by addressing the issue of security three levels authentication, policy and encryption.

1.4 Objectives and Scope

1.4.1 Proposed System

- ✓ We propose a novel Mapblogs authentication protocol, namely MAPBLOGS, including two schemes.
- ✓ The basic scheme (MAPBLOGS) eliminates the correlation among the packets and thus provides the perfect resilience to packet loss and it is also efficient in terms of latency, computation and communication overhead due to an efficient cryptographic primitive called batch signature, which supports the authentication of any number of packets , simultaneously .
- ✓ In this clients can exchange the files like text files, video files, images etc. securely so that no one can view the real data in the network. In this we are dividing the file into packets and assigning the signature to each packet and at the receiver side the client browser will verify the packets and integrate them for the initial sending file using the concept Digital Signature.
- ✓ The proposed system’s premier feature is its whiteboard drawing utility .You can draw freehand , do circles , squares , lines , text , or paste image files to the canvas . This is

ideal when users want to “sketch” concepts for one another. This feature of “BLOGGING” can be a boon for the technical people who want to share their ideas or concepts in the pictorial form .This system includes the facilities of traditional chat servers and clients like providing a window for each Other user, Whisper chat, multiple chat rooms etc. With the help of the “WHITE BOARD” drawing utility now the technical people can carry out their tasks easily and can share their big picture plans regarding their business to the clients , exchange ideas and share their big picture plans regarding their business to the clients , exchange as well as share the information along with the using the drawing utility even long conversations can be made between two users which drawing utility even long conversations can be made between two users which may be important business meetings or deals to be sanctioned and all this is carried out with the support of applets with the help of image web menu images can be transferred .

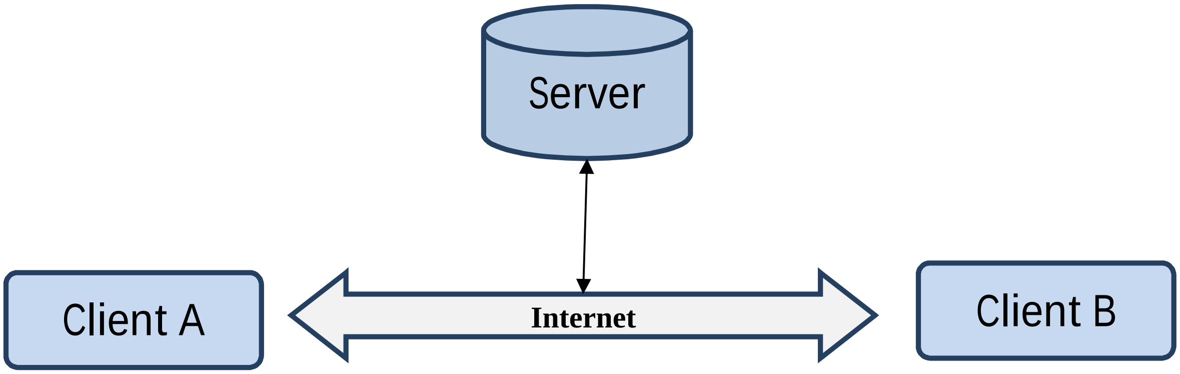


Figure 1.1: Basic Proposed System

Basic Scheme

The goal is to authenticate Mapblogs streams from a sender to multiple receivers. Generally, the sender is a powerful Mapblogs server managed by a central authority and can be trustful. The sender signs each packet with a signature and transmit it to multiple receivers through a Mapblogs routing protocol .Each receiver needs to assure that the received packets are really from the sender (authenticity) and the sender cannot deny the signing operation by verifying the corresponding signatures . Ideally , authenticating a Mapblogs stream can be achieved by signing and verifying each packet .However , the per-packet signature design has been criticized for its high computation cost , and therefore , most previous schemes incorporate a block based design .They do reduce the computation cost , but also introduce new problems .

The block design builds up correlation among packets and makes them vulnerable to packet loss, which is inherent in the internet and wireless networks. Received packets may not be authenticated because some correlated packets are lost. Also, the heterogeneity of receivers means that the buffer resource at each receiver is different and can vary over the time depending on the overall load at the receiver .In the block design , the required block size , which is chosen by the sender , may not be satisfied by each receiver .

Enhanced Scheme

An enhanced scheme called MAPBLOGS combines the basic scheme MAPBLOGS-B and a packet filtering mechanism to tolerate packet injection, the sender attaches each packet with a mark, which is unique to the packet and cannot be spoofed .At each receiver, the MAPBLOGS stream is classified into disjoint sets based on marks .Each set of packets comes from either the real sender or the attacker.

The mark design ensures that a packet from the real sender never falls into any set of packets from the attacker , and vice versa .Next , each receiver only needs to perform Batch Verify() over each set .If the result is true , the set of packets is authentic .If not , the set into smaller subsets for further batch verification . Therefore, a strong resilience to DoS due to injected packets can be provided.

1.4.2 Existing System

- ✓ Efficiency and packet loss resilience can hardly be supported simultaneously by 0conventional Mapblogs schemes.
- ✓ As is well known that existing digital signature algorithms are computationally expensive, the ideal approach of signing and verifying each packet independently raises a serious challenge to resource-constrained devices.
- ✓ They are suitable for RSA which is expensive on signing while cheap on verifying. For each packet, however, each receiver needs to perform one verification on its one-time or k-time signature plus one ordinary signature verification. Moreover, the length of one-time signature is too long(on the order of 1 , 000 bytes) .
- ✓ Existing block-based Mapblogs authentication schemes overlook the heterogeneity of receivers by letting the sender.
- ✓ Choose the block size
- ✓ Divide a Mapblogs stream into blocks
- ✓ Associate each block with a signature and spread the effect of the signature across all the packets in the block through hash graphs or coding algorithms.

There are some problems in existing digital signature algorithms .They are computationally expensive. There is also possibility of packet loss, packet forgery by attackers leading to Denial of Service. The approach of signing and verifying each block independently raises a serious challenge to E-source-constrained devices .Compared with the efficiency requirement and packet loss problems, the DoS attack is not common, but is still important in hostile environments.

1.5 Summary

This chapter provides a basic introduction to the MAPBLOGS .In MAPBLOGS by giving the batch signature to each packet separately we can ensure that the packets are successively received at the receiver end without any disturbance in the transmission medium .We can summarize that Mapblogs is an effective way to deliver a multimedia message from sender to a group of receivers. Some of the security services such as integrity, authentication and non-repudiation are provided by the Mapblogs. We can justify it from the point that in the existing system we faced problems like we can't achieve efficiency and resilience simultaneously which is overcome in Mapblogs stream by assigning and verifying each packet by giving them signature independently.

Chapter 2

LITERATURE SURVEY

Literature survey is the most important step in software development process .Before developing the tool it is necessary to determine the time factor , economy and company strength .Once these things are satisfied , then next step is to determine which operating system and language can be used for developing the tool .Once the programmers start building the tool , the programmers need lot of external support .This support can be obtained from senior programmers , from book or from websites . Before building the system the above consideration are taken into account for developing the proposed system.

2.1 Data Routing in Internet

Data travels across the internet in packets. Each packet can carry a maximum of 1, 500 bytes. Around these packets is a wrapper with a header and footer. The information contained in the wrapper tells computers what kind of data is in the packet, how it fits together with other data, where the data came from and the data's final destination. When you send an e-mail to someone, the message breaks up into packets that travel across the network. Different packets from the same message don't have to follow the same path. That's part of what makes the Internet so robust and fast. Packets will travel from one machine to another until they reach their destination. As the packets arrive, the computer receiving the data assembles the packets like a puzzle, recreating the message.All data transfers across the Internet work on this principle. It helps networks manage traffic -if one pathway becomes blogged with traffic, packets can go through a different route. This works for individual networks and the Internet as a whole. For instance, even if a packet doesn't make it to the destination, the machine receiving the data can determine which packet is missing by referencing the other packets. It can send a message to the machine sending the data to send it again, creating redundancy. This all happens in the span of just a few milliseconds.

2 .2 Mapblogs Routing Internetworks and Extended LANs

Mapblogs Routing, propose an efficient mechanism of sender access control for bidirectional Mapblogs trees in the IP Mapblogs service model .Each on-tree router maintains dynamically the access policy for its downstream senders.With this scheme, data packets from unauthorized hosts are discarded once they hit any on-tree router. As such,group members do not receive irrelevant data , and network service availability is guaranteed since the Mapblogs tree is protected from denial-of-service attacks such as data flooding from malicious hosts .In order to achieve scalability for large-scale Mapblogs applications with many information sources and in order to accommodate more concurrent Mapblogs sessions, we also extend our control mechanism to inter-domain routing where a hierarchical access policy is maintained on the bi-directional tree .

2 .3 Security Issue and Solution in Mapblogs Content Distribution

In security Issues and Solutions in Mapblogs Content Distribution , A survey we outline the various security and protection issues in Mapblogs content distribution .We focus on four areas of work , explain the issues and vulnerabilities that exist , and discuss the research that has been done on to provide solutions .Security in Mapblogs content distribution has matured over the years , but there remain open problem in the area that must be resolved to help Mapblogs enable more applications .

2 .4Batch Based Broadcast Authentication

Broadcast authentication is a critical security in wireless sensor networks(WSNs) , since it enables users to broadcast the WSN in an authenticated way .Symmetric key based schemes such as muTESLA and multilevel muTESLA have been proposed to provide such services for WSNs; however , these schemes all suffer from serious DoS attacks due to the delay in message authentication .This paper presents several effective public key based schemes to achieve immediate broadcast authentication and thus overcome the vulnerability presented in the nuTESLA-like schemes .

To prevent adversaries from injecting bogus messages, authentication is required for broadcast in wireless sensor network. muTESLA is a light-weight broadcast authentication protocol , which uses a one-way hash chain and the delayed disclosure of keys to provide the authentication service .However ,it suffers from several drawbacks in terms of time synchronization , limited broadcast rounds , key chain management at the source node .Therefore , a novel protocol is proposed called Batch-based Broadcast Authentication for wireless sensor networks .Batch-based broadcast Authentication does not require time synchronization , eliminates the requirement of key chain and supports broadcast for infinite rounds .

2 .5 Mapblogs Server Authentication Based(Batch signature)

We can justify our project statement by proposing new techniques for signing digital streams which deals with the problem of continuous authentication and signature of streams .An important requirement of our scheme , signature scheme is that the receiver can continuously verify the signature of packets .Clearly , the receiver can only verify the signature once it can trace the authentication links to a signature packet .Hence , the verification delay depends on the frequency and the transmission reliability of signature packets .The signature packet rate depends on the available computation and communication resources .

Mapblogs is an efficient method to deliver multimedia content from a sender to a group of games, video conference, live video broadcast or video on demand .Authentication is one of the critical topics in securing Mapblogs in an environment attractive to malicious attacks. Conventional block-based Mapblogs authentication schemes overlook the heterogeneity of receivers by letting the sender choose the block size, divide a Mapblogs stream into blocks , associate each block with a signature , and spread the effect of the signature across all the packets in the block through hash graphs or coding algorithms .The correlation among packets make them vulnerable to packet loss , which is inherent in the internet and wireless networks.Moreover, the lack of Denial of Service(DoS) resilience renders most of them vulnerable to packet injection in hostile environments.

2 .6 Summary

The development of software is done by the important step Literature survey .The considerations taken into account for developing the proposed system are:

Firstly, Mapblogs Routing in Internetworks and Extended LANs : here the data packets from unauthorized hosts are discarded once they hit any on-tree router .Secondly issues in Mapblogs content distribution : here we explain the issues and vulnerability that exists .Thirdly , Broadcast Authentication : It enables users to broadcast the wireless sensor networks in an authenticated way .Finally,Mapblogs authentication based on batch signature : The problems of continuous authentication and signature of streams can be proposed for signing digital streams, Mapblogs is an efficient method to deliver multimedia content from a sender to a group of receivers .

Chapter 3

SYSTEM REQUIREMENT SPECIFICATION

3 .1 Feasibility study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates .During system analysis the feasibility study of the proposed system is to be carried out .This is to ensure that the proposed system is not a burden to the company .For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are:

- ✓ Economical feasibility
- ✓ Technical feasibility
- ✓ Social feasibility

3 .1 .1 Economical feasibility

This study is carried out to check the economic impact that the system will have on the organization .The amount of fund that the company can pour into the research and development of the system is limited .The expenditures must be justified .Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available .Only the customized products had to be purchased.

3 .1 .2 Technical feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system .Any system developed must not have a high demand on the available technical resources .This will lead to high demands on the available technical resources.This will lead

To high demands being placed on the client .The developed system must have a modest requirement,as only minimal or null changes are required for implementing this system.

3 .1 .3 Social feasibility

The aspect of study is to check the level of acceptance of the system by the user.This includes the process of training the user to use the system efficiently .The user must not feel threatened by the system instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

3 .2 Software Requirements

Software requirements Specification(SRS) is an important part of software development process.SRS includes overall description, functional requirements, supportability, performance requirement, design constraints etc. For any application.This content is very much useful in fulfilling the goals while implementing software project.

A software requirement specification is a document which is used as a communication medium between the customer and the supplier.The complete description of the functions to be performed by the software specified in the SRS will assist the potential users to determine if the software specified meets their needs or how the software must be modified to meet their needs.Requirements must be measurable, testable, related to identified needs or opportunities, and defined to a level of detail sufficient for system design. This section of the SRS should contain all the software requirements , and testers to test that the system satisfies those requirements .With the help of software requirements we come to know the feasibility and the quality of software .To properly satisfy the basic goals , an SRS should have certain properties and should contain different types of requirements and below stated are some of the important requirements involved in developing software .System requirements should simply describe the external behaviour of the system and its operational constraints .

- Coding Language : Java servlets ,Applets, JSP , HTML
- Tool Used : Eclipse JEE
- Server : Apache Tomcat

3 .2 .1 Java Technology and Its Environment Settings

Java technology is both a programming language and a platform. The Java programming language is a high level language that can be characterized by all of the following buzzwords:

- Simple
- Object oriented
- Architectural neutral
- Portable
- Distributed
- High performance
- Interpreted
- Multithreaded

- ✓ Robust
- ✓ Dynamic

The Java Platform

A platform is the hardware or software environment in which a program runs .We've already mentioned some of the most popular platforms like windows 2000, Linux,Solaris and MacOS. Most of the platforms can be described as a combination of the operating system and hardware .The java platform differs from most other platforms in that it's a software-only platform that runs on top of other hardware-based platforms.

The java platforms has two components:

- ✓ The Java Virtual Machine
- ✓ The Java Application Programming Interface

You've already been introduced to the Java VM .It's the base for the Java platform and is ported onto various hardware based platforms .The Java API is a large collection of readymade software components that provide many useful capabilities, such as graphical user interface(GUI) widgets . The Java API is grouped into libraries of related classes and interfaces; these libraries are known as packages. Highlights what functionality some of the packages in the Java API provide.

Java Environment Settings :

Step1:DownloadJDK http://www.oracle.com/technetwork/java/javase/downloads/index.html

Step 2:Install JDK software

Step 3 Locate the JRE Installation Directory

Step 4: Set the JAVA_HOME Variable

- ✓ Right-click the **My Computer** icon on your desktop and select **Properties**.
- ✓ Click the **Advanced** tab.
- ✓ Click the **Environment Variables** button.
- ✓ Under **System Variables**, click **New**.
- ✓ Enter the variable name as JAVA_HOME.
- ✓ Enter the variable value as the installation path for the Java Development Kit.

  JAVA_HOME: C:\Program Files\Java\jdk1.x_x_x

  JRE_HOME: C:\Program Files\Java\JRE6 or JRE7
- ✓ Click **OK** and **Apply Changes**.
- ✓ Firefox should be enabled with Java to run Java web applications.

The following Figure 3.1 Java Platform depicts a program that's running on the Java platform .As the figure shows, the Java API and the virtual machine insulate the program from the hardware. As a platform-independent environment,the Java platform can be a bit slower than native code.

However, smart compilers, well-tuned interpreters, and just-in-time byte code compilers can bring performance close to that of native code without threatening portability.

Java has so many built in packages for providing security.In this project we concern mainly on providing security to the data in internet while data transmission .Java has a built in security package i.e. java.security Package useful for providing encryption and decryption of data.

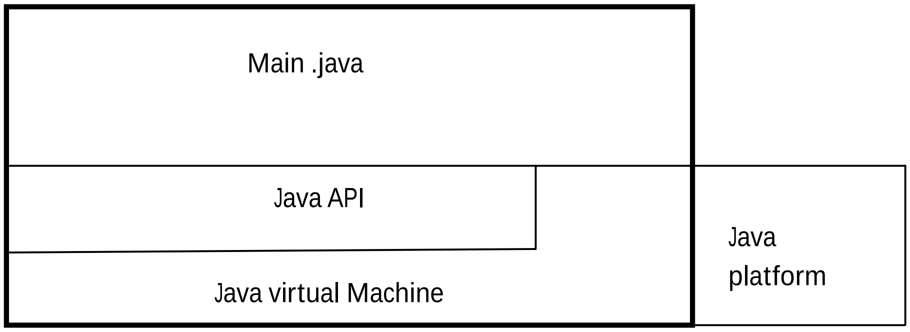


Figure 3.1 Java Platform

3.2.2 Servlets

In any J2EE web applications servlets are an integral part. The server side component of a servlets gives a powerful mechanism for developing server side web applications. It provides an important role in the explosion of Internet, its reusability, performance and scalability By using servlets web developers can run these applications in any servlet enabled web servers .The main advantages of using servlets over CGI are, the CGI programs are run outside the web server so a new process should be started before the execution of a CGI programs. At a time the CGI program ms handle only one request. After the execution of a CGI program they return the result in the web server and exit. But in the case of servlets it can handle multiple requests simultaneously. Servlets generate dynamic content or create dynamic web pages that is easy to write and faster to run within a web servers. Servlets can access any J2SE and J2EE APIs and it can take the full advantage and capabilities of the java programming language. Servlets are component based, platform independent method for create in the web based applications, without the performance limitations of CGI programs.

3 .2 .3 JSP

Java Server Pages (JSP) technology allows you to easily create static data , which can be expressed in any text-based format (such as HTML , SVG , WML , and XML) , and JSP elements , which construct dynamic content .JSP technology makes available all the dynamic capabilities of Java Servlet technology but provides a more natural approach to creating static content .

The main features of JSP technology are as follows:

- ✓ A language for developing JSP pages , which are text-based documents that describe how to process a request and construct a response
- ✓ An expression language for accessing server-side objects
- ✓ Mechanisms for defining extensions to the JSP language

3 .2 .4 HTML

HTML or Hypertext Mark-up Language is the standard mark-up language used to create web pages.

3.3 Apache Tomcat Server

Step 1:Tomcat should be installed before configuring it in Eclipse IDE.If you need to install Tomcat, you can download it from this location:http://tomcat.apache.org/download-70.cgi

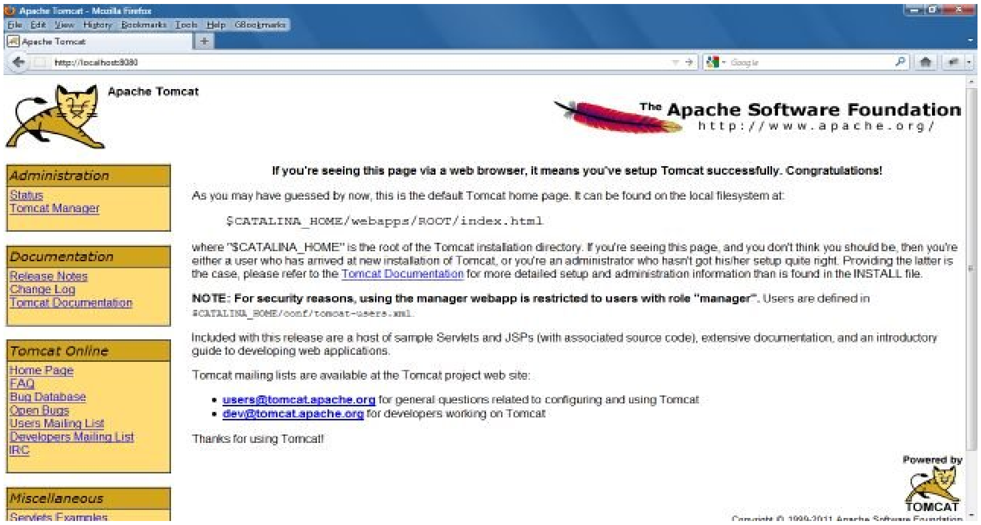
Download Apache Tomcat 7.0.23.zip file.

Step 2:To install Apache Tomcat, all you have to do is simply unzip the downloaded (.zip) file to a safe location on your machine. For simplicity and easy access, we recommend you to unzip Tomcat in “C:\” directory.

Step 3: Set CATALINA_HOME Variable to run the server

CATALINA_HOME=C:\Program Files\Apache Tomcat 7.0.23(path to tomcat server).

Step 4: Test the installation .Open browser and type http://localhost:8080. You should see the Apache Tomcat home page as shown below Figure 3.2 Apache Tomcat Home Page.



If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

```
$CATALINA_HOME/webapps/ROOT/index.html
```

where "$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the Tomcat Documentation for more detailed setup and administration information than is found in the INSTALL file.

NOTE: For security reasons, using the manager webapp is restricted to users with role "manager". Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`

Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation, and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Tomcat project web site:

- **users@tomcat.apache.org** for general questions related to configuring and using Tomcat
- **dev@tomcat.apache.org** for developers working on Tomcat

Thanks for using Tomcat!

Figure 3.2:Apache Tomcat Home Page

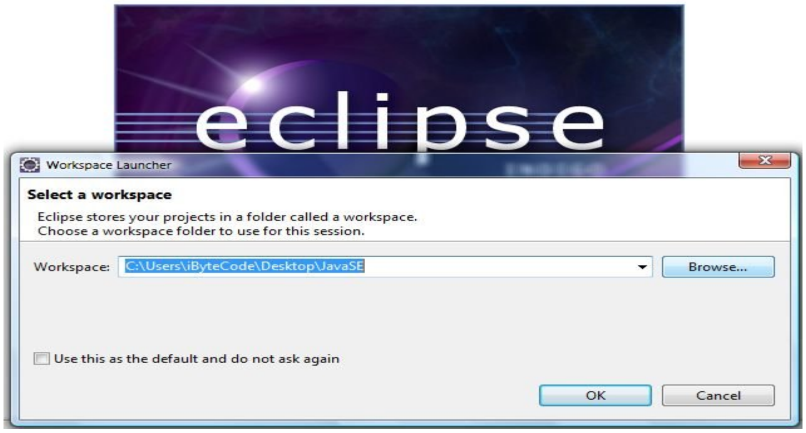
Step 5: Configuring Apache Tomcat with Eclipse JEE

3.4 Eclipse IDE

Step 1: Download Eclipse JEE zip from http://www.eclipse.org/downloads/and unzip the file in the root directory "C:\" and Eclipse would be installed in C:\eclipse.

Step 2:Launching Eclipse:In the eclipse folder you will find the eclipse.exe application (a big blue icon). You can double click on this to launch Eclipse IDE.

Step 3:Select the workspace used to keep project files and press OK to continue.



Select a workspace

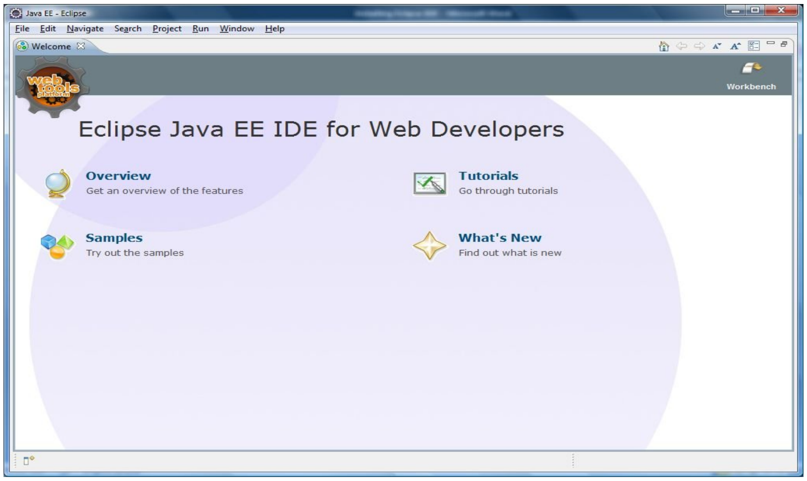
Eclipse stores your projects in a folder called a workspace.
Choose a workspace folder to use for this session.

Workspace: C:\Users\iByteCode\Desktop\JavaSE

□ Use this as the default and do not ask again

Figure 3.3: Eclipse Workspace

Step 4: After pressing OK, you will see the following window in Figure 3.4:Welcome Screen.



Eclipse Java EE IDE for Web Developers

Overview
Get an overview of the features

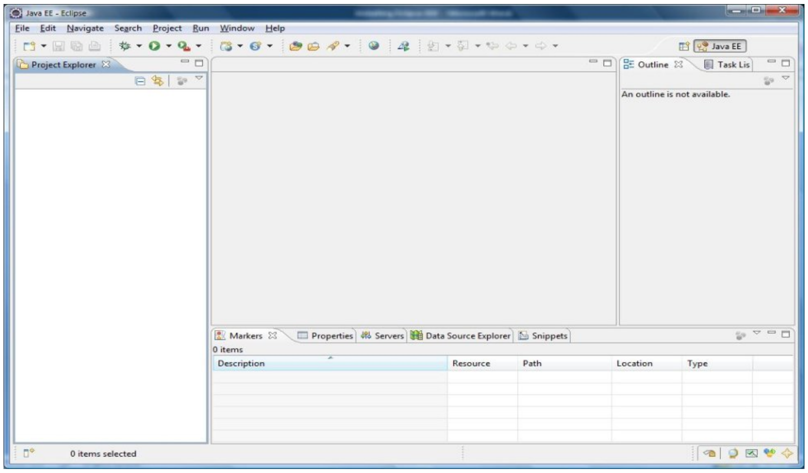
Tutorials
Go through tutorials

Samples
Try out the samples

What's New
Find out what is new

Figure 3.4:Welcome Screen

Step 5: To start working on Eclipse, you can either click on the curved arrow on the top right most corner or close the Welcome tab and you will see the following window in Figure 3.5: Workbench .



An outline is not available.

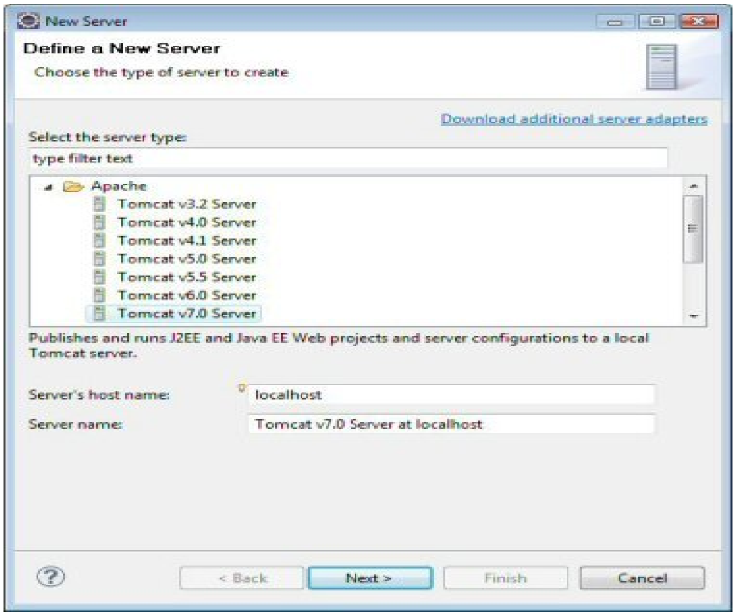
0 items

0 items selected

Figure 3.5:Workbench

3.4.1 Configuring Apache Tomcat in Eclipse IDE

Step 1: click on Servers tab at bottom. (If you don't see Servers tab, add the tab via Window, Show View, Servers.) Right-click on Servers tab, New, Server, Apache, Tomcat v7.0, navigate to the folder where you unzipped Tomcat (e.g., *C*:\apache-tomcat-7.0.34\), OK. You should now see "Tomcat v7.0 Server at localhost" listed under the Servers tab at the bottom as shown in the Figure 3.6:Server Set up.



Define a New Server

Choose the type of server to create

Select the server type:

type filter text

- Apache
  - Tomcat v3.2 Server
  - Tomcat v4.0 Server
  - Tomcat v4.1 Server
  - Tomcat v5.0 Server
  - Tomcat v5.5 Server
  - Tomcat v6.0 Server
  - Tomcat v7.0 Server

Publishes and runs J2EE and Java EE Web projects and server configurations to a local Tomcat server.

Server's host name: localhost

Server name: Tomcat v7.0 Server at localhost

Figure 3.6:Server Set up

Step 2:Click on Servers tab at bottom. R-click on Tomcat v7.0, choose "Start". Open http://localhost:8080/ as shown in Figure 3.7 :Start Server .

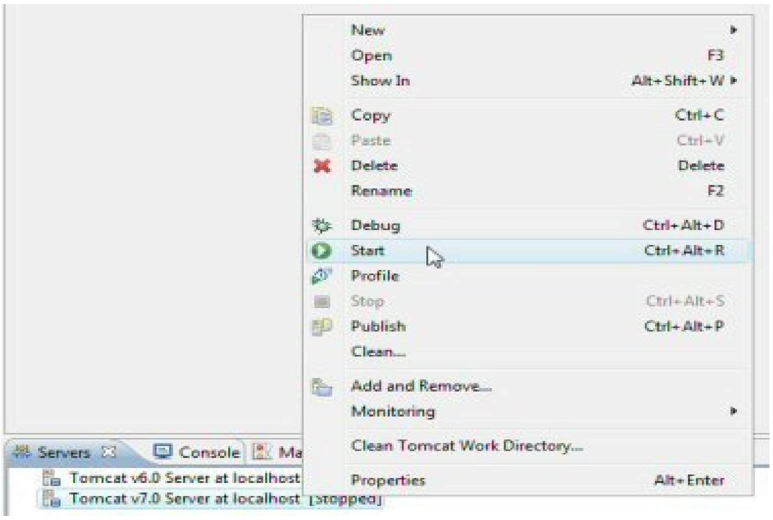
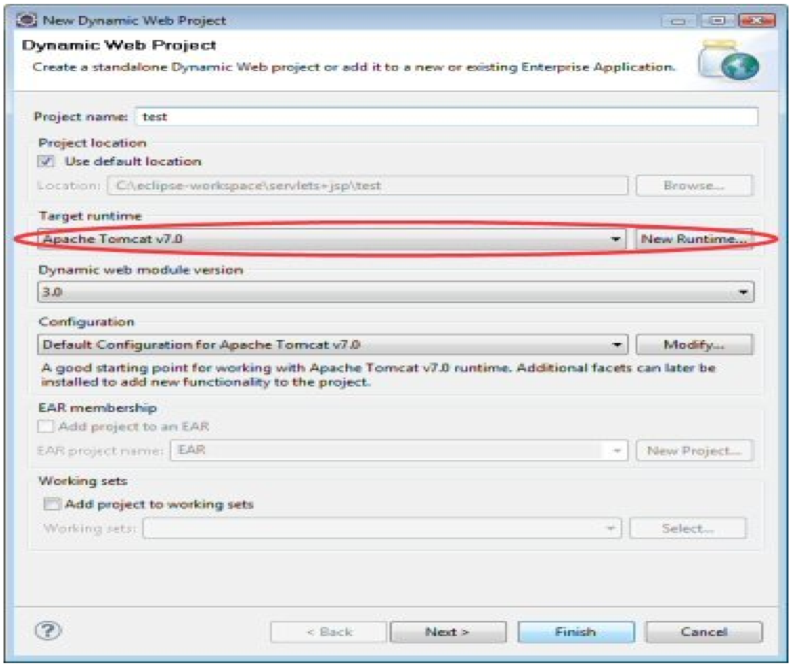


Figure 3.7: Start Server

3.4.2 Creating a Web application

Step 1: As shown in Figure 3.8: Create a Project

- ✓ Make empty project by navigating File-> New-> Project-> Web->Dynamic Web Project.
- ✓ Eclipse remembers the recent project types, so once you do this once, you can just do File, New, Dynamic Web Project.
- ✓ For "Target Runtime", choose "Apache Tomcat v7.0"
- ✓ Give it a name (e.g., "test").
- ✓ Accept all other defaults.


New Dynamic Web Project

Dynamic Web Project

Create a standalone Dynamic Web project or add it to a new or existing Enterprise Application.

Project name: test

Project location

☑ Use default location

Location: C:\eclipse-workspace\servlets+jsp\test

Target runtime

Apache Tomcat v7.0

Dynamic web module version

3.0

Configuration

Default Configuration for Apache Tomcat v7.0

A good starting point for working with Apache Tomcat v7.0 runtime. Additional facets can later be installed to add new functionality to the project.

EAR membership

☐ Add project to an EAR

EAR project name: EAR

Working sets

☐ Add project to working sets

Working sets:

Figure 3.8:Create a Project

Step 2:As shown in Figure 3.9:Adding codes to Project

- ✓ WebContent:Regular Web files (HTML, JavaScript, CSS, JSP, images, etc.)
- ✓ WebContent/some-subdirectory: Web files in subdirectory.
- ✓ WebContent/WEB-INF/lib:JAR files specific to application.
- ✓ src/testPackage: Java code in testPackage package. Make a package by R-clicking on "Java Resources: src" and doing New, package. Always make packages: use of the default package is strongly discouraged in Web apps.

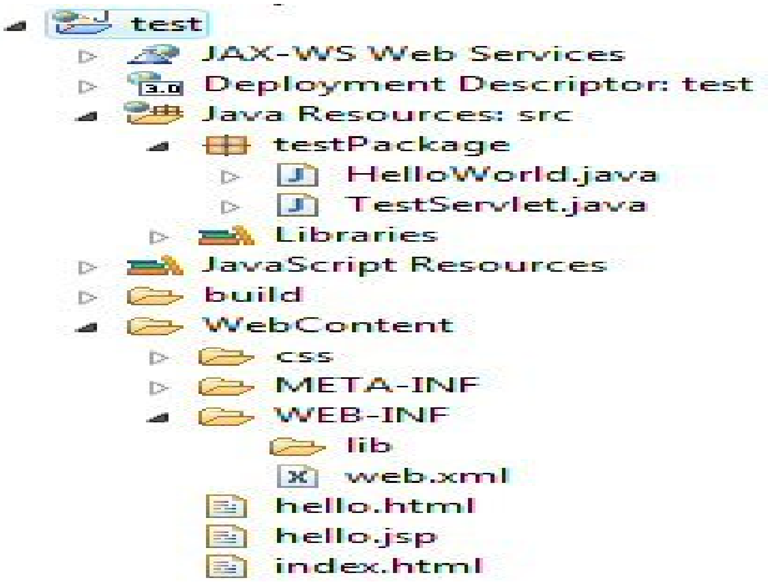


Figure 3.9: Adding codes to Project

3 .5 Networking

3 .5 .1 TCP/IP stack

The TCP/IP stack is shorter than the OSI one:

TCP is a connection-oriented protocol; UDP (User Datagram Protocol) is a connectionless protocol.

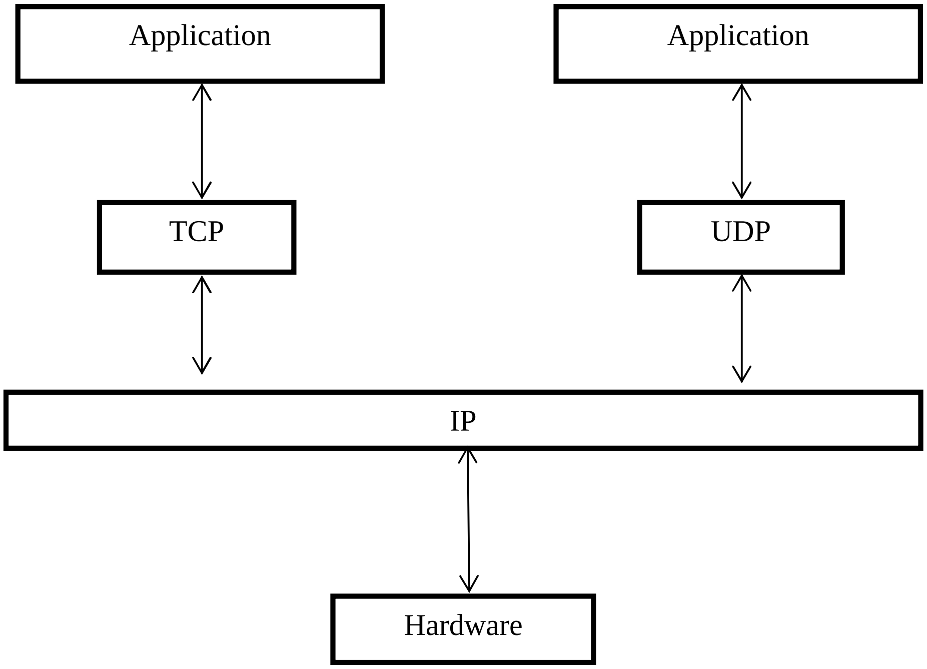


Figure 3.10: TCP/IP Stack

3 .5 .2 IP datagram's

The IP layer provides a connectionless and unreliable delivery system .It considers each datagram independently of the others .Any association between datagram must be supplied by the higher layers .The IP layer supplies a checksum that includes its own header .The header includes the source and destination addresses .The IP layer handles routing through the internet .It is also responsible for braking up large datagram into smaller ones for transmission and reassembling them at the other hand .

3 .5 .3 UDP

UDP is also connectionless and unreliable. What it adds to IP is a checksum for the contents of the User Datagram Protocol(UDP) is one for the Internet .With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data plans, datagram and port numbers .These are used to give a client/server model.

UDP uses a simple transmission model without handshaking dialogues for providing reliability ordering or data integrity. Thus, UDP provides an unreliable service and datagrams may arrive out of order, appear duplicated, or go missing without notice.UDP assumes that error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level.Time sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets , which may not be an option in a real-time system .If error correction facilities are needed at the network interface level , an application may use the Transmission Control Protocol (TCP) UDP applications use diagram sockets to establish host-to-host communications.An application binds a socket to its endpoint of data transmission, which is a combination of an IP address and a service port.A port is a software structure that is identified by the port number.

3 .5 .4 TCP

TCP supplies logic to give a reliable connection-oriented protocol above IP .It provides a virtual circuit that two processes can use to communicate.The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol suite.TCP is one of the two original components of the suite,complementing the Internet Protocol (IP), and therefore the entire suite is commonly referred to as TCP/IP. TCP provides reliable,ordered delivery of a stream of bytes from a program on one computer to another program on another computer.TCP is the protocol used by major Internet applications such as the World Wide Web ,email ,remote administration and file transfer .Other applications , which do not require reliable data stream service , may use the User Datagram Protocol (UDP) , which provides a datagram service that emphasizes reduced latency over reliability.The protocol actually corresponds to the transport layer of TCP/IP suite.TCP provides a communication service at an intermediate level between an application program and the Internet Protocol (IP). That is, when an application program desires to send a large chunk of data across the Internet using IP, instead of breaking the data into IP-sized pieces and issuing a series of IP requests,the software can issue a single request to TCP and let TCP handle the IP details .IP works by exchanging pieces of information called packets .A packet is a sequence of octets and consists of a header followed by a body.The header describes the packet’s destination and optionally the routers to use for forwarding until it arrives as its destination .The body contains the data IP is transmitting.

3 .5 .5 HTTP

The Hypertext Transfer Protocol - provides a standard for Web browsers and servers to communicate. The definition of HTTP is a technical specification of a network protocol that software must implement. HTTP is an application layer network protocol built on top of TCP. HTTP clients (such as Web browsers) and servers communicate via HTTP request and response messages. The three main HTTP message types are GET, POST, and HEAD. HTTP utilizes TCP port 80 by default, though other ports such as 8080 can alternatively be used.

3 .5 .6 Internet address

In order to use a service, you must be able to find it .The internet uses an address scheme for machines so that they can be located .The address is a 32-bit integer which gives the IP address .This encodes a network ID and more addressing .The network ID falls into various classes according to the size of the network address.

3 .5 .7 Network address

Class A uses 8 bits for the network address with 24 bits left over for other addressing .Class B uses 16 bit network addressing .Class C uses 24 bit network addressing and Class D uses all 32.

3 .5 .8 Subnet address

Internally,the UNIX network is divided into sub networks.Building 11 is currently on one sub network and uses 10-bit addressing, allowing 1024 different hosts.

3 .5 .9 Host address

8 bits are finally used for host addresses within our subnet .This places a limit of 256 machines that can be on the subnet.

3 .5 .10 Total address

The 32-bit address is usually written as 4 integers separated by dots.

137 .92 .11 .13

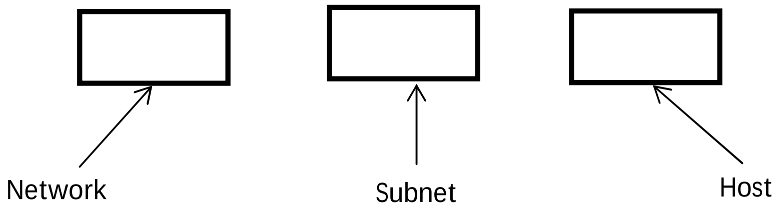


Figure: 3.11Total Address

3 .5 .11 Port address

A service exists on a host , and is identified by its port .This is a 16 bit number .To send a message to a server , you send it to the port for that service of the host it is running on .This is not location transparency Certain of these ports are “well known” .

3.5.12 Sockets

A socket is a data structure maintained by the system to handle network connections .A socket is created using the call socket.It returns an integer that is like a file descriptor. In fact, under Windows, this handle can be used with Read File and Write File functions.

```
                    #include<sys/types.gh>
                    #include<sys/socket.h>
int socket(int family, int type, int protocol);
```

Here “family” will be AF_INEF for IP communications, protocol will be zero, and type will depend on whether TCP or UDP is used. Two processes wishing to communicate over a network create a socket each. These are similar to two ends of a pipe – but the actual pipe does not yet exist.Like all other functionalities provided by Java, functionalities to work with sockets are also “packaged” and its classes.The following are the package and its main classes that help in accessing sockets:

1. java.net package
2. Server Socket
3. Socket

Java abstracts out most of the low-level aspects of socket programming.Here are the details.The java.net package contains all the classes required to create network enabled application.Server Socket and Socket are also part of this package .Apart from these classes, it also contains classes to connect to the web server, create secured sockets, and so forth.

The Server Socket class provides server sockets at server side/ such sockets wait for requests over the network.Once such requests arrive, a server socket performs operations based on the request and may return a result.The Server Socket class wraps most of the options required to create server-side sockets.The socket class provides client-side sockets or simply sockets.They are at the client side connecting to the server, sending the request to the server and accepting the returned result.Just as Server Socket exposes only the compulsory parameters required to create a server-side socket, similarly, Socket asks the user to provide only those parameters that are most necessary.This Socket serves the purpose of communication in the network; basically with the help of this data structure therefore one can handle network communication.

3 .6 Hardware Requirements

✓	System	: Pentium IV 2 .4 GHz.
✓	Hard Disk	: 40 GB.
✓	Floppy Drive	: 1 .44 Mb.
✓	RAM	: 256 MB

Chapter 4

SYSTEM DESIGN

Design is a strategic approach for someone to achieve a unique expectation.It defines specifications, plans, costs, activities, processes. A design approach is a general philosophy for specific approach to guide the overall goal of the design. Design is rarely perfect and sometimes repetitive. In this using live blogging chat application the server sends every byte data of the message from sender to receiver. Here the client is provided with canvas board option using that the client can draw the pictures and other can view it lively and the client can upload the files to the chat room, file uploaded after dividing it into to packets and signed is done. Mapblogs stream via the internet, where digitally signing takes place with the help of private key. The router forwards the packets to the clients and verification takes place using the public key at the client side.In this project the server sends the data packets to clients through internet to the specific clients using internet routing.

4.1 Architecture

Architecture is both the process and product of planning, designing and construction. Architectural works , in the material form of buildings , are often perceived as cultural symbols and as works of art .Historical civilizations are often identified with their surviving architectural achievements .Architecture is a medium of cultural expression displayed using a specific set of principles .These principles are meant to be interpreted so that the cultural of a period or nation can be fully expressed and understood.Architectural design is the initial design process of identifying sub-systems and establishing a framework for sub-system control and communication. Using large-grain components improves performance, and using fine-grain components improves maintainability, so if both of these are important system requirements developers should find some compromise solution .There is an overlap between the process of requirements engineering and architectural design.

Sub-system design is an abstract decomposition of a system into large-grain components, each of which may be a substantial system in its own right .Block diagrams are often used to describe sub-system designs where each box in the diagram represents sub-system. Sub-systems can have their own sub-systems; in that case boxes are laced into boxes. Arrows mean that data and/or control signal are passed from sub-system to sub-system in the direction of the arrows.

Architectural design is a creative process so many decisions are being made depending on requirements, specific rules for particular project and experience of an architect.

4.4.1 Flow Diagram

A data flow diagram(DFD) is a graphical representation of the "flow" of data through an information system , modeling its process aspects .Often they are a preliminary step used to create an overview of the system which can later be elaborated .DFDs can also be used for the visualization of data processing (structured design).

A DFD shows what kinds of data will be input to and output from the system, where the data will come from and go to, and where the data will be stored. It does not show information about the timing of processes or information about whether processes will operate in sequence or in parallel .In our project we are having three levels.

- ✓ Level 0: Server and client connects through internet
- ✓ Level 1: Data transfer from client to Server
- ✓ Level 2: Data transfer from server to client

Level 0: Server and Client connects through Internet

In level 0, the clients connect to server through internet, where the server is already connects to internet. Therefore the connections between server and clients are done by establishing a communication channel over internet .The clients exchange the messages and data through server in the communication channel over internet.

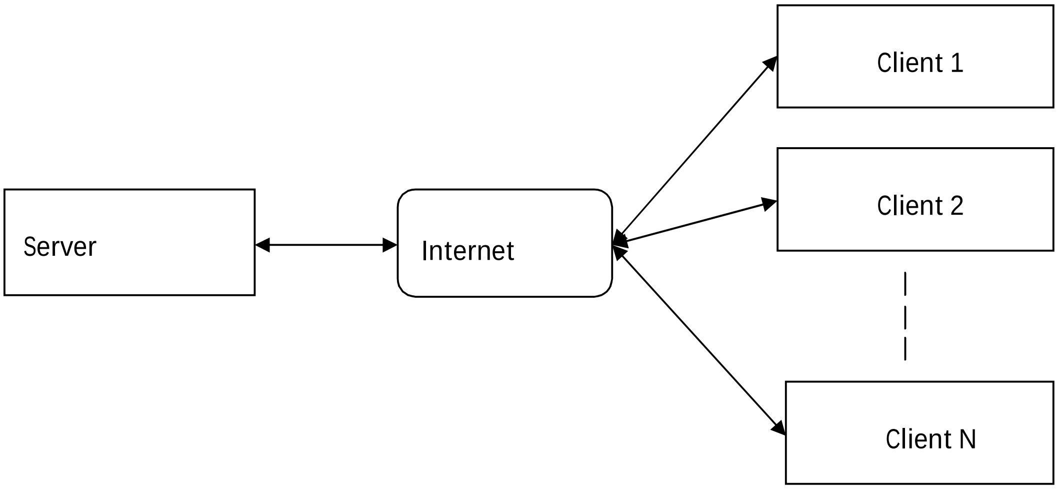


Figure 4.1: Server and Client connects through Internet

Level 1:Data Transfer from Client to Server

In this level 1, we see how the client uploads the file to the server. In this the client uploads a file to the sever .The file is divided into packets of size 1 KB after that it is signed with a digital signature using private key of the sender. The signing will apply a batch signature on the packets. Then the digitally signed packet enters into the internet network and stored in the server. Server makes it accessible to all the clients in the chat room.

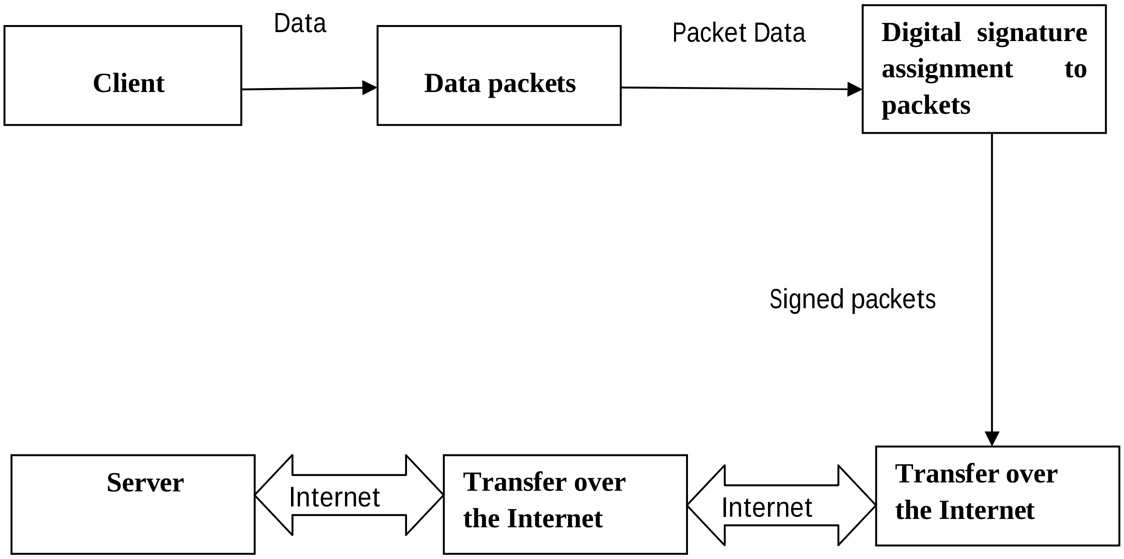

Client
Data
Data packets
Packet Data
Digital signature assignment to packets
Signed packets
Server
Internet
Transfer over the Internet
Internet
Transfer over the Internet

Figure 4.2:Data Transfer from Client to Server

Level 2:Data Transfer from Server to Client

In level 2, we see how the data transfer from server to client .The client access the file from server in the chat room and the signed packets over the internet received by the client and at the client side the signed packets are verified by using the public key and integrates all the packets to get the original data file. If the verification is done successfully then the data is not modified in the network while transmission.

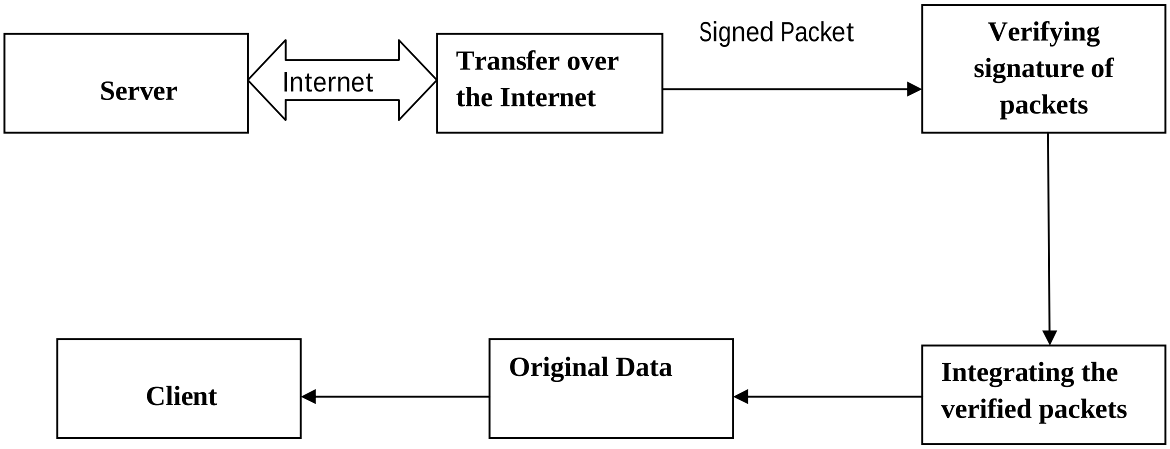

Server
Internet
Transfer over the Internet
Signed Packet
Verifying signature of packets
Client
Original Data
Integrating the verified packets

Figure 4.3: Data Transfer from Server to Client

4.1.2 Use Cases

Use cases describe the behaviour of the system when one of these actors sends one particular stimulus. A use case diagram is an excellent way to communicate to management, customers and other non-development people what a system will do when it is completed. According to our project we have three actor server, client and internet. For each actor we have a use case diagram.

Server

According to this , Server connects with clients .Server does all the use case actions like connecting with clients over internet , Splitting data into packets and assigns batch signature , receiving data packets from clients and sending data packets to clients .

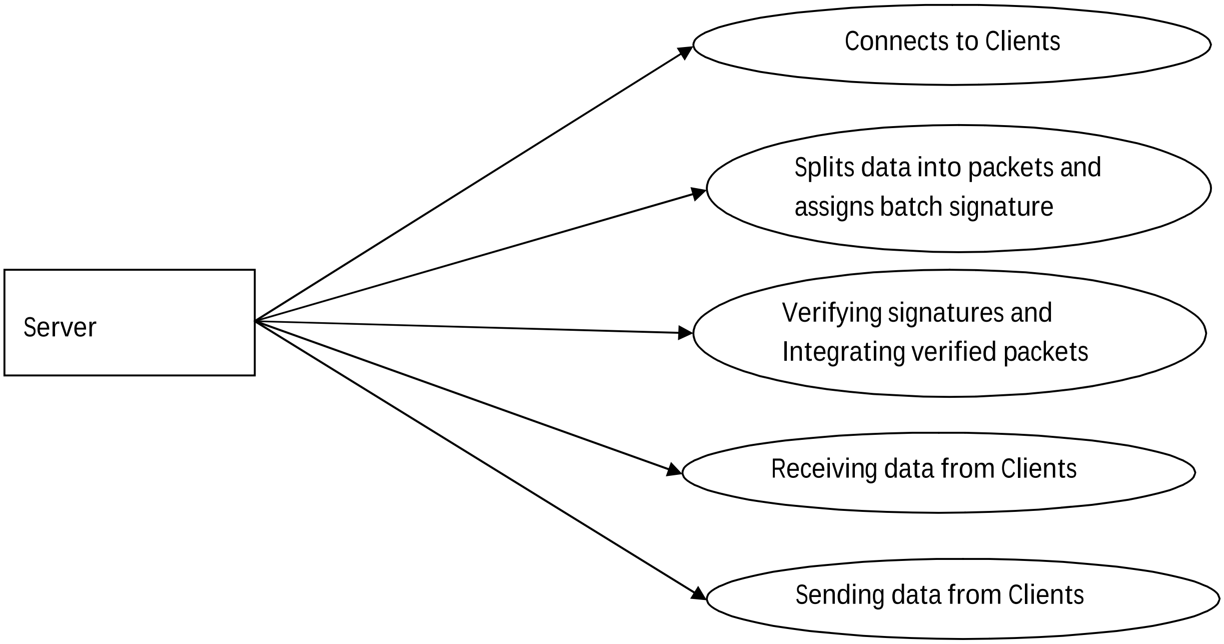

Server
Connects to Clients
Splits data into packets and assigns batch signature
Verifying signatures and Integrating verified packets
Receiving data from Clients
Sending data from Clients

Figure 4.4: Use case Diagram for Server

Client

According to this,Client connects with server .Client can do all the actions mentioned in the use case diagram. Client can create a chat room, login into a chat room.Client can perform actions like sending data i.e., messages, files and can use canvas board facility etc. to other clients through server and can receive the data from other clients.

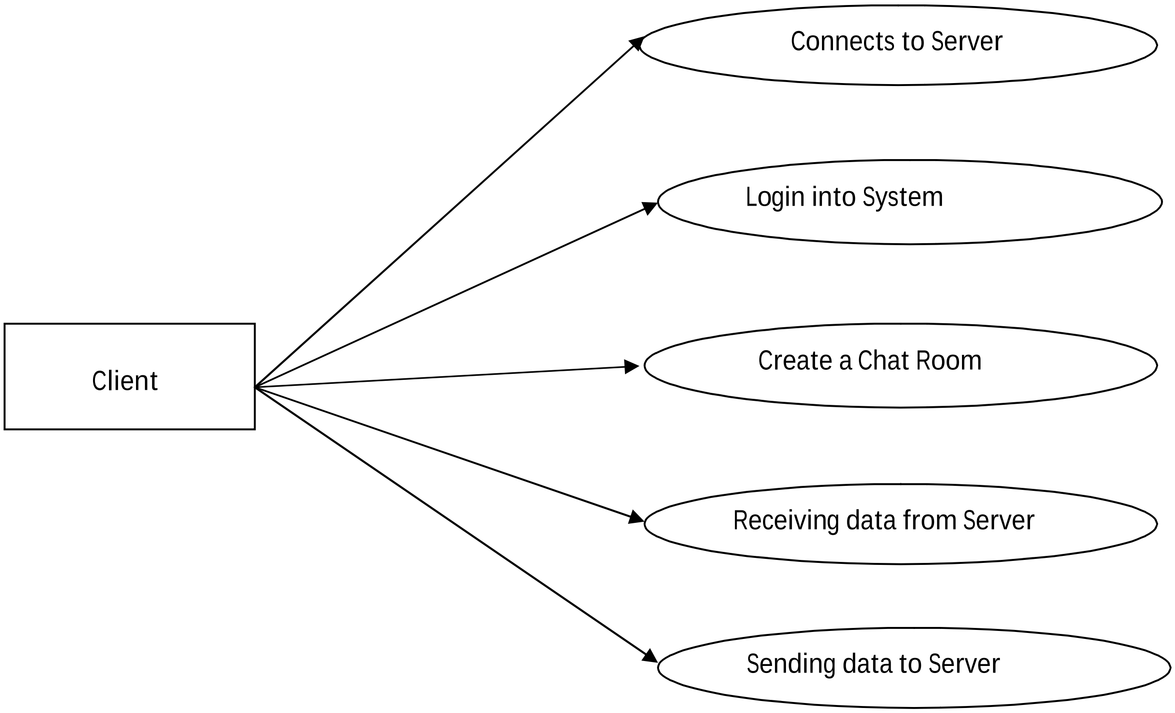


Figure 4.5: Use case Diagram for Client

Internet

According to this, Internet connects server with clients.It acts as medium between server and client to exchange data. It forwards data packets from client to server vice-versa.

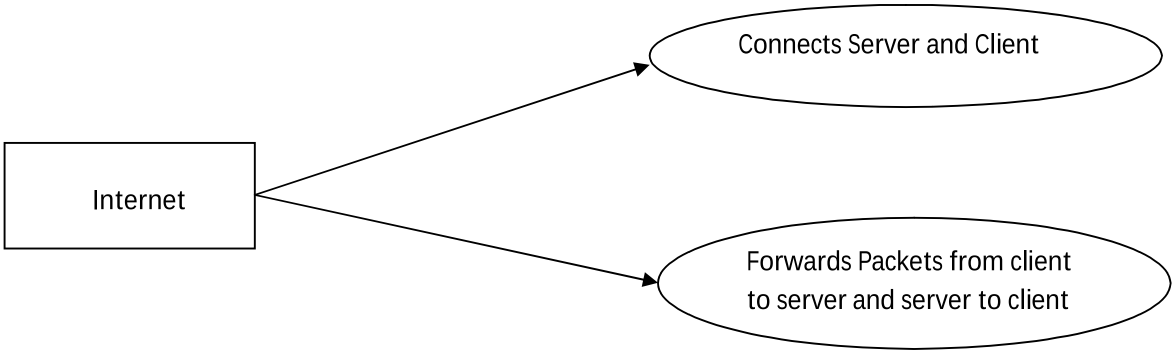

Internet
Connects Server and Client
Forwards Packets from client
to server and server to client

Figure 4.6:Use case Diagram for Internet

4.1.3 Sequence Diagram

Sequence diagrams typically are associated with use case realizations in the Logical view of the system under development. Sequence diagrams are sometimes called event diagrams , event scenarios and timing diagrams .In this when the client request the server to sign the data the client just request to sign the data but don't send the original message to server for signing.

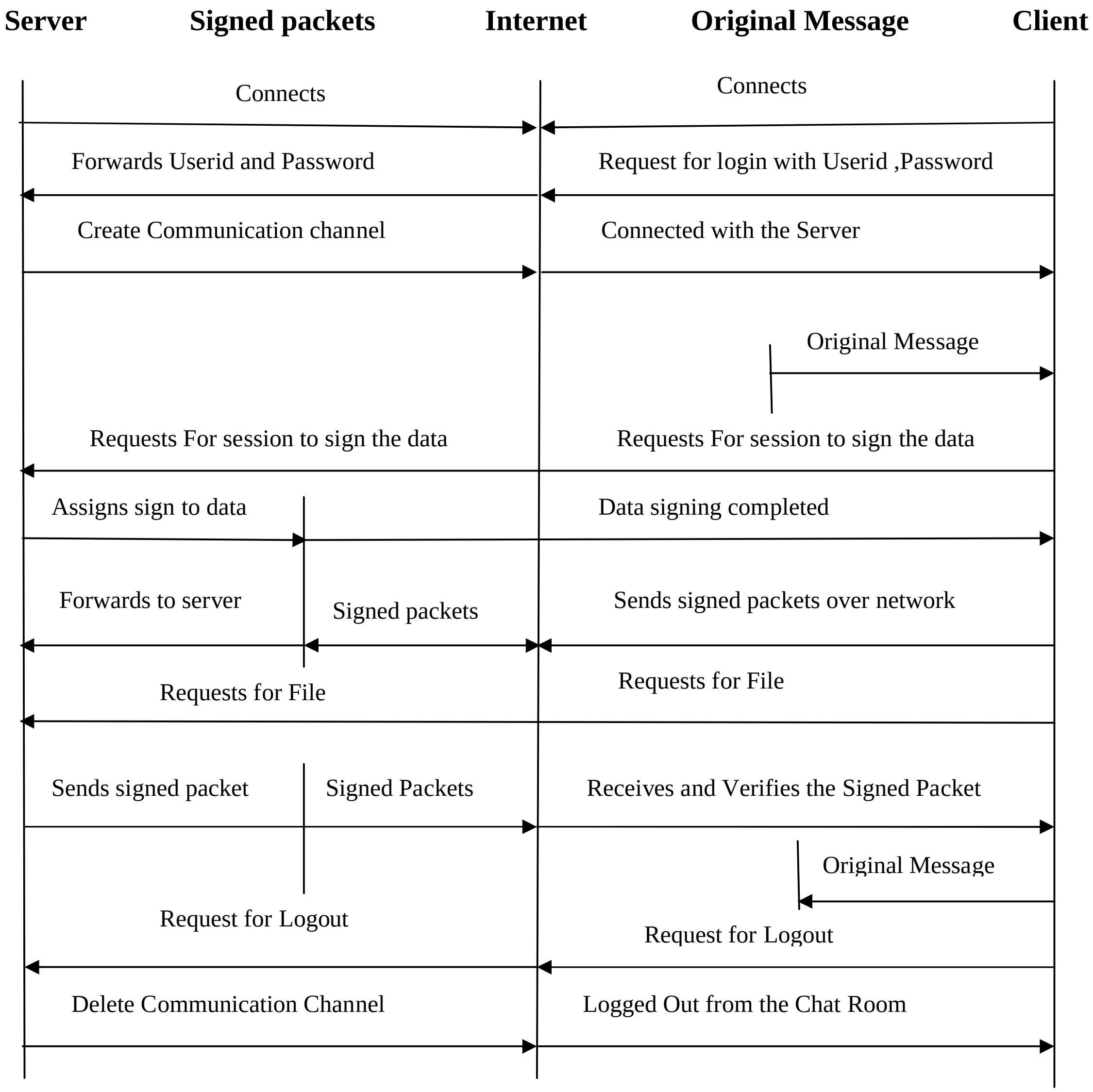

Server
Signed packets
Internet
Original Message
Client
Connects
Connects
Forwards Userid and Password
Request for login with Userid ,Password
Create Communication channel
Connected with the Server
Original Message
Requests For session to sign the data
Requests For session to sign the data
Assigns sign to data
Data signing completed
Forwards to server
Signed packets
Sends signed packets over network
Requests for File
Requests for File
Sends signed packet
Signed Packets
Receives and Verifies the Signed Packet
Original Message
Request for Logout
Request for Logout
Delete Communication Channel
Logged Out from the Chat Room

Figure 4.7:Sequence Diagram for Server and Client actions

4.2 System Design

According to our system design the packets are sent from server to clients. Firstly at client side the data is transmitted over internet. During the transmission it divides the data into packets and applies batch signature to the data packets. The internet forwards the data packets to server .Then the server forwards the data packets to other receivers .At receiver side the data packets are verified using the public of sender and if the verification is done correctly then the data packets are received by client by integrating all the packets. If the packets are not properly signed and matched then those packets are discarded and other packets which matches correctly are received and finally message is delivered to receivers.

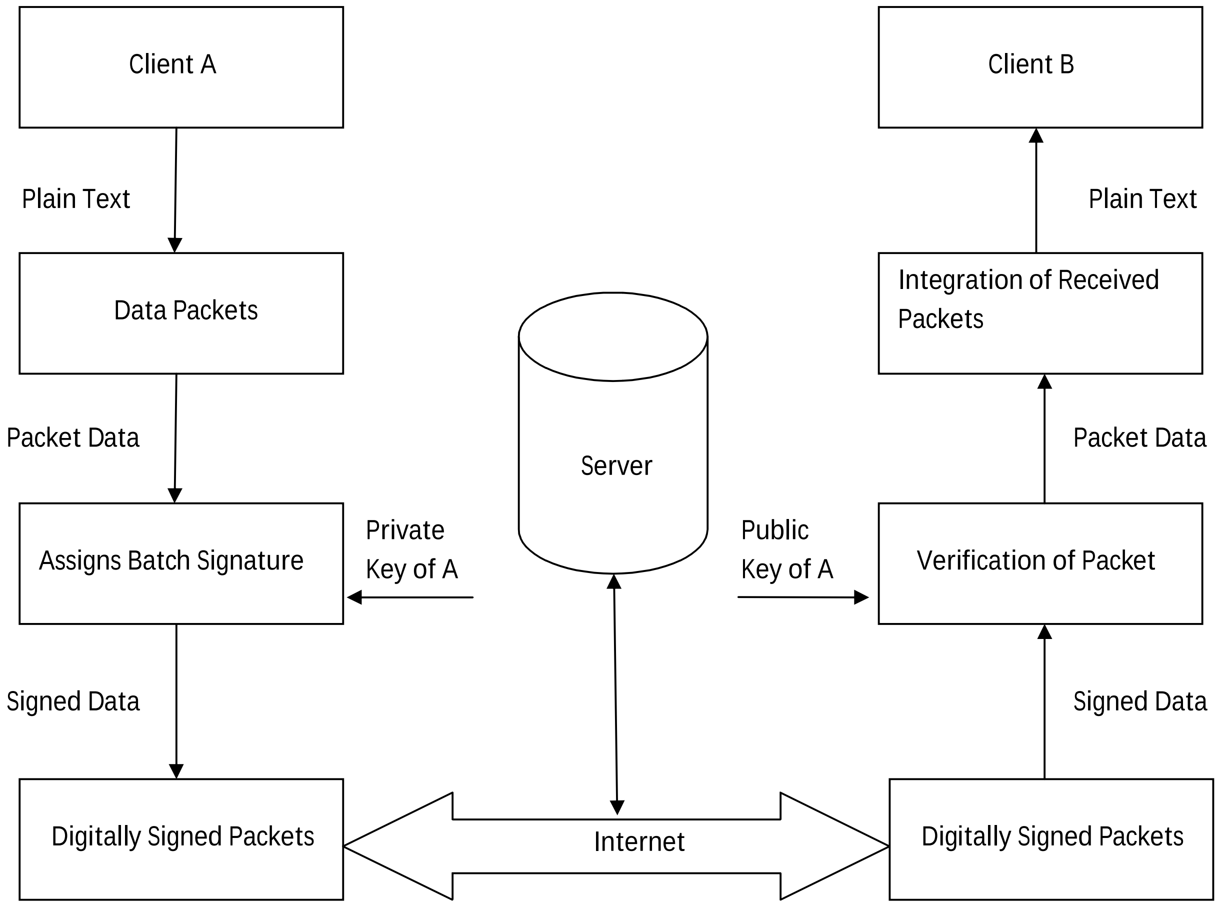


Figure 4.8: System Design for Data Transmission

4.3 Modules

1. Server
2. Client
3. Internet

4.3.1 Server Module

A server machine is a high performance host that is running one or more server programs which share its resources with clients .Client-server computing or networking is a distributed application architecture that partitions tasks or workloads between service providers (servers) and service requesters, called clients.Often clients and servers operate over a computer network on separate hardware .When discussing networks, different conceptual views can be used. One view is how the computers and networks are connected to one another and another view is a layered view of how the protocols operate on top of each other. A server is a computer that serves information to other computers. These computers, called clients, can connect to a server through either a local area network (LAN) or a wide area network (WAN), such as the Internet.

There are a number of different types of servers, including Web servers, mail servers, and file servers. A web server serves Web pages to computers that connect to it. It also can parse scripting languages such as PHP, ASP and JSP.A mail server stores users email accounts and sends and receives e-mail messages .For example, when you send an e-mail to a friend, the message is sent by a mail server, using the SMTP protocol. A file server is a computer that stores files that can be accessed by other computers .File servers are often used within local networks and typically require password or some kind of authentication to connect to it. Server used in this project shows which clients are connected in the chat room. It has an option to send the files to the chat room and any client who logged into the chat room can access the file. It also has an option to do live chatting with an option canvas board where the client can send the canvas board drawings lively.

4.3.2 Client

A client is a computer that allows a user or users to log on to the network and take advantage of the resources available on the network .A client computer will make a client operating system. The purpose of the client is to get user onto the network; therefore, client computers don’t usually have the processing power, the storage space, or the memory found on a server because the client does not have to serve up resources to other computers on the network.

We have implemented the client, such that the client can access and view the data in the logged chat room .Chat room has files uploaded by the clients and other can access the files .The client checks for the validity of the packets by verifying the signature on the packets with the help of public key .This ensures that the data has not been manipulated. Once the verification is done, data is decrypted and shown on the client side. Any desired client can enter the live blogging system and communicate parallel with other clients.

4.3.3 Internet

Data travels across the internet in packets. Each packet can carry a maximum of 1, 500 bytes. Around these packets is a wrapper with a header and footer. The information contained in the wrapper tells computers what kind of data is in the packet, how it fits together with other data, where the data came from and the data's final destination.When you send an e-mail to someone, the message breaks up into packets that travel across the network. Different packets from the same message don't have to follow the same path. That's part of what makes the Internet so robust and fast. Packets will travel from one machine to another until they reach their destination. As the packets arrive, the computer receiving the data assembles the packets like a puzzle, recreating the message.All data transfers across the Internet work on this principle. It helps networks manage traffic -if one pathway becomes blogged with traffic, packets can go through a different route. This works for individual networks and the Internet as a whole. For instance, even if a packet doesn't make it to the destination, the machine receiving the data can determine which packet is missing by referencing the other packets. It can send a message to the machine sending the data to send it again, creating redundancy. This all happens in the span of just a few milliseconds.

4.4 Summary

In system design it mainly explains how the system has been designed .Architecture design tells how the system is constructed, designed etc.; it gives overview of how the input is given at the sender and how efficiently the clients receive those packets. Architectural design is the initial design process of identifying sub-systems and establishing a framework for sub-system control and communication. Systems design is simply the design of systems. It implies a systematic and rigorous approach to design –an approach demanded by the scale and complexity of many systems problems .System design tell how the server transfers the packets to the clients by using internet as the medium for transmission by applying batch signature and how those packets are finally received by the clients .

Chapter 5

IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user,confidence that the new system will work be effective.

The implementation stage involves careful planning,investigation of the existing system and it’s constraints on implementation,designing of methods to achieve change over and evaluation of change over methods.

5.1 Functionalities

1. DSA key generation
2. Digital signature (sending packets)
3. Signature verification (receiving packets)
4. LIVE Blogging System
5. CANVAS Board

5.1.1 DSA key generation

Key generation has two phases .The first phase is a choice of algorithm parameters which may be shared between different users of the system:

In the original DSS,H was always SHA-1 ,but the stronger SHA-2 hash functions are approved for use in the current DSS .The hash output may be truncated to the size of a key pair.Decide on a key length L and N.This is the primary measure of the cryptographic strength of the key.The original DSS constrained L to be a multiple of 64 between 512 and 1024 (inclusive).Recommends lengths of 2048 (or 3072) for keys with security lifetimes extending beyond 2010 (or 2030) ,using correspondingly longer N[3] specifies L and N length pairs of (1024,160),(2048,224),(2048,256) and (3072,256).

Key generation is the process of generating keys for cryptography .A key is used to encrypt and decrypt whatever data is being encrypted/decrypted. Modern cryptographic systems include symmetric-key algorithms use a single shared key ,keeping date secret requires keeping this key secret.Public-key algorithms use a public key and a private key.The public key is made available to anyone(often by means of a digital certificate).A sender encrypts data with the public key, only the holder of the private key can decrypt this data.Since public-key algorithms tend to be much slower than symmetric-key algorithms, modern systems such as TLS and SSH use a combination of the two : one party receives the other’s public key , and encrypts a small piece of data (either a symmetric key or some data used to generate it).The remainder of the conversation uses a (typically faster) symmetric key algorithm for encryption .Computer cryptography uses integers for keys.In some cases keys are randomly generated using a random number generator(RNG) or pseudorandom number generator(PRNG).A PRNG is a computer algorithm that produces data that appears random under analysis.PRNGs that use system entropy to send data generally produce better results,since this makes the initial conditions of the PRNG much more difficult for an attacker to guess. In other situations , the key is created using a passphrase and a key generation algorithm, usually involving a cryptographic hash function such as SHA-1 .The public key is ‘hard’ knapsack , and the private key is an ‘easy’ , or super increasing ,knapsack, combined with two additional numbers , a multiplier and a modulus , which were used to convert the super increasing knapsack into the hard knapsack.These same numbers are used to transform the use of the subnet of the hard knapsack into the sum of the subnet of the easy knapsack, which is solvable in polynomial time.

To encrypt a message , a subnet of the hard knapsack is chosen by comparing it with a set of nits(the plaintext) equal in length to the key , and making each term in the public key that corresponds to a 1 in the plain text an element of the subnet ,while ignoring the terms corresponding to 0 terms in plain text.The elements of this subset are added together and the resulting sum is the cipher text.Decryption is possible because the multiplier and modulus used to transform the easy,super increasing knapsack into the public key can also be used to transform the number representing the cipher text into the sum of the corresponding elements of the super increasing knapsack.Then, using a simple greedy algorithm, the easy knapsack can be solved using O(n) arithmetic operations, which decrypts the message.

5.1.2 Digital Signature (sending packets)

Digital signatures employ a type of asymmetric cryptography.For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signatures schemes in the sense used here are cryptographically based, and must be implemented properly to be effective.

Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature,but not all electronic signature use digital signature use digital signatures. In some countries, including United States, India and members of European union, electronic signatures have legal significance. Digital signatures employ a type of asymmetric cryptography. For messages sent through a non-secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claim sender.

Digital signatures are equivalent to traditional hand written signature in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer can’t successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless.

5.1.3 Signature verification (Receiving Packets)

Signature verification may be performed by any party (i.e., the signatory, the intended recipient or any other party) using the signatory’s public key. A signatory may wish to verify that the computed signature is correct, perhaps before sending the signed message to the intended recipient. The intended recipient (or any other party) verifies the signature to determine its authenticity.

Prior to verifying the signature of a signed message, the domain parameters, and the claimed signatory’s public key and identity shall be made available to the verifier in an authenticated manner. The public key may, for example, be obtained in the form of a certificate sign by a trusted entity (e.g., a Certification Authority) or in a face-to-face meeting with the public key owner. Asceria’s ADSS Server product range is based on the industry-accepted concept of delegating complex security, PKI and digital signature functionality to trusted server applications.

Ascertia’s ADSS Server is based on industry accepted protocols for communicating with an e-Trust server, including OASIS Digital Signature Specifications (DSS and SDD-X) for server-side signing and verification, W3C XML Key Management Specifications (XKMS) for certificate validation, IETF Online Certificate Status Protocol for real-time revocation status checking, IETF TSP for communicating with a Time Stamping Authority and IETF Long-Term Archive & Notary Service (LTANS) for secure data archiving. Ascertia ADSS Server can verify a wide range of digital signature formats as shown here. It also complies with the latest EU PEPPOL project requirements for online Validation Authorities.

5.1.4 LIVE Blogging System

Live blogging is basically posting regular updates to your blog as the event is taking place, rather than blogging about it after the fact. There will a communication between clients using parallel computing were the queries of other clients can be posted and can be replied by group of users with in the network .Only clients who are already connected to the server can take part in blogging **.**Live blogging requires a bit of preparation that isn’t necessary for regular blogging. The most important thing, of course, is internet access from the event. In this whenever the user completed to give one byte(8 bits) of input in the chatting room the data is transferred to all the other users , whoever logged into that room . Once if the sender selects the send button the message will be stored finally. If haven’t selected send button while typing the message, then the sender can change the previously typed message and the changes will be done in other users accounts also in that chat room .The chat rooms are also provided with canvas board . If the user wants maintain a private chat room, then user can create his/her own room. Only the user who knows the room password can enter into the room to participate in discussion. If it is a public chat room anyone can participate in the discussion and can post messages to the chat room.

5.1.5 CANVAS BOARD

Drawing utility now the technical people can carry out their tasks easily and can share their big picture plans regarding their business to the clients, exchange ideas exchange ideas exchange as well as share the information along with the using the drawing utility even ling conversations can be made between two users which may be important business meetings or deals to be sanctioned and all this is carried out with the support of applets with the help of image based web menu images can be transferred. And many more things, basically.

5.3 Summary

Network module describes the communication between the sender and the receiver based on how they send and receive the message. In DSA key generation we come across how the keys are generated by using the cryptographic has function and how these keys are implemented base on the hash function. Digital signature helps to sign each packet digitally and send them to receiver. Signature verification verifies each signature independently at the receiver end and sees that all the packets are received correctly.

Chapter 6

SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product.

6.1 Types of Tests

6.1.1. Unit Testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated.

Unit testing usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases.

Test strategy and approach

Field testing will be manually and functional tests will be written in detail.

Test objectives

- ✓ All field entries must work properly
- ✓ Forms must be activated from the identified link
- ✓ The entry screen, messages and responses must not be delayed.
- ✓ Data sent and received are matching are not.
- ✓ Data is received by the actual receiver or not.

Features to be tested

- ✓ Verify that the entries are of the correct format
- ✓ No duplicate entries should be allowed
- ✓ All links should take the user to the correct page
- ✓ Unauthenticated user can’t enter the chat room.
- ✓ Private chat rooms are accessible only those users who knows it’s password.

6.1.2 Integration testing

Integration tests are designed to test integrated components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields.

Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully aimed at exposing the problems that arise from the combination of components.

Software integration testing is the internal integration of two or more integrated software components on a single platform to produce failures caused by interface defects. The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up –software applications at the company level-interact without error.

Test Results: All the test cases mentioned above passed successfully .No defects were encountered.

Table 6.1 Integration Testing

Test Case	**Input**	**Expected Result**	**Actual Result**	**Status**
Connectivity to Website	URL or IP of the Website	Connects with WebServer	Connected to WebServer	Pass
File Uploading	File	File should be stored as signed data packets	File is stored as signed packets in the server	Pass
File Downloading	Packets	Signed packets are integrated to build file	All packets integrated and Downloaded as a file	Pass
Live Chatting	Stream of Characters	Send each character to the server and displayed on the screen.	Sending data is displayed on the screen	Pass
Canvas	Draw	Auto Display in other clients	Visible	Pass

6.1.3 Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirement, system documentation, and user manuals.

Functional testing is cantered on the following items:

Valid Input: Identified classes of valid input must be accepted.

Invalid Input: Identified classes of invalid input must be rejected.

Functions: Identified functions must be exercises.

Output: Identified classes of application outputs must be exercised.

Systems/Procedures: Interfacing systems or procedures must be involved.

6.1.4 Acceptance Testing

User acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

User acceptance testing (UAT), is the term used when the acceptance tests are performed by the person or persons who will be using the live system once it is delivered. If the system is being built or developed by an external supplier, this is sometimes called customer acceptance testing (CAT).

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

6.2 Summary

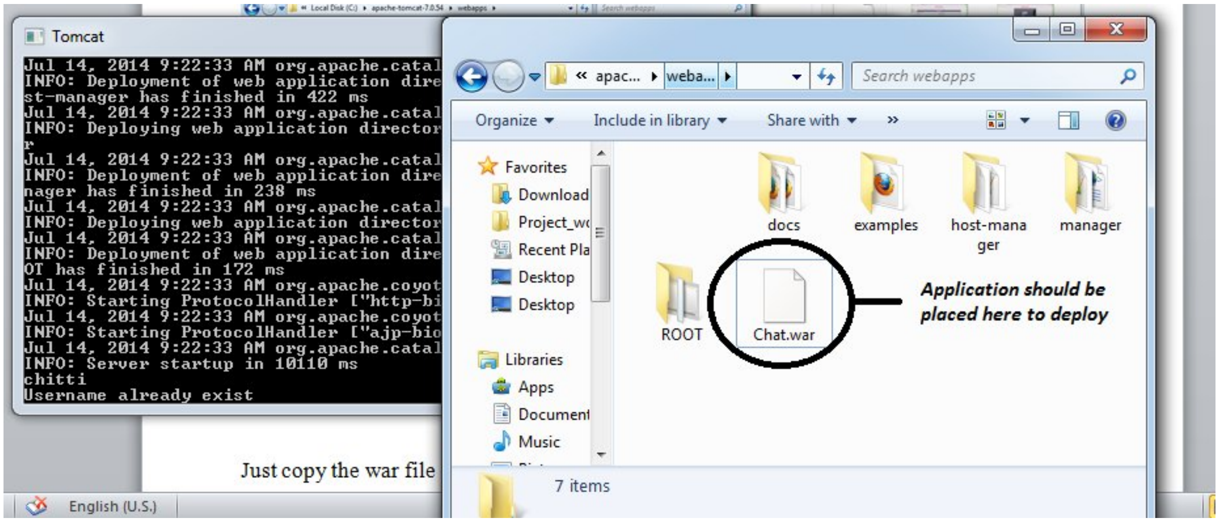
System testing of software or hardware is testing conducted on a complete, integrated system to evaluate the system’s compliance with its specified requirements. System testing falls within the scope of black box testing , and as such , should require no knowledge of the inner design of the code or logic .As a rule, system testing takes, as its input , all of the “integrated” software components that have passed integration testing and also the software itself integrated with any applicable hardware system.

The purpose of integration testing is to detect any inconsistencies between the software units that are integrated together (called assemblages) or between any of the assemblages and the hardware. System testing is a more limited type of testing; it seeks to detect defects both within the “inter-assemblages” and also within the system as a whole.

Chapter 7

RESULT AND RESULT ANALYSIS

7.1 Deployment

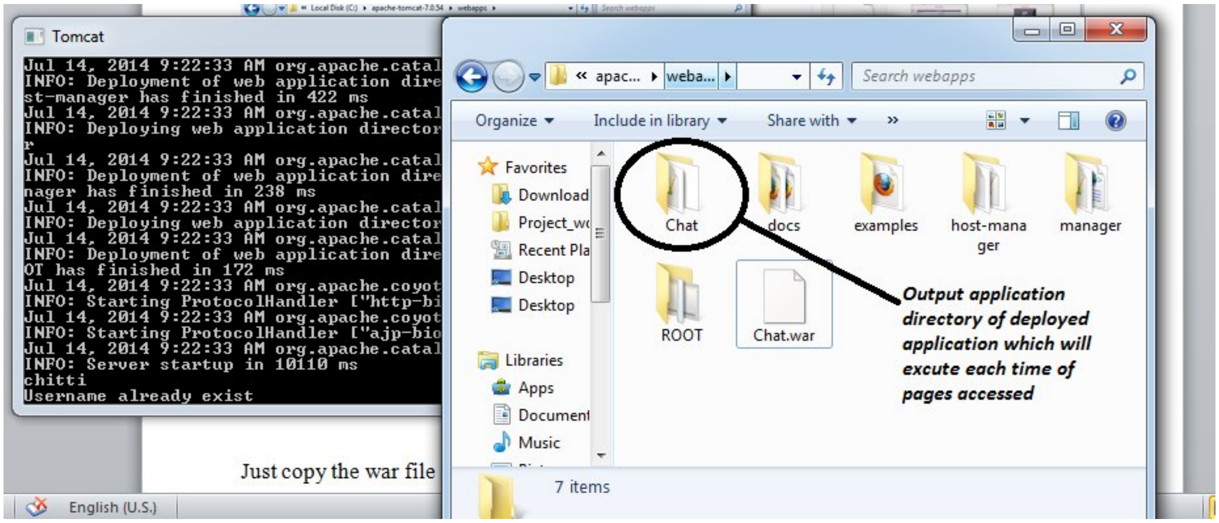


```
Jul 14, 2014 9:22:33 AM org.apache.catal
INFO: Deployment of web application dire
st-manager has finished in 422 ms
Jul 14, 2014 9:22:33 AM org.apache.catal
INFO: Deploying web application director
r
Jul 14, 2014 9:22:33 AM org.apache.catal
INFO: Deployment of web application dire
nager has finished in 238 ms
Jul 14, 2014 9:22:33 AM org.apache.catal
INFO: Deploying web application director
Jul 14, 2014 9:22:33 AM org.apache.catal
INFO: Deployment of web application dire
OT has finished in 172 ms
Jul 14, 2014 9:22:33 AM org.apache.coyot
INFO: Starting ProtocolHandler ["http-bi
Jul 14, 2014 9:22:33 AM org.apache.coyot
INFO: Starting ProtocolHandler ["ajp-bio
Jul 14, 2014 9:22:33 AM org.apache.catal
INFO: Server startup in 10110 ms
chitti
Username already exist
```

Application should be placed here to deploy

Figure7.1 Deployment

Just copy the war file into the webapp folder of apache-tomcat (Path is **"C:\apache-tomcat-7.0.54\webapps"**) as shown in the Figure 7.1.



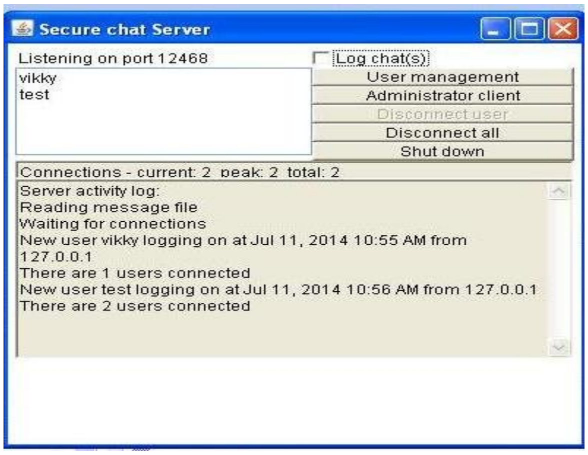
```
Jul 14, 2014 9:22:33 AM org.apache.catal
INFO: Deployment of web application dire
st-manager has finished in 422 ms
Jul 14, 2014 9:22:33 AM org.apache.catal
INFO: Deploying web application director
r
Jul 14, 2014 9:22:33 AM org.apache.catal
INFO: Deployment of web application dire
nager has finished in 238 ms
Jul 14, 2014 9:22:33 AM org.apache.catal
INFO: Deploying web application director
Jul 14, 2014 9:22:33 AM org.apache.catal
INFO: Deployment of web application dire
OT has finished in 172 ms
Jul 14, 2014 9:22:33 AM org.apache.coyot
INFO: Starting ProtocolHandler ["http-bi
Jul 14, 2014 9:22:33 AM org.apache.coyot
INFO: Starting ProtocolHandler ["ajp-bio
Jul 14, 2014 9:22:33 AM org.apache.catal
INFO: Server startup in 10110 ms
chitti
Username already exist
```

Output application directory of deployed application which will excute each time of pages accessed

Figure7.2 Deployment

7.2 Running Server

Run Startup.bat to start apache-tomcat Server which is located in “**C:\apache-tomcat-7.0.54\bin**” **.** There is a need for running other server to connect users for utilizing the service of Canvas technology. For this we should go the directory “**C:\apache-tomcat-7.0.54\webapps\Chat**”in that folder run the bat file named as “**command.bat”.** After running the bat file we get the pop-up shown in the Figure 7.3.

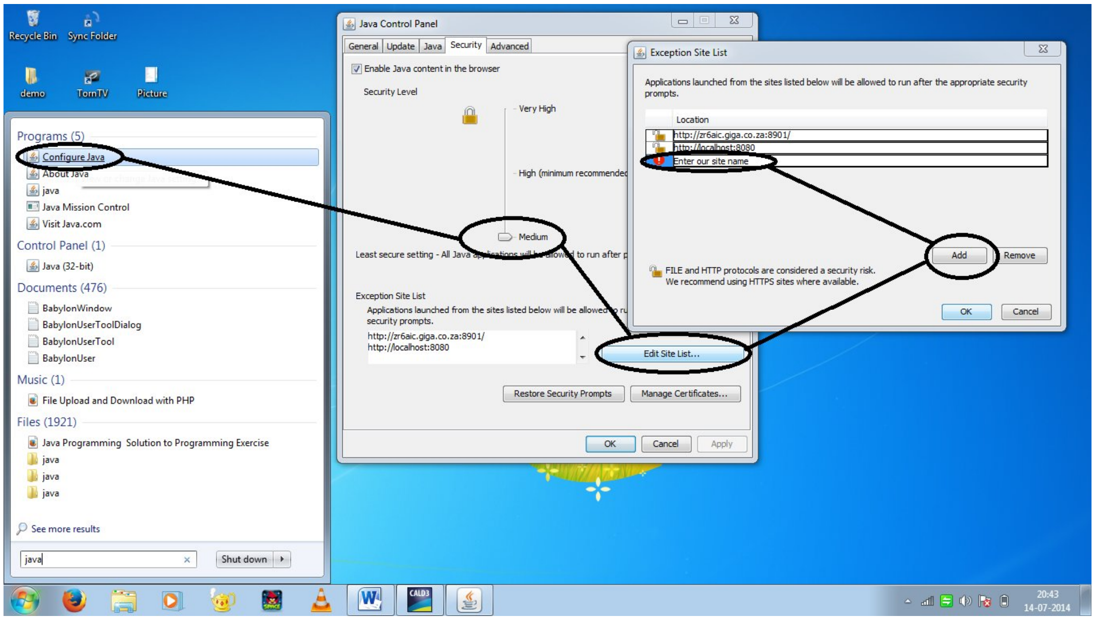


```
Listening on port 12468
vikky
test
Connections - current: 2  peak: 2  total: 2
Server activity log:
Reading message file
Waiting for connections
New user vikky logging on at Jul 11, 2014 10:55 AM from
127.0.0.1
There are 1 users connected
New user test logging on at Jul 11, 2014 10:56 AM from 127.0.0.1
There are 2 users connected
```

Figure7.3 Server manager

This is the starting phase of our project implementation. While running the apache tomcat server a java program will run automatically it generates a pop-up shown above, which is for connecting different clients with sockets for the purpose of white board technology using canvas.

7.3 Enable java in Browser



☑ Enable Java content in the browser

Security Level

Least secure setting - All Java applications will be allowed to run after p

Exception Site List

Applications launched from the sites listed below will be allowed to ru security prompts.

http://zr6aic.giga.co.za:8901/
http://localhost:8080

Applications launched from the sites listed below will be allowed to run after the appropriate security prompts.

Location
http://zr6aic.giga.co.za:8901/
http://localhost:8080
Enter our site name

FILE and HTTP protocols are considered a security risk.
We recommend using HTTPS sites where available.

Figure7.4: Enable java in Browser

To enable java in web browser, go to configure java option and select security option in that go to edit site list button and add site name to the list. Everything clearly shown in the Figure 7.4.

7.4 Login page

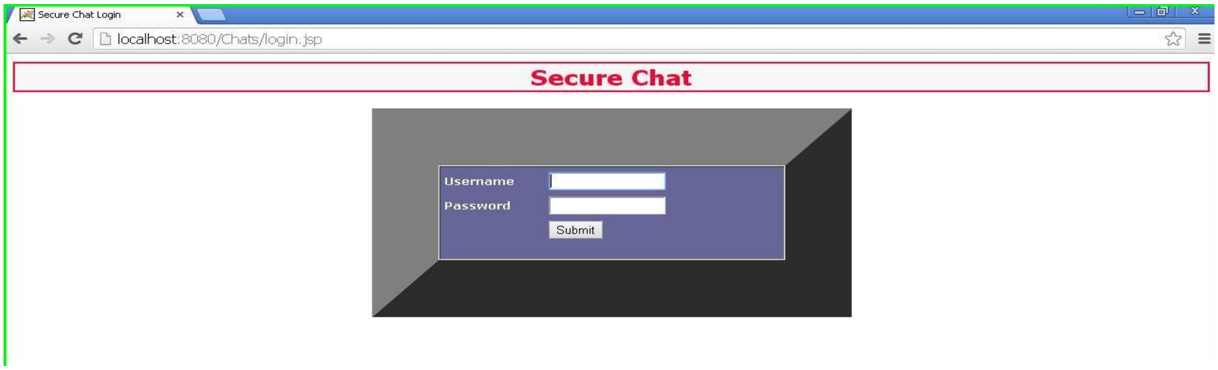


Figure7.5 Login Page

When the client access the website a login page will be displayed. The client should provide Username and Password with which client registered. If the user is not existing then a registration link will be displayed.

7.5 Registration Form

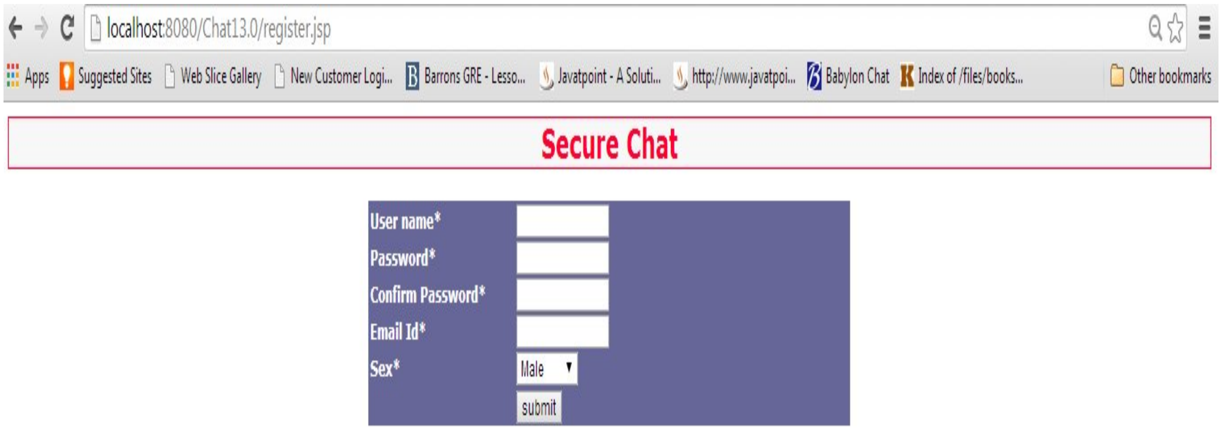
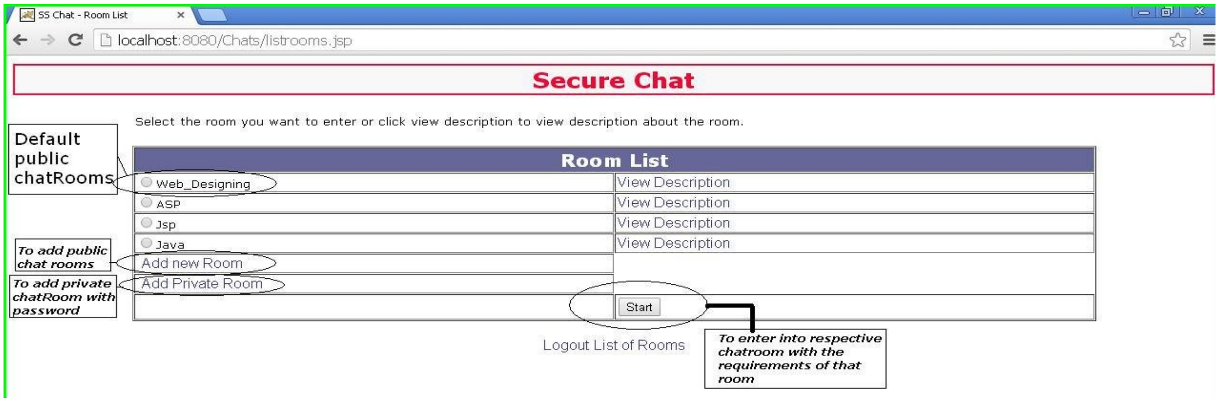


Figure 7.6: Registration Form

If the user entered wrong username a link for signup given. The new user can register using the form shown in the Figure 7.4.

7.6 List Rooms



SS Chat - Room List

localhost:8080/Chats/listrooms.jsp

Secure Chat

Select the room you want to enter or click view description to view description about the room.

Room List	
○ Web_Designing	View Description
○ ASP	View Description
○ Jsp	View Description
○ Java	View Description
Add new Room	
Add Private Room	
	Start

Logout List of Rooms

Default public chatRooms

To add public chat rooms

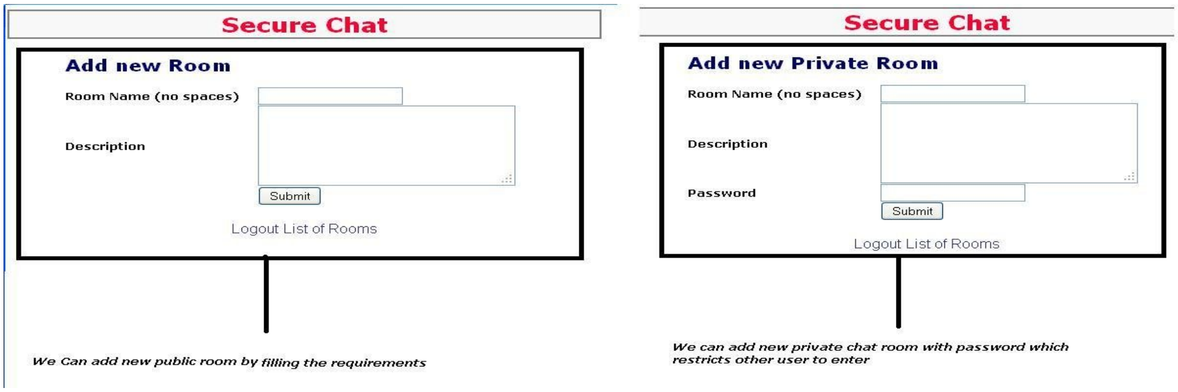
To add private chatRoom with password

To enter into respective chatroom with the requirements of that room

Figure 7.7: List Rooms

After logging in to the website, list of chat rooms will be displayed to the clients. There will be some set of pre-defined rooms and options for adding public and private rooms. In the picture every option clearly described.

7.7 Adding Public and Private Rooms



Secure Chat

Add new Room

Room Name (no spaces)

Description

Submit

Logout List of Rooms

We Can add new public room by filling the requirements

Secure Chat

Add new Private Room

Room Name (no spaces)

Description

Password

Submit

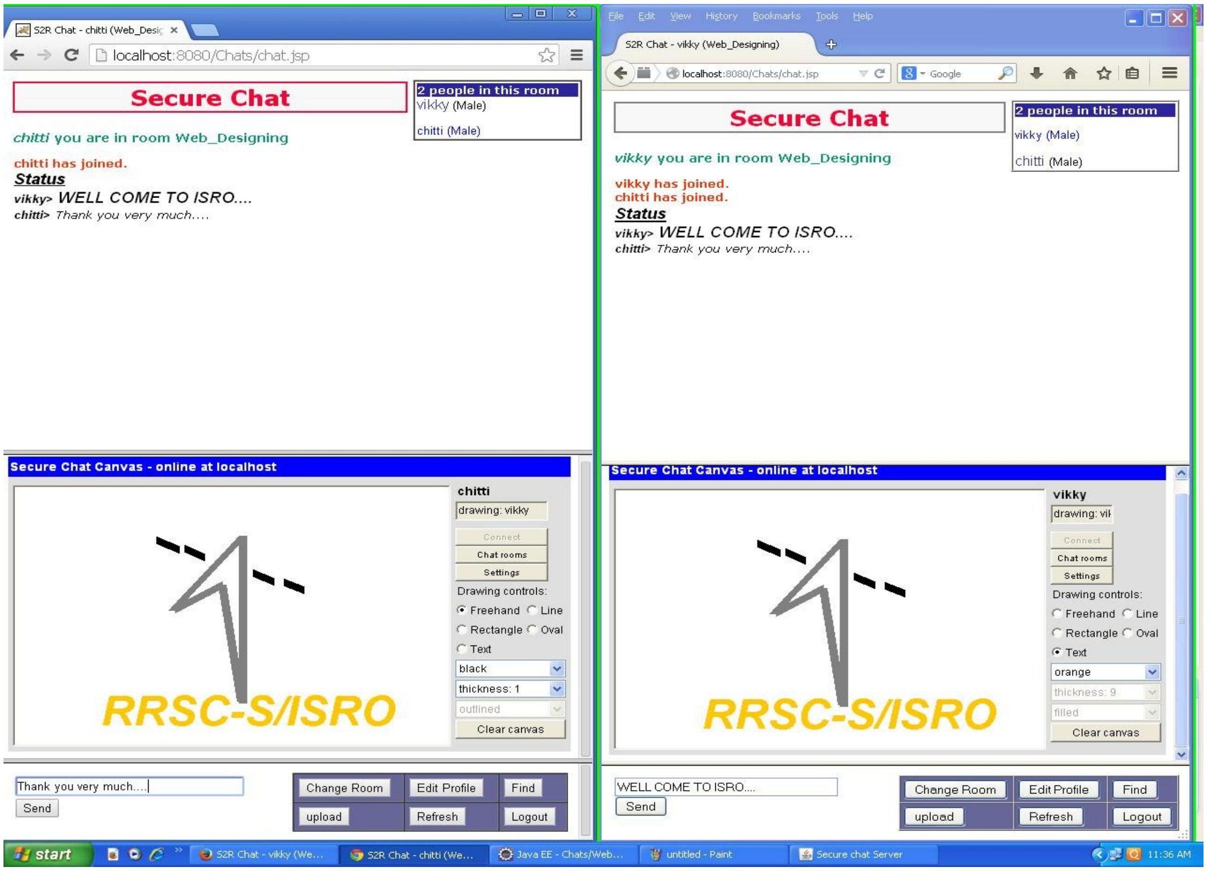
Logout List of Rooms

We can add new private chat room with password which restricts other user to enter

Figure 7.8: Add Rooms

When the client selects the option to add Public or Private Rooms the webpage will be displayed as shown in the above Figure 7.3. The client needs to enter Name and Description. In private rooms we can give the password.

7.8 Live Blogging with Canvas


Secure Chat

2 people in this room
vikky (Male)
chitti (Male)

chitti you are in room Web_Designing

chitti has joined.

Status

vikky> WELL COME TO ISRO....
chitti> Thank you very much....

Secure Chat Canvas - online at localhost

chitti
drawing: vikky

Drawing controls:
● Freehand ○ Line
○ Rectangle ○ Oval
○ Text
black
thickness: 1
outlined

Thank you very much....

Secure Chat

2 people in this room
vikky (Male)
chitti (Male)

vikky you are in room Web_Designing

vikky has joined.
chitti has joined.

Status

vikky> WELL COME TO ISRO....
chitti> Thank you very much....

Secure Chat Canvas - online at localhost

vikky
drawing: vik

Drawing controls:
○ Freehand ○ Line
○ Rectangle ○ Oval
● Text
orange
thickness: 9
filled

WELL COME TO ISRO....

Figure 7.9: Live Blogging with Canvas

In above Figure 7.5, the status will be updated to other clients as the client type a single character in the text field, when he click the send button the whole text will be added to the chat room messages. If we click on the Names of the users we will get the details of the user.We are providing different buttons named like Change Room, Edit Profile, Find, Upload, Refresh and Logout for doing the respective operations. By clicking on the change room button we will redirect you to page shown in Figure 7.2.Find button will provide an opportunity to client to search for other user’s details. Logout will close the current session of the user.

Canvas Board provides services like drawing models like Free hand drawing , Rectangle, line, oval and Clear Canvas and pasting the text on canvas with all variable properties, filling the models with colors with different marker sizes. It sends the drawings to other allowed chat rooms while texting in same chat room.

Chapter 8

CONCLUSION AND FUTURE ENHANCEMENT

8.1 Conclusion

To reduce the signature verification overheads in the secure multimedia Mapblogging, block based authentication schemes have been proposed. Unfortunately, most previous schemes have many problems such as vulnerability to packet loss and lack of resilience to denial of service (DoS) attack. To overcome these problems, we develop a novel authentication scheme MAPBLOGS .We have demonstrated that MAPBLOGS is perfectly resilient to packet loss sue to the elimination of the correlation among packets and can effectively deal with DoS attack. Moreover, we also show that the use of batch signature can achieve the efficiency less than or comparable with the conventional schemes. Finally, we further develop two new batch signature schemes based on Boneh–Lynn–Shacham (BLS) and DSA, which are more efficient than the batch RSA signature scheme.

This application provides

1. This system was developed so that clients can exchange information securely as well as converse with each other in real time.
2. Through this system client can access blogging rooms globally.
3. The system is interactive and user friendly.
4. Entire system is fully automatic to the clients and satisfies the client’s requests.
5. Especially the system is more useful to the technical peoples when there is a need of sending files securely.
6. This system also provides key feature of live drawing using “**WHITE BOARD UTILITY OF CANVAS”,** so that users can send drawings while conversation with specific group.
7. It satisfies user privacy conditions by providing private rooms, which gains the user confidentiality.

8.2 Future Enhancement

This paper describes new methods in pairing-based signature schemes for identifying the invalid digital signatures in a batch, after batch verification has failed. These methods efficiently identify non-trivial numbers of invalid signatures in batches of (potentially large) numbers of signatures. Our methods use “divide-and-conquer” search to identify the invalid signatures with in a batch but prune the search tree to substantially reduce the number of pairing computations required. The methods presented in this paper require computing on average O(w) products of pairings to identify w invalid signatures within a batch of size N compared with the $O(w(\log_2(N/w)+1))$[for $w<N/2$] that traditional divide-and-conquer methods require. Our methods avoid the problem of exponential growth in expected computational cost that affect earlier proposals which, on average, require computing O(w) products of pairings.

We compare the expected performance of our batch verification methods with previously published divide-and-conquer and exponential cost methods for Cha-Cheon identity-based signatures. However, our methods also apply to a number of short signature schemes and as well as to other identity based signature schemes.

This project can be enhanced by implementing different protocols and can be made more useful for varied clients according to the requirements of the client, it can also possible in future that each client in this globe has his own customized “Blogging”.

1. It can be enhanced in the field of live voice chatting. Using VoIP protocol.
2. It can be enhanced in the field of Video Conferencing.
3. It can be used for monitoring the stock market.
4. It can be used for machine or architectural design.

Chapter 9

Making of Three Dimensional Models of Historical Buildings Present in Mysore City Using SketchUp for Bhuvan

9.1 Introduction

Bhuvan gives you an easy way to experience, explore and visualize IRS images over Indian region. ISRO is well known amongst space faring nations for its world-leading reputation in developing new, indigenous and innovative service oriented applications using remote sensing technology. Over the past 2 decades, ISRO has mastered the art of developing these unique applications using various spectral, spatial and temporal resolutions offered by the versatile IRS satellites and these have been successfully institutionalized in many important areas of policy making, natural resources management, disaster support, and enhancing the quality of life across all sections of the society. Now ISRO is adding famous historical buildings present in India in to Bhuvan. So, in this project 3d modeling of famous historical buildings present in mysore city has been carried out using SketchUp.

9.2 Objective

- ✓ To capture the photographs of Historical buildings present in Mysore city.
- ✓ To make 3D models of Historical buildings present in Mysore city Using SketchUp.
- ✓ To import SketchUp model in to ArcScene.

9.3 Study Area

Mysore is located at a north latitude of 12^{o} 17' 45" N and east longitude of 76^{o} 38' 22" E of Karnataka in India.

9.4 Software Used

- ➢ Google Sketchup 8
- ➢ Adobe Photoshop CS3
- ➢ ArcScene

9.5 Methodology

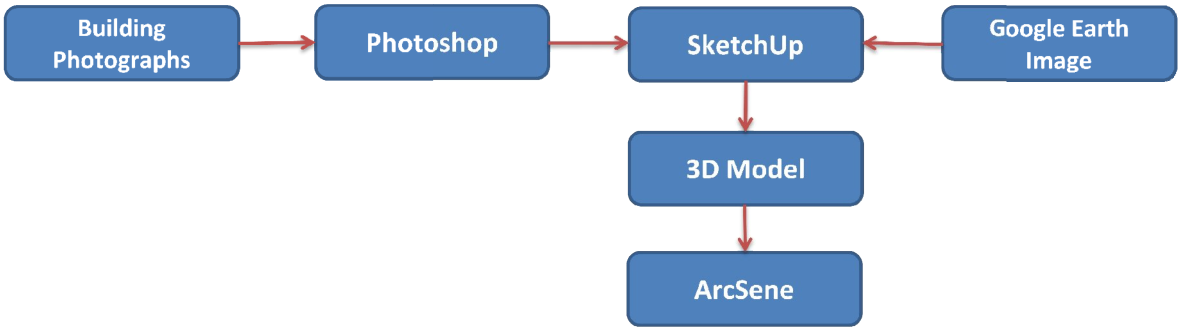
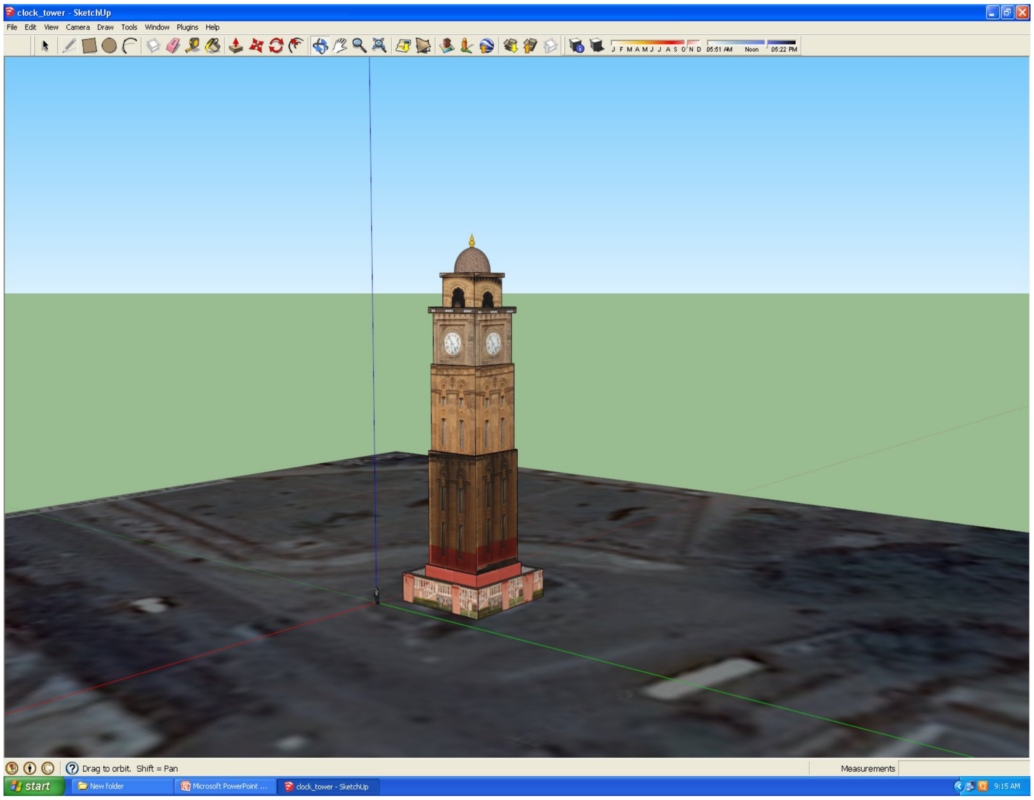


Figure 9.1 3D Model Design Methodology

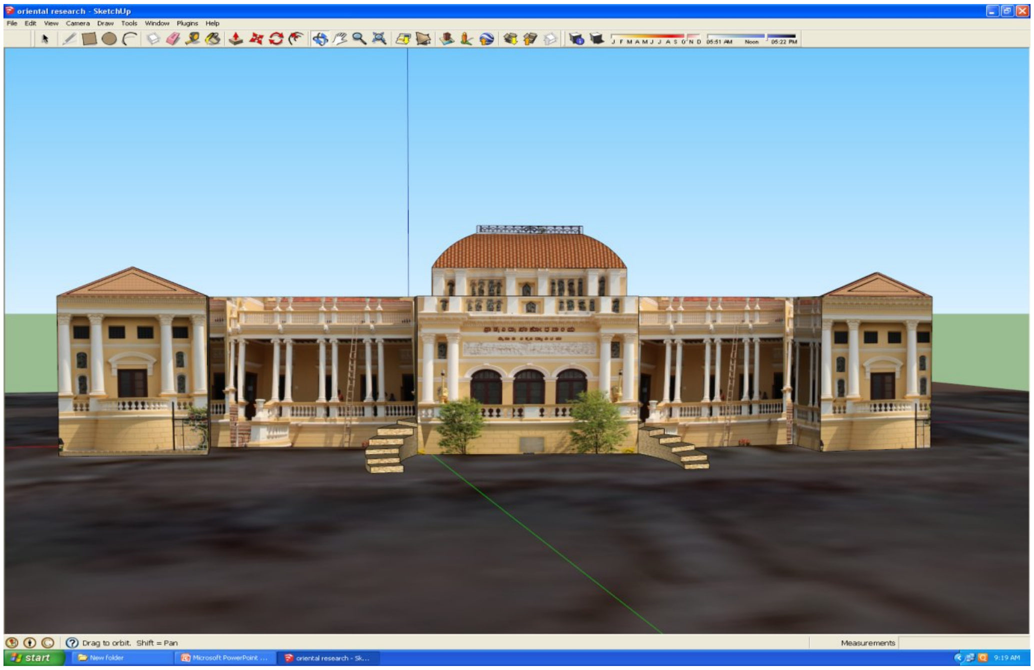
Photographs of all historical buildings present in Mysore have been captured using good quality DSLR camera. Google maps of respective buildings have been imported in to SketchUp to make it as a reference for its exact geographical location and extraction of approximate building boundary. Line has been drawn along the boundary of the building to create single plane surface (Building layout) by using line tool. Push/Pull tool has been used to convert single plane surface in to three dimensional building by specifying approximate building height. Some architectural shapes have been added to building to look like original building. A captured photograph has been imported in to Photoshop software to crop them in to required size and also their brightness has been adjusted according to the requirement. Modified images have been imported as texture in to sketch up and they have been pasted on the surface of the building. Some images have became skewed due to the change in the direction of angle of capture so texture pins have been adjusted to make these images in to perfect plane. later texture has been made as a unique texture for future use. Finally completed 3D buildings have been exported to collada(.dae) file extension. Later 3D buildings have been imported in to Arc Scene by converting collada(.dae) to multipatch(.shp) format.

9.6 Results

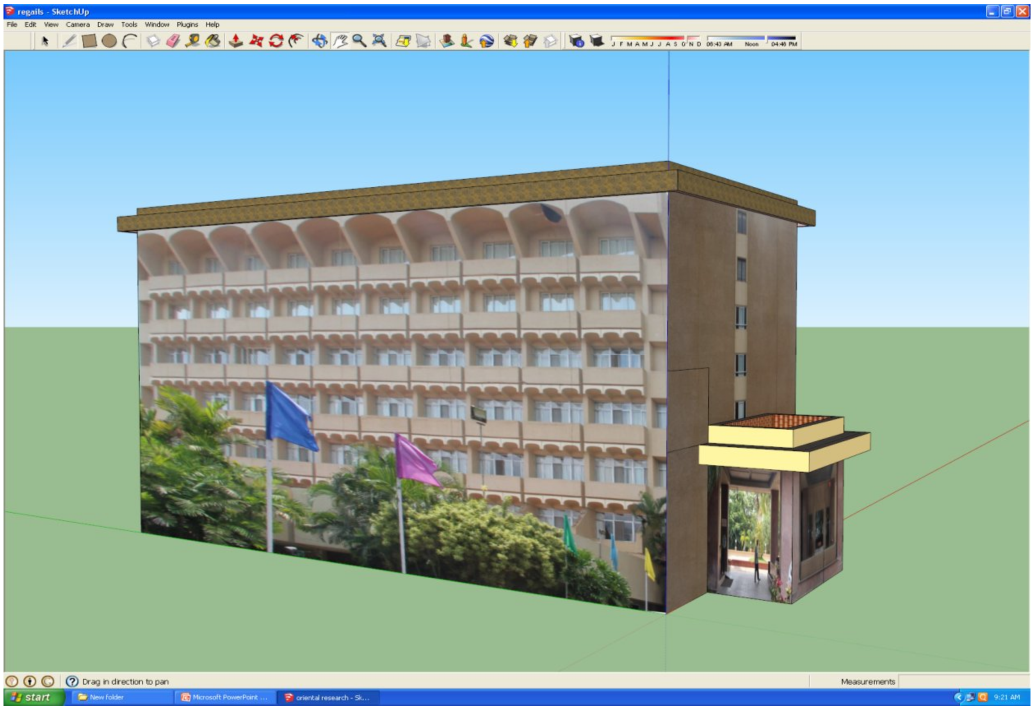
Clock Tower


clock_tower - SketchUp
File Edit View Camera Draw Tools Window Plugins Help
J F M A M J J A S O N D 05:51 AM Noon 05:22 PM
Drag to orbit. Shift = Pan
Measurements
start
New folder
Microsoft PowerPoint ...
clock_tower - SketchUp
9:15 AM

Oriental Research Building


oriental research - SketchUp
File Edit View Camera Draw Tools Window Plugins Help
J F M A M J J A S O N D 05:51 AM Noon 05:22 PM
Drag to orbit. Shift = Pan
Measurements
start
New folder
Microsoft PowerPoint ...
oriental research - Sk...
9:19 AM

Regalis


regails - SketchUp
File Edit View Camera Draw Tools Window Plugins Help
J F M A M J J A S O N D 06:43 AM Noon 04:46 PM
Drag in direction to pan
Measurements
start
New folder
Microsoft PowerPoint ...
oriental research - Sk...
9:21 AM

REFERENCES

[1]William Stallings," Cryptography and Network Security: Principles and Practice 5th Edition "

[2] S.E Deering, "Mapblogs Routing in Internetworks and Extended LANs," Proc .ACM SIGCOMM Symp. Comm. Architectures and Protocols,pp. 55-64, Aug. 1988.

[3]T.Ballardieand J.Crowcroft,"Mapblogs-Specific Security Threats and Counter-Measures," Proc. Second Ann. Network and Distributed System Security Symp.(NDSS'95), pp. 2-16,Feb. 1995 .

[4] P.Judge and M.Amar, "Security Issues and Solutions in Multicast Content Distribution

Distribution: A Survey," IEEE Network Magazine, vol. 17, no. 1,pp. 30-36, Jan./Feb. 2003.

[5]Y.Challal, H.Bettahar, and A.Bouabdallah, "A Taxonomy of Mapblogs Data Origin Authentication: Issues and Solutions," IEEE Comm. Surveys & Tutorials, vol. 6, no. 3,pp. 34-57,Oct. 2004

[6]Y.Zhou and Y.Fang, "BABRA: Batch-Based Broadcast Authentication in Wireless Sensor Networks," Proc. IEEE GLOBECOM, Nov. 2006.

[7]Y.Zhou and Y.Fang, "Multimedia Broadcast Authentication Based on Batch Signature," IEEE Comm. Magazine, vol. 45, no. 8, pp. 72-77,Aug. 2007.

[8]K.Ren,K.Zeng,W.Lou, and P.J.Moran, "On Broadcast Authentication in Wireless Sensor Networks, " Proc. First Ann. Int'l Conf. Wireless Algorithms, Systems, and Applications (WASA'06), Aug. 2006.

[9]S.Even, O.Goldreich and S.Micali, "On-Line/Offline Digital Signatures," J.Cryptology, vol. 9,pp. 35-67, 1996.

[10]P.Rohatgi, "A Compact and Fast Hybrid Signature Scheme ForMapblogs Packet," Proc Sixth ACM Conf. Computer and Communication.Security (CCS'99), Nov. 1999.

[11]C.K. Wong and S.S. Lam, "Digital Signatures for Flows and Mapblogs," Proc. Sixth Int'l Conf. Network Protocols (ICNP'98),pp. 198-209,Oct. 1998.

Websites Referred

http:1//java.sun.com

http://javatpoint.com

http://www.networkcomputing.com/

http://www.tutorialspoint.com

http://www.stackoverflow.com

Contact details:

Vikramkumar allakonda : vikramkumariiit@gmail.com

Chittibabu Tirupathi : chittiplt.rgukt@gmail.com

Sravani Murakonda : murakondasravani64@gmail.com