MAPBLOGS - Implementation Of Secure Multimedia With Client-Server Architecture Using White Board as Canvas In Network Security

[1]Tanveer Ahmed, [2]Gunti Spandan, [3]Abdul Saleem Javeed, [4]Yathish D.P
[1]Asst. Professor, [2]Asst. Professor, [3]Asst. Professor, [4]Asst. Professor
[1]Dept. Of CSE, [2]Dept. Of CSE, [3]Dept. Of CSE, [4]Dept. Of CSE
[1]GITAM School of Technology, Bengaluru, India
[2]GITAM School of Technology, Bengaluru, India
[3]KNS Institute of Technology, Bengaluru, India
[4]GITAM School of Technology, Bengaluru, India

Abstract: 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 Mapblogs in an environment attractive to malicious attacks. Basically, Map blogs authentication may provide the following security services: Data integrity: Each receiver should be able to assure that received packets have not been modified during transmissions. Data origin authentication: Each receiver should be able to assure that each received packet comes from the real sender as it claims. Non-repudiation: The sender of a packet should not be able to deny sending the packet to receivers in case there is a dispute between the sender and receivers. All the three services can be supported by an asymmetric key technique called 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: 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 clients within the network.

IndexTerms **- Mapblogs, Multimedia, Broadcast.**

I. INTRODUCTION

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 bogs in an environment attractive to malicious attacks. Map bogs authentication may provide three security services such as data integrity, data origin authentication, 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 the sender's public key, which is called verifying. If the verification succeeds, the receiver knows the packet is authentication .There are following issues in real world challenging the design. . First, efficiency needs to be considered, especially for receivers. Compared with the Map bogs 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 losses 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 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 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; 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. Efficiency and packet loss resilience can hardly be supported simultaneously by conventional Map bogs schemes.

1.1 Advantages and Limitations

1.1.1 Advantages

The advantages of using digital signatures include:

1.1.1.1 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 signature serves the purpose of authenticity in the communication network. Using digital signature frauds can be prevented and security issues can be resolved.

1.1.1.2 Message integrity

By having a digital signature you are in fact proving the document to be valid. You are assuring the recipient that the document is free from Forgery or false information.

1.1.1.3 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 text, pictures, video and audio.

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 Inline images, fonts & document layouts. When 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 or multimedia and provided by servers located around the world. The usability of the Web depends largely on the performance of these servers.

This application is a 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 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 images.
- At any given point of time, up-to-date information is provided.

1.1.2 Limitations

1.1.2.1 Cost

Digital signatures, even some of the simpler ones, come at a cost. You must have the necessary software to encode the signatures, and if you're 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.

1.1.2.2 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.

1.2 Application Areas

1.2.1 Multimedia

It comes in many different formats. It can be almost anything you can hear or see like text, pictures, music, sound, videos, records, films, animations, and more. Multimedia elements also have their own file formats with different extensions like

mp3, and mp4. Multimedia is usually recorded and played, displayed or accessed by information content processing devices. Multimedia authentication deals with confirming the genuineness or 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 watermarking to provide more desirable authentication. It is worth mentioning that multimedia authentication is different from user authentication.

1.2.2 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 a 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 TANDBERG's firewall traversal solution are making it
possible to communicate across boundaries.

But, with open communication comes risk. Network administrators cite 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 in developing solutions to resolve security concerns. By addressing the issue of security at three levels authentication, policy and encryption.

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 transmits 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.

1.2.3 Enhanced Scheme

An enhanced scheme called MAPBLOGS-E combines the basic scheme MAPBLOGS-B and a packet filtering mechanism to tolerate packet injection. In particular, 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 of packets is from the attacker, and the receiver simply drops them and does not need to divide the set into smaller subsets for further batch verification. Therefore, a strong resilience to DoS due to injected packets can be provided.

1.3 Existing System

Efficiency and packet loss resilience can hardly be supported simultaneously by conventional 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 more 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-

 To choose the block size.
 To 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 resource-constrained devices. Compared with the efficiency requirement and packet loss problems, the DoS attack is not common, but it is still important in hostile environments.

1.4 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 a 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.

II. RELATED WORK

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 n company strength. Once these things r satisfied, ten 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 r taken into account for developing the proposed system.

2.1 Mapblogs Routing in Internetworks and Extended LANs

Mapblogs Routing, propose an efficient mechanism of sender access control for bi-directional 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 bidirectional tree.

2.2 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 to provide solutions. Security in Mapblogs content distribution has matured over the years, but there remain open problems in the area that must be resolved to help Mapblogs enable more applications.

2.3 Batch Based Broadcast Authentication

Broadcast authentication is a critical security service 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 attack 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 muTESLA-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.

2.4 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 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 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 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.

2.5 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, Security 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.

III. 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 requirements 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 to a level of detail sufficient to enable designers to design a system to satisfy those 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 behavior of the system and its operational constraints.

- • Operating system : - Windows XP Professional.
- • Coding Language : - Java.
- • Tool Used : - NetBeans IDE.

IV. PROPOSED SYSTEM:-

4.1 Architecture of the proposed system

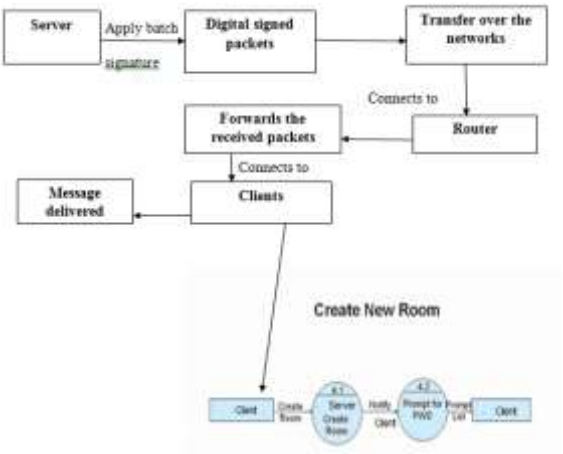


Fig 1:- Block Diagram of the Proposed System

We planned a unique Mapblogs verification convention, specifically MAPBOGS, including two plans.

- The essential plan disposes of the connection among parcels and along these lines gives the ideal versatility to bundle misfortune, and it is additionally proficient as far as dormancy, calculation, and correspondence overhead because of an effective cryptographic indigence called cluster mark, and bolsters verifying many bundles, at same time.
- The proposed framework's chief element is its whiteboard sketch use. We can draw freehand, do circles, squares, lines, content, glue picture records to canvas. Its perfect when clients need "portray" ideas to each other. The component of "BLOGGING" can shelter to specialized individuals need help their thoughts ideas in sketch structure. This framework incorporates the offices of customary visit slave and customers like giving to each client, talk, and numerous visit rooms and so on. With assistance of 'WHITE BOARD' sketch use now specialized individuals do errands effortlessly and help their enormous image arranges in regards to their business to the customers, trade thoughts and ideas and numerous more things, fundamentally trade and in addition impart the data along to the utilizing the sketch discussions between two clients might essential conferences.

4.2 Components Required:

4.2.1 Software Requirements

- Operating System:- Windows XP Professional
- Coding language:- Java
- Tool Used:- Net Beans IDE 7.3.1
- Server:- Apache Tomcat 8.0

4.2.2 Hardware Requirements

- Processor:- Pentium IV 2.4 GHz / Above
- Hard disk:- 40 GB
- RAM:- 256 Mb
- Monitor:- 15 VGA Color

V. 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 and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

5.1 Modules

- Network model.
- DSA key generation.
- Digital Signature (sending packets)
- Signature Verification (receiving packets).
- LIVE Blogging System
- CANVAS BOARD

5.1.1 Network Model

Customer server registering or systems administration is a conveyed application design that parcels undertakings or workloads between administration suppliers and administration requesters, called customers. Regularly customers and servers work over a PC system on particular equipment. A server machine is a superior host that is running one or more server projects which impart its assets to customers. A customer likewise shares any of its assets; Customers subsequently start correspondence sessions with servers which anticipate approaching solicitations.

At the point when talking about systems, distinctive theoretical perspectives can be utilized. One perspective is the manner by which the PCs and systems are associated with each other and another perspective is a layered perspective of how the conventions work on top of each other. Each sub-model passage characterizes a model inside the system model, either by unequivocally portraying it, or by importing its depiction from a document. These models will be alluded to as sub-models in the continuation keeping in mind the end goal to recognize the system model itself and its fused parts. Also to the depiction of the sub-model, each Sub-model portrayal contains articulations about its info ports and in addition its yield ports. The sub-model made by the relating explanation is connected with a name got from name. This name is utilized when one sub-model alludes to yield ports of another. The system model offers highlights that keep even broad reenactment errands viable to a TCAD engineer. Because of its adaptable structure, it empowers an extensive variety of recreation applications, since it suggests basically no confinements to the clients inventiveness. The system model serves as a flawless premise for modern TCAD applications like advancement, alignment, or measurable investigation, since it empowers the definition of convoluted matters by method for models of different sorts.

5.1.2 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:

Choose an approved cryptographic hash function H. 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. Recommends lengths of 2048 or 3072 for keys with security lifetimes extending beyond 2010 or 2030, using correspondingly longer N specifies L and N length pairs of (1024,160), (2048,224), (2048,256), and (3072,256).

5.1.3 Digital Signature

Advanced marks utilize a kind of hilter kilter cryptography. For messages sent through an unreliable channel, an appropriately executed computerized signature gives the recipient motivation to trust the message was sent by the asserted sender. Advanced marks are comparable to conventional transcribed marks in numerous regards; appropriately executed computerized marks are more hard to fashion than the manually written sort. Computerized signature plans in the sense utilized here are cryptographically based, and should be executed appropriately to be viable. Computerized marks can likewise give non-renouncement, implying that the underwriter can't effectively assert they didn't sign a message, while additionally guaranteeing their private key stays mystery; further, some non-revocation plans offer a period stamp for the advanced mark, so that regardless of the fact that the private key is uncovered, the mark is v A computerized signature or advanced mark plan is a scientific plan for showing the genuineness of a computerized message or report. A substantial computerized signature gives a beneficiary motivation to trust that the message was made by a known sender, and that it was not changed in travel. Computerized marks are generally utilized for programming conveyance, money related exchanges, and in different situations where it is imperative to identify falsification or altering.

Computerized marks are frequently used to execute electronic marks, a more extensive term that alludes to any electronic information that conveys the purpose of a signature, however not every single electronic mark use advanced marks. In a few nations, including the Assembled States, India,[4] and individuals from the European Union, electronic marks have legitimate criticalness. Advanced marks utilize a kind of awry cryptography. For messages sent through a non-secure channel, an appropriately actualized computerized signature gives the recipient motivation to trust the message was sent by the asserted sender. Computerized marks are identical to conventional manually written marks in numerous regards; appropriately actualized advanced marks are more hard to fashion than the transcribed sort. Computerized signature plans in the sense utilized here are cryptographically based, and should be actualized appropriately to be compelling. Advanced marks can likewise give non-denial, implying that the underwriter can't effectively assert they didn't sign a message, while additionally guaranteeing their private key stays mystery; further, some non-renouncement plans offer a period stamp for the computerized signature, so that regardless of the fact that the private key is uncovered, the mark is legitimate in any case.

5.1.4 Signature Verification

Signature verification may be performed by any 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 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 signed by a trusted entity or in a face-to-face meeting with the public key owner. Ascertia'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. This simplifies business applications to focus on business-related functionality only, makes integration easier and improves security through centralized management, control and auditing features, not to mention much reduced costs as a result of this simplified architecture.

Ascertains ADSS Server is based on industry accepted protocols for communicating with an e-Trust server, including OASIS Digital Signature Specifications (DSS and DSS-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. Ascertains 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, see here for more details.

Before relying on digitally signed documents and transactions, it is essential for business applications to verify the trustworthiness of the e-signatures and validity of the signer's IDs. The application also need to determine if the certificate issuers can be trusted, what time the signature was created, whether the signer's certificate chain was valid at that time, if the signer was authorized to sign the data, and so on. End-users can verify signatures using local Trust Anchors managed by desktop applications or even better for those applications to request verification from central verification server and than just display the results. Server-side verification of any signature at some specified earlier date and time. The signature may be advanced long-term or even basic signatures can be verified historically using archived CRLs.

5.1.5 LIVE Blogging System:-

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 clients within the network

5.1.6 CANVAS BOARD

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 as well as share the information along with the using the 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 based web menu images can be transferred. And concepts and many more things, basically.

5.2 DSA Algorithm:-

5.2.1 Signing

Let H be the hashing function and m the message:

- Generate a random per-message value k where $0 < k < q$
- Calculate $r = (g^k \bmod p) \bmod q$
- In the unlikely case that $r = 0$, start again with a different random k
- Calculate $s = (k^{-1}(H(m) + x \cdot r)) \bmod q$
- In the unlikely case that $s = 0$, start again with a different random k
- The signature is (r, s)

The first two steps amount to creating a new per-user key. The modular exponentiation here is the most computationally expensive part of the signing operation, and it may be computed before the message hash is known. The modular inverse $k^{-1} \bmod q$ is the second most expensive part, and it may also be computed before the message hash is known. It may be computed using the extended Euclidean algorithm or using Fermat's little theorem as $k^{q-2} \bmod q$.

5.2.2 Verifying

- Reject the signature if $0 < r < q$ or $0 < s < q$ is not satisfied.
- Calculate $w = s^{-1} \bmod q$
- Calculate $u1 = H(m) \cdot w \bmod q$
- Calculate $u2 = r \cdot w \bmod q$
- Calculate $v = ((g^{u1} \cdot y^{u2}) \bmod p) \bmod q$
- The signature is valid if $v = r$

DSA is similar to the ElGamal signature scheme.

5.2.3 Correctness of the algorithm

The signature scheme is correct in the sense that the verifier will always accept genuine signatures. This can be shown as follows:

First, if $g = h^{(p-1)/q} \bmod p$ it follows that $g^q \equiv h^{p-1} \equiv 1 \pmod p$ by Fermat's little theorem. Since $g > 1$ and q is prime, g must have order q.

The signer computes

$s=k^{-1}(H(m)+xr) \bmod q$

$k= =H(m)s^{-1}+ xrs^{-1}$

$= =H(m)w + xrw \pmod q$

Since g has order q (mod p) we have

$g^k = = g^{H(m)w}\ g^{xrw}$

$= =g^{H(m)w}\ y^{rw}$

$= =g^{u1}y^{u2} \pmod p$

Finally, the correctness of DSA follows from

$r=(g^k \bmod p) \bmod q$

$=(g^{u1}y^{u2} \bmod p) \bmod q$

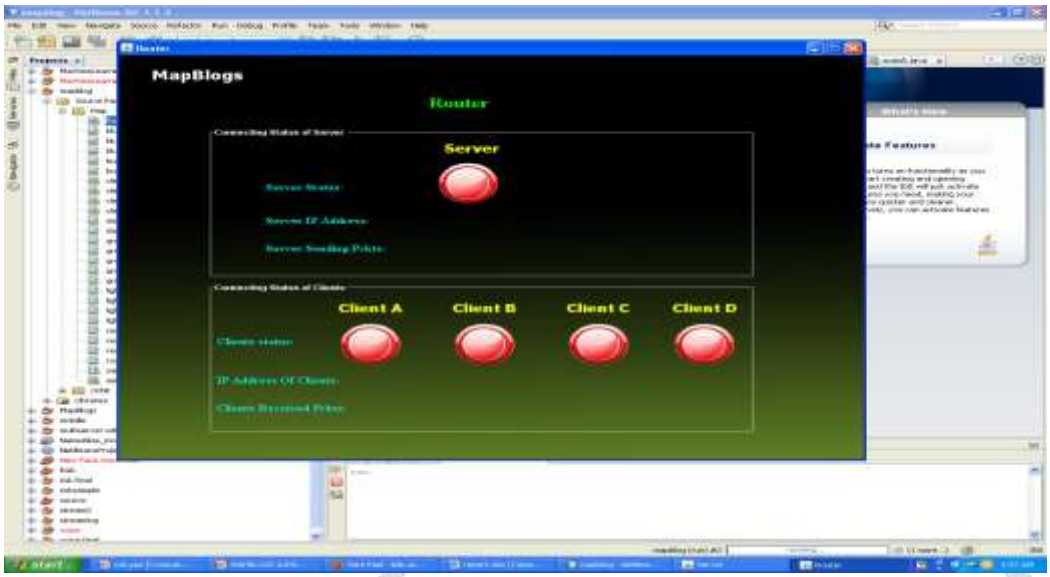
$=v$

VI. RESULTS

6.1 Server:-

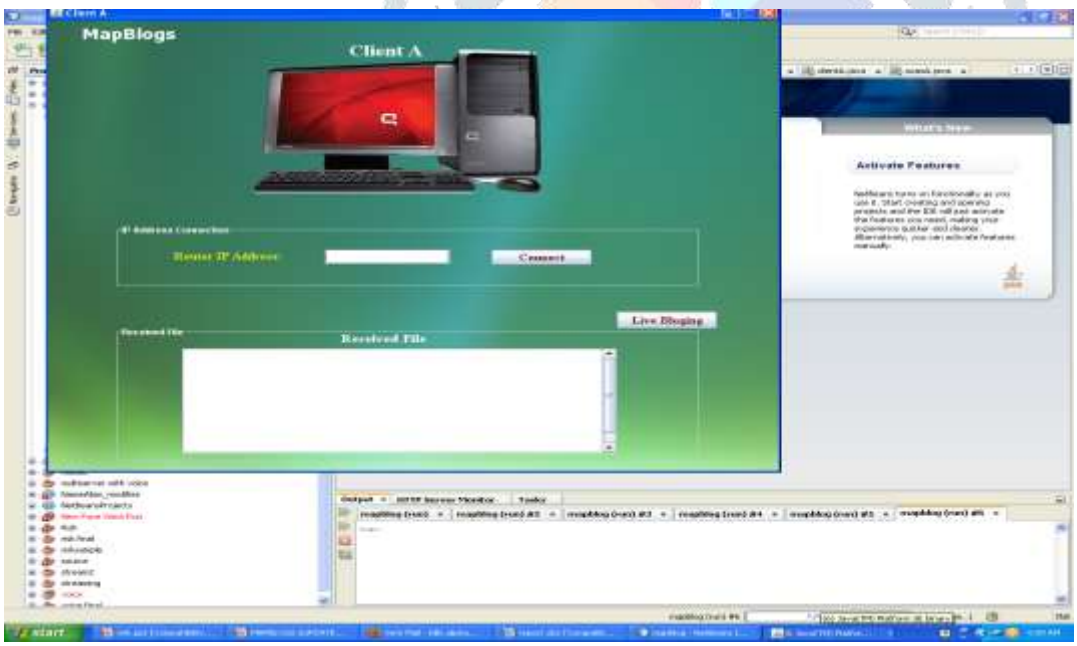
This is the starting phase of our project where we implement our conceptual and design view to our desired project. Here we used java functions to give a organized and structured view to propose a overall architecture of our project. We use the java frame which holds all the components together provided with individual properties assigned to each component the frame is divided into three levels including the file operation, key generate and file transfer acknowledgement. Key generate comprises of the key generate and sign on data button all the clients are hold by file transfer acknowledgement.

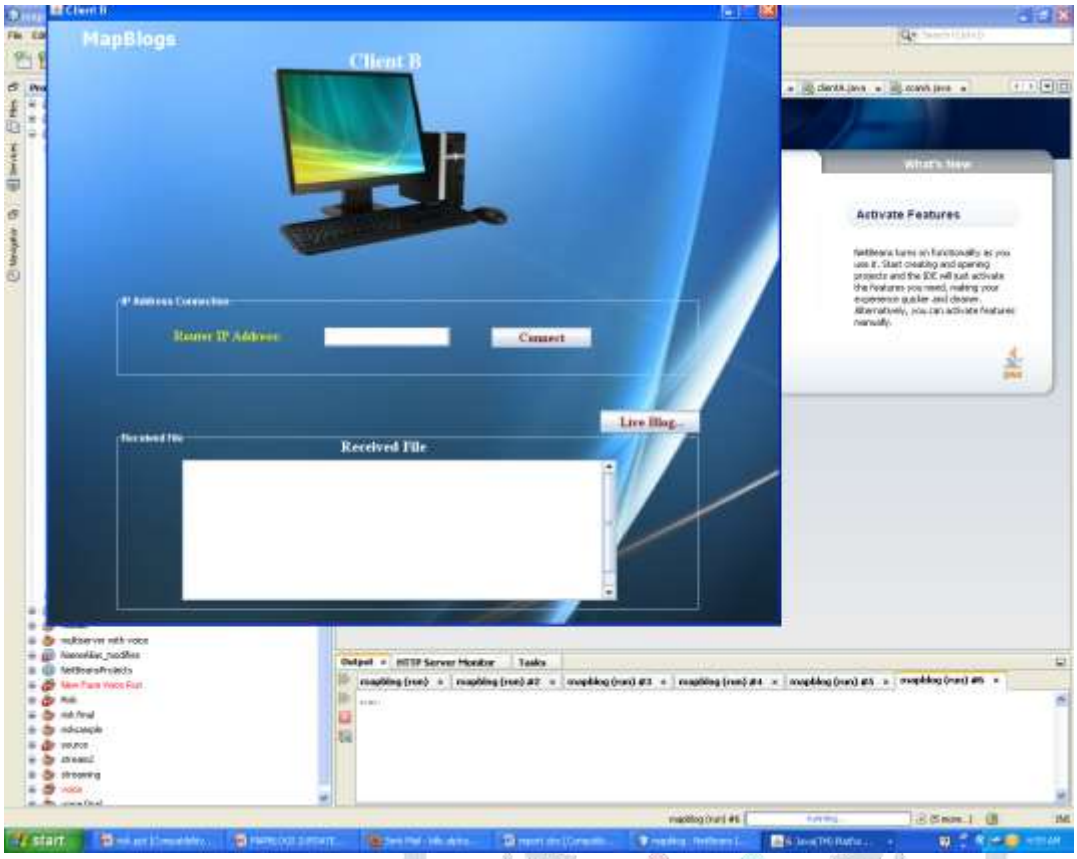
6.2 Router

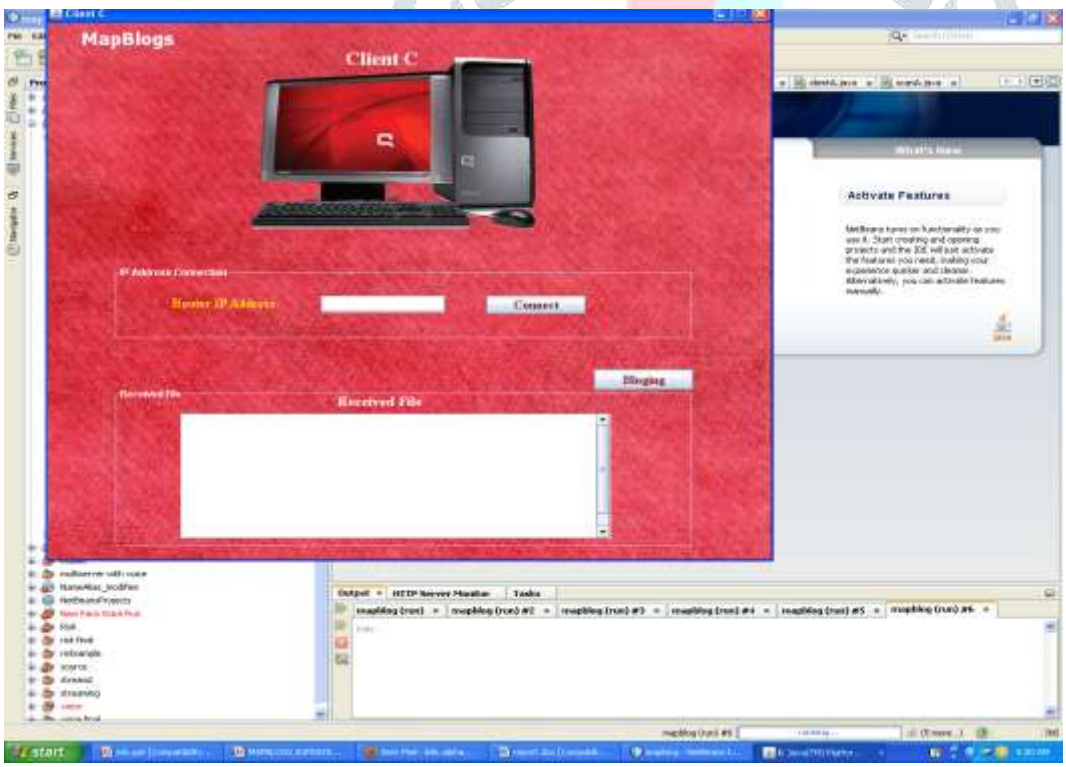


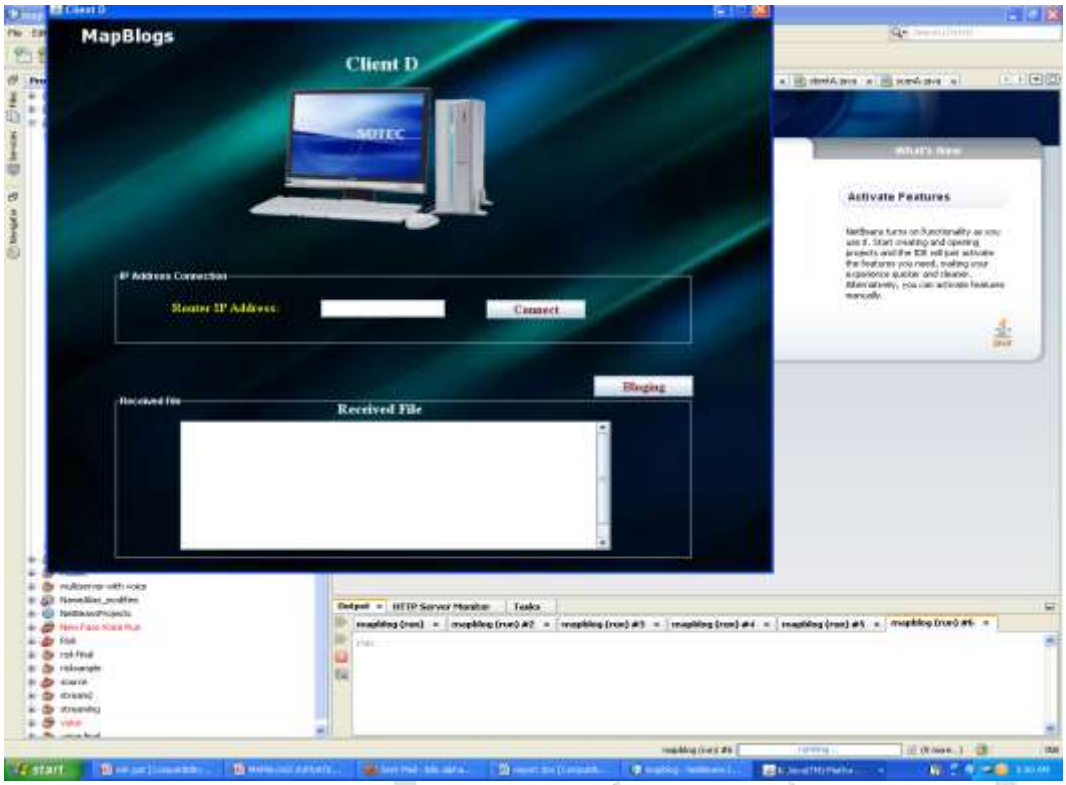
As mentioned previously all the components are arranged accordingly. The server initially is not found to be connected, as it symbolizes a red light. And the clients are also not connected, they symbolize a red light, demonstrating that clients and servers are disabled and are found to be enabled by providing their appropriate IP address. We build a design which includes four clients, one server and one router. Each clients are named as client A, client B, client C and client D . These clients are connected individually to the server via the router. After that we expect all the clients get enabled after giving the appropriate IP address along with the server and router.

6.3 Clients



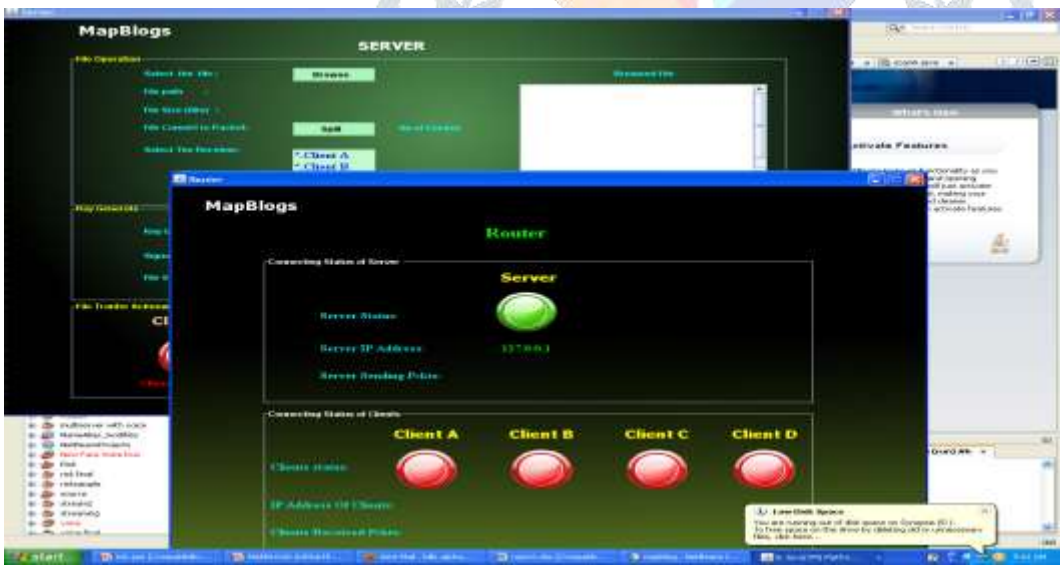

MapBlogs
Client B
Router IP Address:
Connect
Live Blog..
Received File
What's New
Activate Features


MapBlogs
Client C
Router IP Address:
Connect
Blogging
Received File
What's New
Activate Features



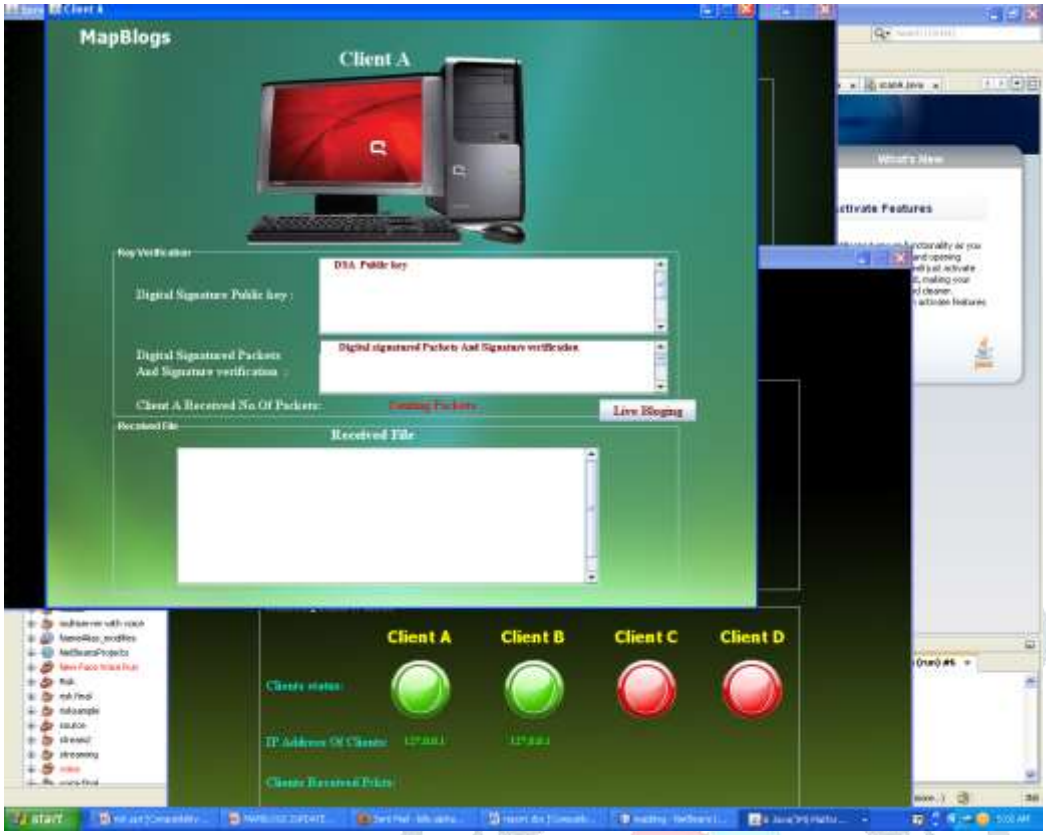
The above figure demonstrates that in IP address panel, we need to enter the valid router IP address and then connection is found to be made between the server and the clients. As soon as all the clients gets enabled the signatures assigned will be delivered to it and the messages is stored in a text form in the received files. The router then checks the authenticity for each client sequentially whether it matches the valid IP address, if yes connectivity is found to be enabled, otherwise the router will display a message as "please enter a valid IP address".

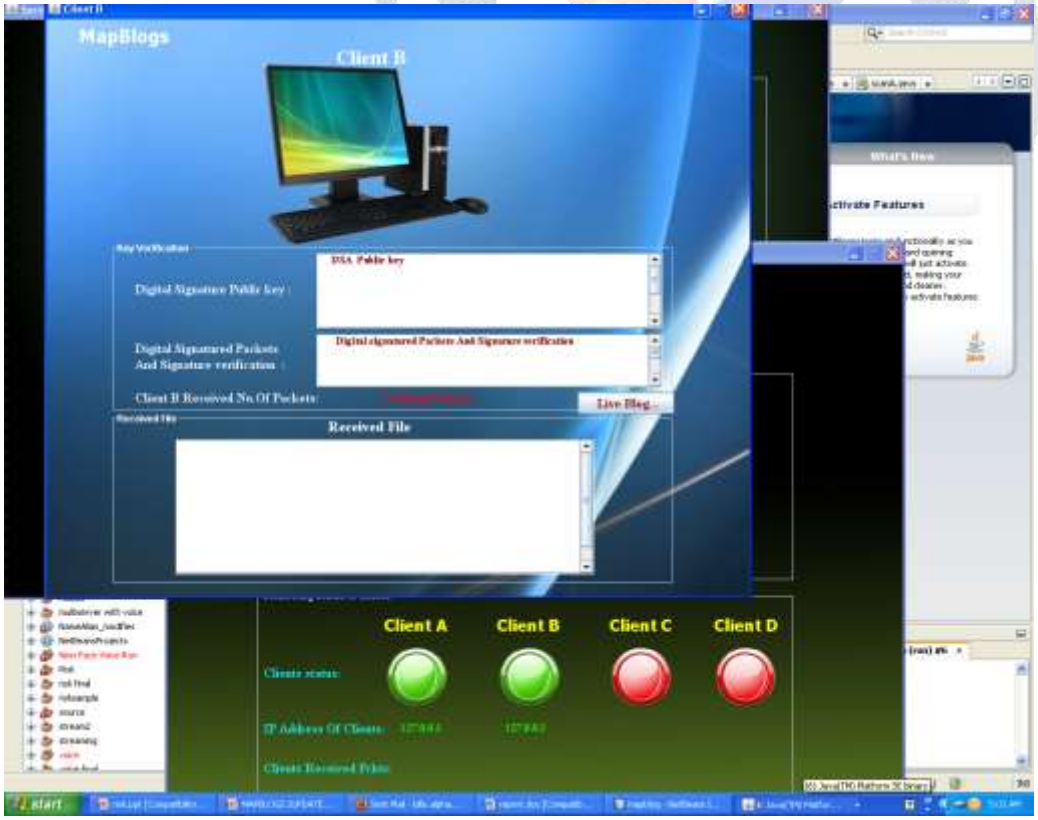
6.4 Server Connection

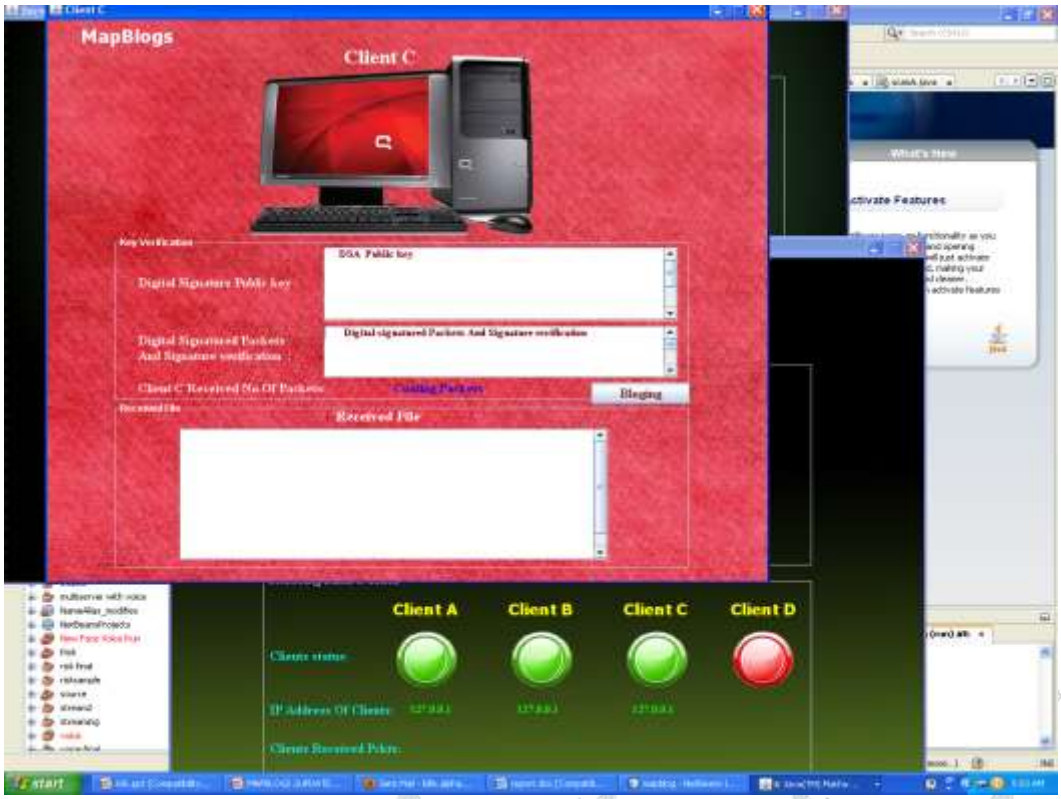


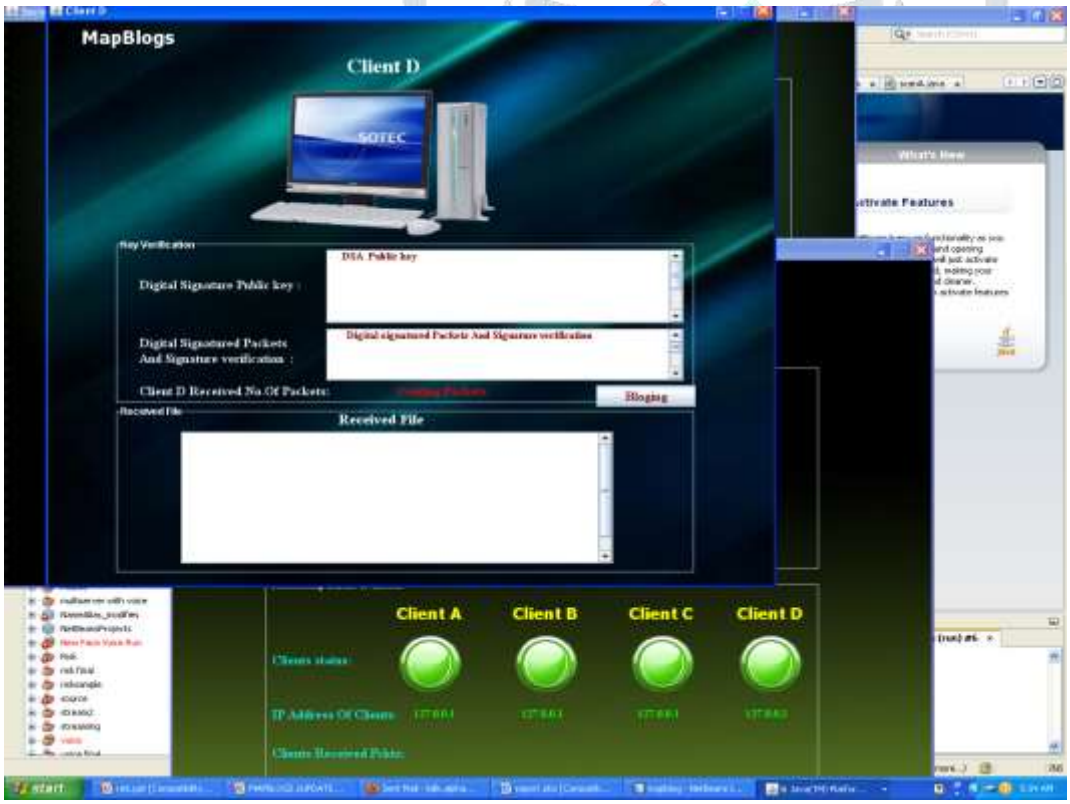
One can observe that the server has got enabled and it is displaying its IP address assigned through the router. All the clients are still awaiting and as soon as it gets enabled it will be ready to send its request to the server. In the router IP address connect panel, the IP address of the current client which is found to be connected with the server is connected via the router. The server is found to be enabled which can be seen in the router frame. As soon as the server is assigned with its authenticated IP address, the server will get activated transforming its red light to green, showing that the server is enabled.

6.4 Router connected to Server and Clients:-







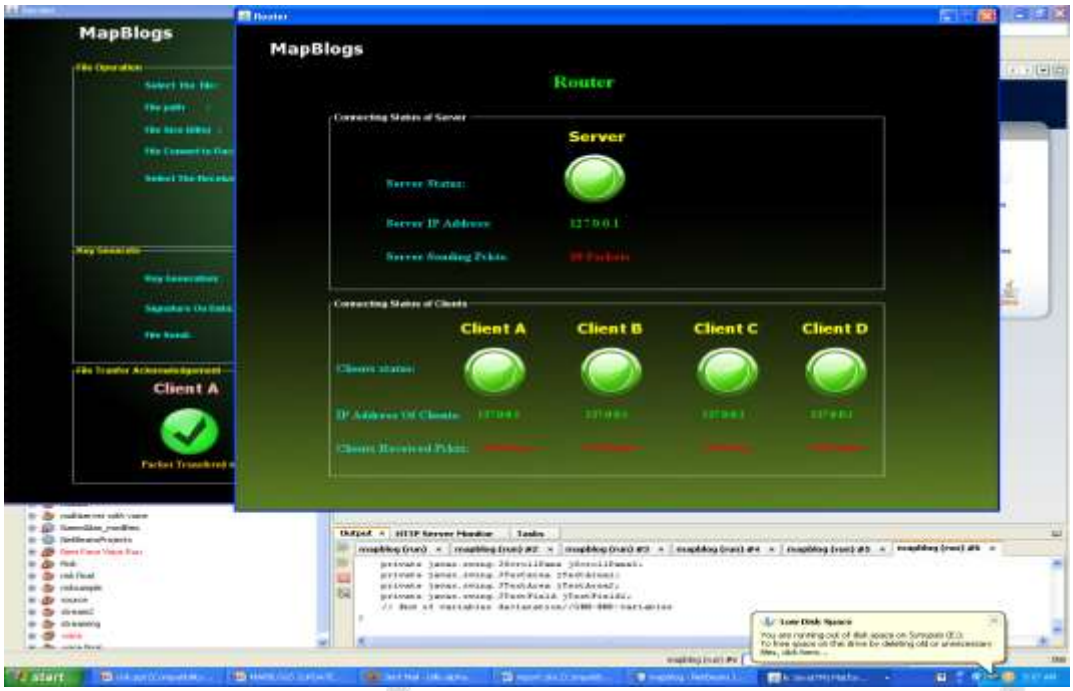


Through this snapshot, we can systematically come to know how the server is found to be connected to all the clients via the router with their IP addresses. We can see how before the IP address was connected all of them were in red color, once it was connected from server to clients it changed to green which symbolizes there exists a connectivity, so packets can be transferred from sender to receiver .The IP address of clients and server is found to be seen 127.0.0.1.

6.5 Files sent to server

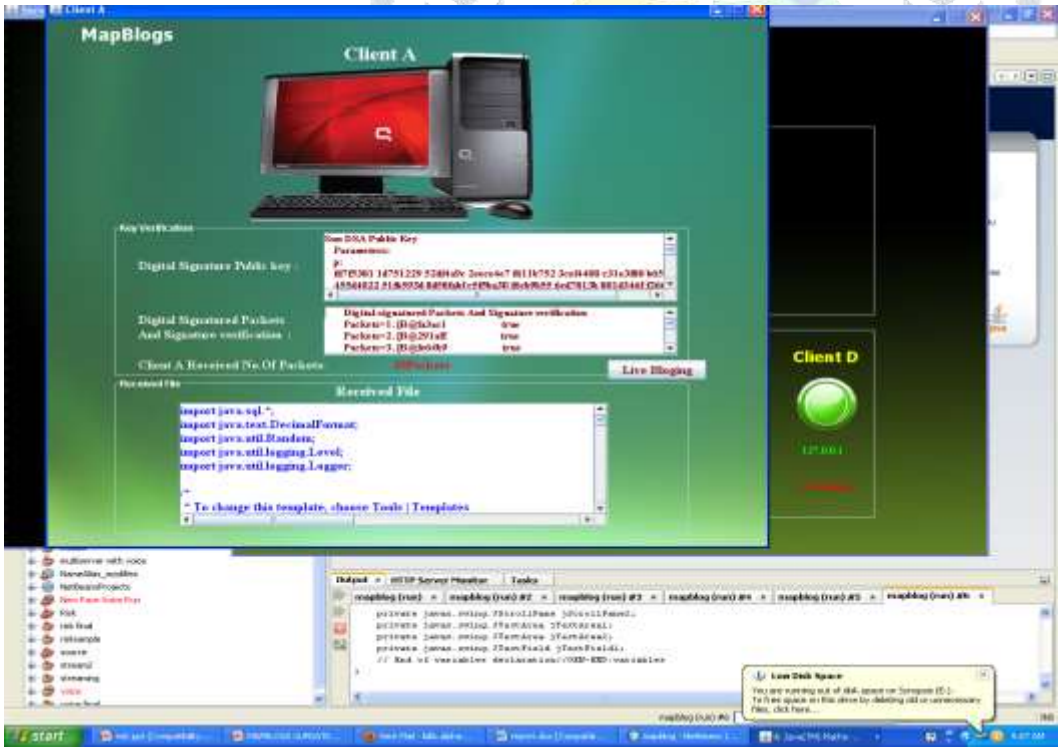
After the generation of the keys, the next step is to sign the data which is done by a button known as sign on data. The signature packets with their respective packet number's are being generated which is shown on a separate panel called as signature on data .Here ,for clustering.java , 3packets are generated along with their sign is shown. Once the packets are generated with their signatures files are sent to their clients respectively.

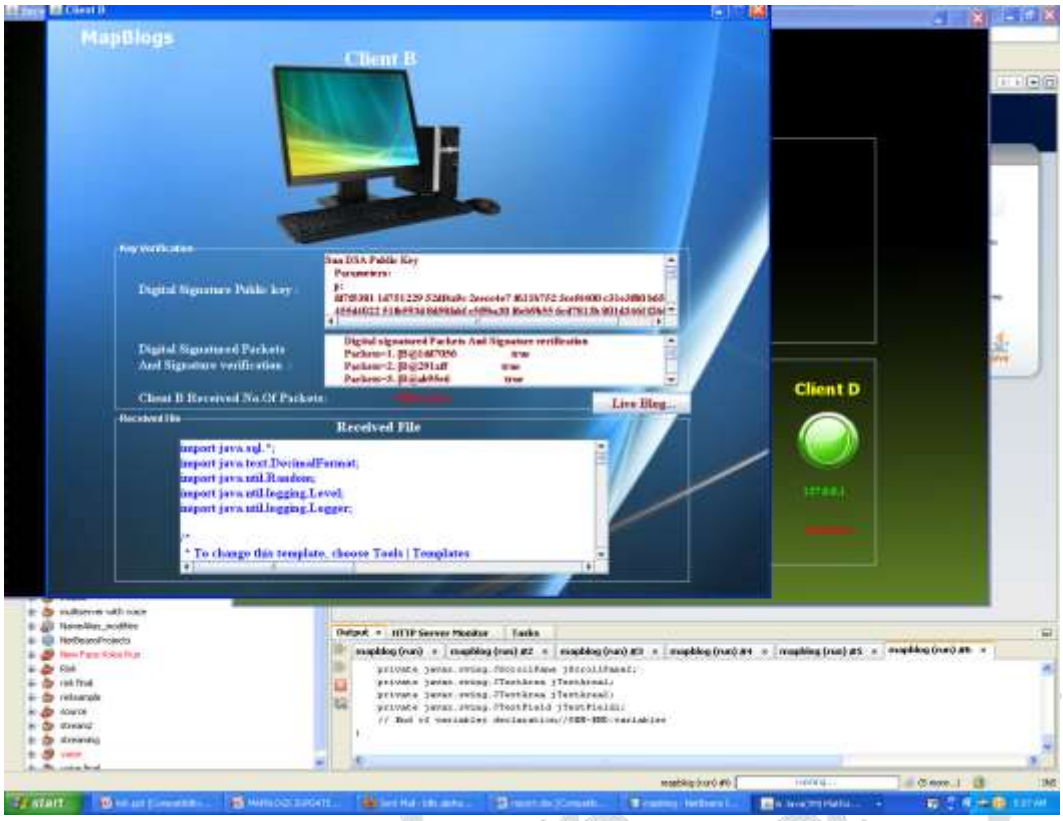
6.6 Files are received in Router



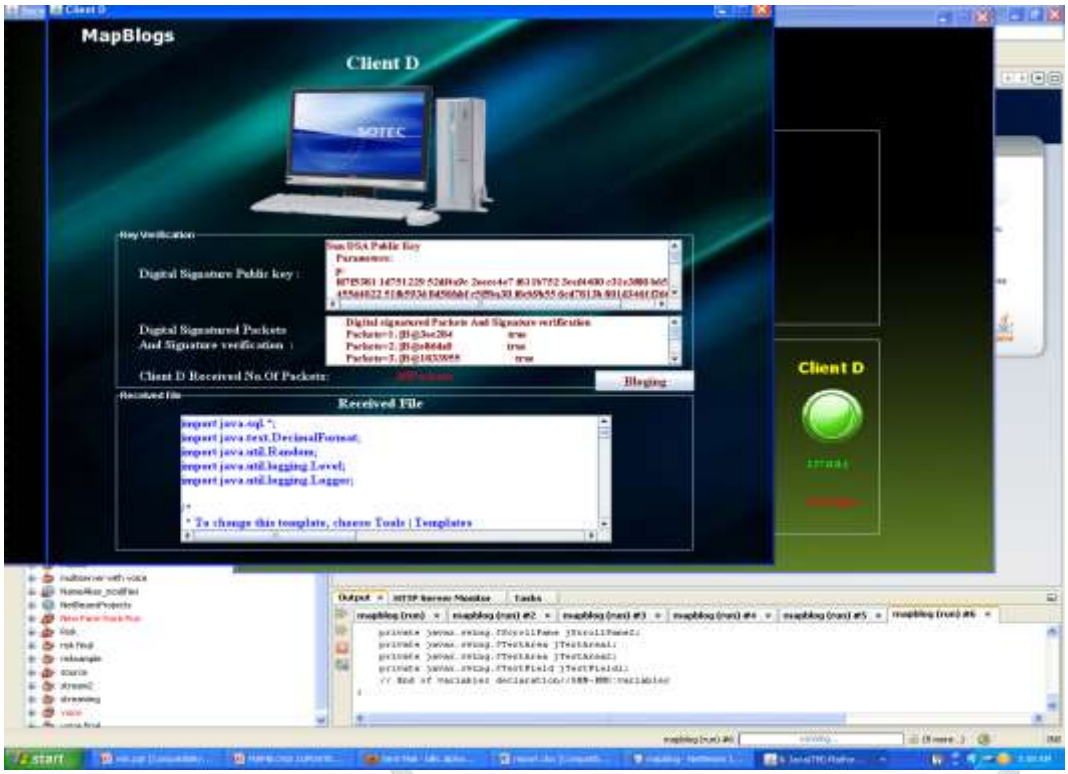
The connecting status of server and client can be seen ,when the 3 packets generated are found to be transferred from the server to clients and actual server contains 3 packets and the 4 clients ,client A, client B, client C, client D receive 3 packets each respectively. We can see that the clients have received 3 packets each .In the server Jframe, it shows that the packets have been transferred to clients with a green tick on all the clients .

6.7 Files are received to clients




MapBlogs
Client B
Client D
Received File


MapBlogs
Client C
Client D
Received File



When the file is send from the server to client A ,in the key verification frame there is a panel, we can see the generation of keys which is Sun DSA public key with their parameters. The signature packets with the number of packets to client A is generated as 3 in this case, the digital signature is found to be verified and it displays as true. In the received file panel, the sender sends file is found to be received by the client A demonstrating in the received file.

VII. CONCLUSION

To reduce the signature verification overheads in the secure multimedia Mapbloging, 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 due 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 BLS and DSA, which are more efficient than the batch RSA signature scheme. Even though this application has been developed with the
users own Protocols, this can be used in an Intranet based organization.

1. This system was developed so that people can exchange information as well as converse with each other.

2. Through this system people can access Blogging rooms globally.

3. The system is interactive and friendly.

4. Entire system is fully automatic to the clients and satisfies the clients request

5. Especially the system is more useful to the technical people when the need for sending pictures, images it is solved through WHITE BOARD UTILITY OF CANVAS.

FUTURE ENHANCEMENTS

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 within 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 (log2(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 voice chatting. Using VoIP protocol.

2. It can be enhanced in the field of Video Conferencing.

REFERENCES

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

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

[3] P. Judge and M. Ammar, "Security Issues and Solutions in Mulicast Content Distribution: A Survey," IEEE Network Magazine,
vol. 17, no. 1, pp. 30-36, Jan./Feb. 2003.

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

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

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

[7] 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.

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

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

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