AN SSL BACKEND FORWARDING ALGORITHM IN CLUSTER BASED WEB SERVERS

By

MEGALA.T

Register Number: **71206621031**

Of

KUMARAGURU COLLEGE OF TECHNOLOGY

COIMBATORE-6

A PROJECT REPORT

Submitted to the

FACULTY OF INFORMATION AND COMMUNICATION ENGINEERING

In partial fulfillment of the requirements
for the award of the degree
of

MASTER OF COMPUTER APPLICATIONS

ANNA UNIVERSITY
CHENNAI 600 025

June 2009

BONAFIDE CERTIFICATE

Certified that this project report titled **An SSL Backend Forwarding Algorithm in Cluster based web servers** is the bonafide work of **Megala.T**. (Register Number: **71206621031**) who carried out the research under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

30/6/09

Project Guide

Head of the Department

Submitted for the University Examination held on 6.7.2009

6/7/09

Internal Examiner

6/7

External Examiner

Ascentz
Solutions You Can Count On..........

ASCENTZ TECHNOLOGIES

Ph : 0422 - 4213170 / 900 367 0809
E-mail : ascentztech@yahoo.com
www.ascentz.com

17th June 2009
Coimbatore

TO WHOMSOEVER IT MAY CONCERN

This is to certify that Miss. **MEGALA.T (Reg. No: 71206621031)** Department of Master of Computer Applications studying in **Kumaraguru College of Technology** is doing her final year project **"AN SSL BACKEND FORWARDING ALGORITHM IN CLUSTER BASED WEB SERVERS"** in our esteemed concern under my supervision and guidance during the time period of 20th Dec 2008 to 29th May 2009.

For Ascentz Technologies

Ascentz Technologies ★ 0422 4213170 ★ batore-12

HR Manager

ABSTRACT

The SSL-session (Secure Socket Layer) reuse scheme has been tested on a single Web server node and extended to a cluster system that consisted of three Web servers. In this paper, the SSL-session reuse scheme using 16-node and 32-node cluster systems with various levels of workload are explored. Thirdly, proposed a back-end forwarding mechanism by exploiting the low-overhead user-level communication to enhance the SSL-enabled network server performance.

Three distribution models in clusters are compared: Round Robin (RR), ssl_with_session, and ssl_with_bf (backend_forwarding). The RR model, widely used in Web clusters, distributes requests from clients to servers using the RR scheme. ssl_with_session uses a more sophisticated distribution algorithm in which subsequent requests of the same client are forwarded to the same server, avoiding expensive SSL setup costs. The proposed ssl_with_bf uses the same distribution policy as the ssl_with_session, but includes an intelligent load balancing scheme that forwards client requests from a heavily loaded back-end node to a lightly loaded node to improve the utilization across all nodes. This policy uses the underlying user-level communication for fast communication.

ACKNOWLEDGEMENT

First and foremost I thank God for his good will and blessings showered on me throughout the project. The success of this project needs cooperation and encouragement from different quarters.

I wish to express my deep unfathomable feeling of gratitude and indebtedness to **Mr,R.Annamalai,Vice Principal,Kumaraguru College of Technology, Coimbatore** for the successful completion of the project work.

I am very gladly taking this opportunity to express a special word of thanks to **Dr. M. Gururajan, Head of the Department of MCA, Kumaraguru College of Technology, Coimbatore** for encouraging me to do this work.

I am very much indebted to my guide and project co-ordinator **Ms.V.Geetha,Assistant Professor,Department of MCA, Kumaraguru College of Technology, Coimbatore** for her complete assistance, guidance and support given to me throughout my project.

My hearty thanks to my Guide **Mr. R.Tamilselvan** of **Ascentz Technologies, Coimbatore**, for their valuable guidance throughout the project. Also, I am grateful to my parents and friends who were the real source of my project.

TABLE OF CONTENT

Appendices

LIST OF TABLES

LIST OF ABBREVATIONS

ACRONYMS	FULL FORM
SSL	Secure Socket Layer
NLB	Network Load Balancing
RR	Round Robin
Bf	Back-end Forwarding
VIA	Virtual Interface Architecture
HTML	Hyper Text Markup Language

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 PROJECT OVERVIEW

Due to the growing popularity of the Internet, data centers/network servers are anticipated to be the bottleneck in hosting network-based services, even though the network bandwidth continues to increase faster than the server capacity. It has been observed that network servers contribute to approximately 40 percent of the overall delay, and this delay is likely to grow with the increasing use of dynamic Web contents. For Web-based applications, a poor response time has significant financial implications. For example, E-Biz reported about $1.9 billion loss in revenue in 1998 due to the long response time resulting from the Secure Sockets Layer (SSL), which is commonly used for secure communication between clients and Web server.

Even though SSL is the de facto standard for transport layer security, its high overhead and poor scalability are two major problems in designing secure large-scale network servers. Deployment of SSL can decrease a server's capacity by up to two orders of magnitude.

In addition, the overhead of SSL becomes even more severe in application servers. Application servers provide dynamic contents and the contents require secure mechanisms for protection. Generating dynamic content takes about 100 to 1,000 times longer than simply reading static content. Moreover, since static content is seldom updated, it can be easily cached. Several efficient caching algorithms have been proposed to reduce latency and increase throughput of front-end Web services. However, because dynamic content is generated during the execution of a program, caching dynamic content is not an efficient option like caching static content?

Recently, a multitude of network services have been designed and evaluated using cluster platforms. Specifically, the design of distributed Web servers has been a major research thrust to improve the throughput and response time. It is the first Web server model that exploits user-level communication in a cluster-based Web server. Existing System reduces the response time in a cluster-based Web server using co- scheduling schemes.

In this paper, investigation has been done on the impact of SSL offering in cluster-based network servers, focusing on application servers, which mainly provide dynamic content. Secondly showed the possible performance improvement when the SSL-session reuse scheme is utilized in cluster based servers. The SSL-session reuse scheme has been tested on a single Web server node and extended to a cluster system that consisted of three Web servers.

In this paper, the SSL-session reuse scheme using 16-node and 32-node cluster systems with various levels of workload are explored. Thirdly, proposed a back-end forwarding mechanism by exploiting the low-overhead user-level communication to enhance the SSL-enabled network server performance.

Three distribution models in clusters are compared: Round Robin (RR), ssl_with_session, and ssl_with_bf (backend_forwarding). The RR model, widely used in Web clusters, distributes requests from clients to servers using the RR scheme. ssl_with_session uses a more sophisticated distribution algorithm in which subsequent requests of the same client are forwarded to the same server, avoiding expensive SSL setup costs. The proposed ssl_with_bf uses the same distribution policy as the ssl_with_session, but includes an intelligent load balancing scheme that forwards client requests from a heavily loaded back-end node to a lightly loaded node to improve the utilization across all nodes. This policy uses the underlying user-level communication for fast communication.

Extensive performance analyses with various workload and system configurations are summarized as follows: First, schemes with reusable sessions, deployed in the ssl_with_session and ssl_with_bf models, are essential to minimize the SSL overhead. Second, the average latency can be reduced by 40 percent with the proposed ssl_with_bf model compared to the ssl_with_session model, resulting in improved throughput. Third, the proposed scheme provides high utilization and better load balance across all nodes. The rest of this paper is organized as follows: a brief overview of cluster-based network servers, user-level communication, and SSL is provided.

1.2 ORGANIZATION PROFILE

Ascentz Technologies is a custom software development and Solutions Company based in Kovai, India. Ascentz Technologies possesses an experience in providing complex and diverse enterprise software development solutions to a large range of clients.

Ascentz Technologies, premier software solution providers in India. In brief stint we grown and developed many customized solutions across various domains/verticals. Our team works cooperatively to produce success for our clients. Gaining their trust and building a long-lasting affiliation. This tie up helps us to give in our best and generate good results and accomplishing the goals in a well premeditated structure. Our solutions not only productive but also have valued affordably for all our clients ranging from start ups, small business to leading corporations. Our team of experts provides a variety of best services on Sustainability, Focus, Dedication, and Cost Effectiveness. We explore it into all the major facets of corporate information technology.

Ascentz Technologies has the exclusive experience in the software development stature, which takes pleasure of the customer retention rate.

Ascentz Technologies excels principled technology for the services promising outstanding business exposure for its clients. Ascentz Technologies providing services that influence evolving efficient business model for the exclusive liberation.

Associated with a highly skilled team we are tweaking exclusive development and execution procedure to its benefited clients. Moreover, this is enabling us for the time bound delivery of the challenging solutions with confidence.

The company is focusing on providing technical consultancy and solutions in the automation industry for various applications. Also looks at providing the necessary business computing systems for optimizing the total systems integration, with the help of its vast product range. They increase their clients' competitiveness by rolling out industry solutions leveraging our proven software products, information technology solutions and business Process optimization services.

CHAPTER 2

SYSTEM REQUIREMET SPECIFICATION

The Software requirement specification is a technical specification of requirements for the software product. The goal of software requirements definition is to completely specify the technical requirements for the software products in a concise and unambiguous manner.

2.1 HARDWARE ENVIRONMENT

The hardware support required for deploying the application

➢ Processor	:	Intel Pentium III or Above
➢ RAM	:	512 MB
➢ Monitor	:	17" Color Monitor
➢ Hard Disk	:	40 GB

2.2 SOFTWARE ENVIRONMENT

The software support required for deployment

➢ Operating System	:	Windows 98/2000/XP/NT
➢ Front-End tool	:	ASP.NET
➢ Back-End Tool	:	SQL Server

2.3 SOFTWARE OVERVIEW

2.3.1 VB.Net Framework

VB.Net is a simple, type-safe, object-oriented, general-purpose programming language. It provides code-focused developers with powerful tools and language support to build rich, connected Web and client applications on the .NET Framework.

2.3.1.1 VB.Net overview

- Visual Studio .Net has flexibility, allowing one or more language to interoperate to provide the solution. This Cross Language Compatibility allows to do project at faster rate.
- Visual Studio. Net has Common Language Runtime, which allows the entire component to converge into one intermediate format and then can interact.
- Visual Studio. Net has provide excellent security when the application is executed in the system

2.3.1.2 Features of VB.Net

- Visual Studio.Net has flexibility, allow to configure the working environment to best suit for individual style. It can choose between a single and multiple document interfaces, and can adjust the size and positioning of the various IDE elements.
- Visual Studio. Net has Intelligence feature that make the coding easy and also dynamic help provides very less coding time.
- The working environment in Visual Studio.Net is often referred to as Integrated Development Environment because it integrates many different functions such as design, editing, compiling and debugging within a common environment. In most

traditional development tools, each of separate program, each with its own interface.

- The Visual Studio.Net language is quite powerful – can imagine a programming task and accomplished using Visual Basic .Net.
- After creating a Visual Studio. Net application,it can be freely distribute it to others who uses Microsoft windows. it can be distributed by applications on disk, on CDs, across networks, or over an intranet or the internet.
- Toolbars provide quick access to commonly used commands in the programming environment. By clicking a button on the toolbar once to carry out the action represented by that button. By default, the standard toolbar is displayed when Visual Basic starts. Additional toolbars for editing, form design, and debugging can be toggled on or off from the toolbars command on the view menu.
- Many parts of Visual Studio are context sensitive. Context sensitive is a help on some parts directly without having to go through the help menu. For example, to get help on any keyword in the Visual Basic language, place the insertion point on that keyword in the code window and press F1.
- Visual Studio interprets the code as once entered , catching and highlighting most syntax or spelling errors on the fly. It's almost like having an expert watching over the shoulder as once enters into the code.

2.3.2 SQL SERVER 2000

The OLAP Services feature available in SQL Server version 7.0 is now called SQL Server 2000 Analysis Services. The term OLAP Services has been replaced with the term Analysis Services. Analysis Services also includes a new data mining component. The Repository component available in SQL Server version 7.0 is now called Microsoft SQL Server 2000 Meta Data Services. References to the component now use the term Meta Data Services. The term repository is used only in reference to the repository engine within Meta Data Services

2.3.2.1 Overview of SQL Server 2000

SQL-SERVER database consist of five type of objects. They are,

1. **TABLE**
2. **QUERY**
3. **FORM**
4. **REPORT**
5. **MACRO**

2.3.2.1.1 Table:

A database is a collection of data about a specific topic.

Views of Table:

We can work with a table in two types,

1. Design View
2. Datasheet View

Design View

To build or modify the structure of a table we work in the table design view. We can specify what kind of data will be hold.

Datasheet View

To add, edit or analyses the data itself we work in tables datasheet view mode.

2.3.2.1.2 Query:

A query is a question that has to be asked the data. Access gathers data that answers the question from one or more table. The data that make up the answer is either dynaset (if manually edited) or a snapshot (it cannot be edited).Each time while run query, latest information in the dynaset is reported. Access either displays the dynaset or snapshot to view or perform an action on it, such as deleting or updating.

2.3.2.1.3 Forms:

A form is used to view and edit information in the database record by record. A form displays only the information we want to see in the way we want to see it. Forms use the familiar controls such as textboxes and checkboxes. This makes viewing and entering data easy.

Views of Form:

We can work with forms in several primarily there are two views. They are,

1. Design View

2. Form View

Design View

To build or modify the structure of a form, we work in forms design view. We can add control to the form that are bound to fields in a table or query, includes textboxes, option buttons, graphs and pictures.

Form View

The form view which display the whole design of the form.

2.3.2.1.4 Report:

A report is used to view and print information from the database. The report can ground records into many levels and compute totals and average by checking values from many records at once. Also the report is attractive and distinctive because we have control over the size and appearance of it.

2.3.2.1.5 Macro:

A macro is a set of actions. Each action in macros does something. Such as opening a form or printing a report .We write macros to automate the common tasks the work easy and save the time.

2.3.2.2 Features of SQL Server 2000

SQL SERVER 2005 provides statements for a variety of tasks, including

- Querying data
- Inserting, updating, and deleting rows in a table
- Creating, replacing, altering, and dropping objects
- Controlling access to the database and its objects
- Guaranteeing database consistency and integrity

CHAPTER 3

SYSTEM ANALYSIS

System Analysis is the process of understanding a problem domain and the user requirements for the purpose of developing a computer application system to serve the users.

3.1 EXISTING SYSTEM

In existing system, they have used to develop the project using Round Robin [RR] model and SSL_with_Session model. Those models are not effective. Those models are not able to give the out put in time and the thorough put also lesser than that their expected output.These models had made the Latency problem and minimal through put. For this problem they introduced the SSL_with_bf (Backend forwarding) model is to overcome the existing problems.

3.1.1 Limitations of existing system

- Long response time
- Poor scalability
- Not suitable for large-scale network servers
- Less security

3.2 PROPOSED SYSTEM

In the Proposed System, SSL_with_Backend Forwarding model (Algorithm) has been implemented to overcome the problem of existing system. This model will reduce the latency and increase the throughput than the existing system (Round Robin model and SSL_with_Session).The Secure Socket Layer_with_BF model is very helpful for load balancing of the server. This will reduce the load of the server while the server is being busy. The ssl_with_bf scheme can minimize the average latency by about 40 percent and improve throughput across a variety of workloads. It is the first Web server model that exploits user-level communication in a cluster-based Web server.

3.2.1 Advantages of proposed system

- Latency time is minimized.
- Fast response time
- High security
- Throughput time is increased
- More scalability

CHAPTER 4

SYSTEM DESIGN

System design is the most creative and challenging phase in the life cycle of system development. The first step to determine is what input data is needed to form the system and the database that has to be designed should meet the requirement of the proposed system. The next step is to determine how the output is produced and in what format.

4.1 ELEMENTS OF DESIGN

The following are the elements of the system design

- Input design
- Output design
- Database design

4.1.1 Input design

The input design is the process of converting the user-oriented inputs into computer –based format. The goal of designing input data is to make the automation as easy and free from errors as possible. The requirements of input design such as user friendliness, consistent format and interactive dialogues for giving the right message and help for the user at right time are also considered for development of the project.

The input forms used in this system are:

a. Login Form: This form gets the user name and password from the user and administrator as input, and verifies the details if they have already registered.

b. New user Login Form: If new user entering into the project they have to register and they should give some details like user name, password, address, phone number and e-mail.

c. IP Address Representation: In this module the user can enter new IP address of the server and system. Previous IP address can also be used

d. Key Generator: After selecting the file to encrypt the key should be generated. Keys will be generated automatically if the user selects the key generator button.

e. Downloading a File: The user should select what file to be downloaded from the displayed. list information like customer name, address, personal details, bank name, card type and the pan number through which his transaction details are updated.

f. Browse: The administrator uses the browse option to locate the file for uploading and to open private keys and public keys browse option can be used.

g. Save: This option is used for saving public keys and private keys

h. Upload: The administrator uses this option to upload the file in the server.

4.1.2 Output design

The outputs are mainly used to communicate with the user processing the input data given by the user. It is documented in each stage of the project to ensure error free output. The output screens are designed in a very simple ad easy to understand format. All user options are presented in well-formatted forms. The user friendliness of the output screen makes it very easy to use. The quality refers to the way by which the output is presented to the user.

The main outputs of the system are:

a. IP Address: The customer can view the IP address of the servers and the listeners or they can enter the new IP address

b. Encryption: Encryption has to be done while uploading the file. Encrypted format is displayed after the key is generated

c. Selection of files: All files will be displayed which are uploaded in the server. The user has to select the file name that is to be downloaded

d. Response Time: After selecting the file the response time of the particular file in the different server will be displayed. The user can make out the difference of the servers.

e. Downloaded form: The file will be downloaded in the encrypted form. The user has to open private key to convert in the original text.

4.1.3 Database design

An entity-relationship model is an abstract conceptual representation of structured data. **Entity-relationship modeling** is a relational schema database modeling method, used in software engineering to produce a type of conceptual data model (or semantic data model) of a system, often a relational database, and its requirements in a top-down fashion. Diagrams created using this process are called *entity-relationship diagrams*, or *ER diagrams* for short. The E-R diagram for the project is shown in figure 4.1

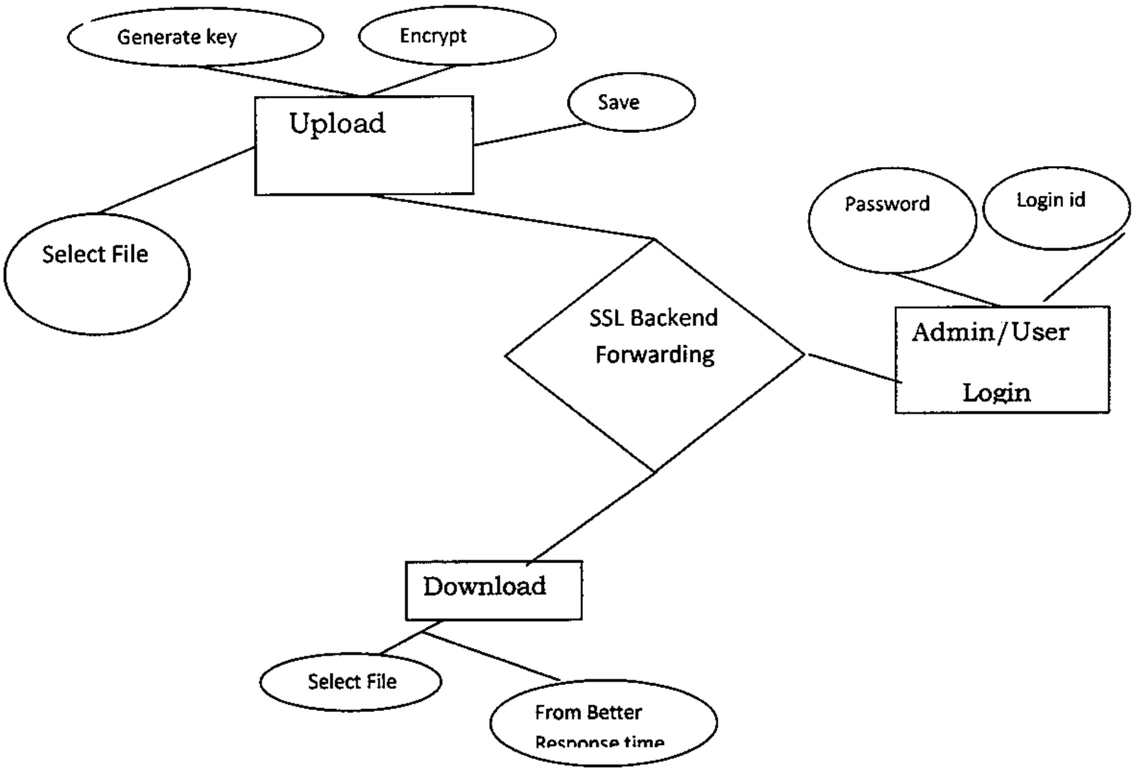


Figure 4.1: Entity Relationship Diagram

4.2 DATABASE DESIGN

A database is a collection of inter-related data stored with minimum redundancy to serve many users quickly and efficiently. The general objective of database design is to make the data access easy, inexpensive and flexible to the user. An elegantly designed database can play a strong foundation for the whole system.

The details about the relevant data for the system are first identified. According to their relationship, tables are designed through the following method.

- The data type for each data item in the table is decided.
- The tables are then normalized.

The tables are normalized so that they can provide better response time, have data integrity, avoid redundancy and be secure. The table formats are shown from table 4.1-4.4

Table Name : **Login**

Description: This table is used to maintain username and password of previously registered users.

Name	**Type**	**Description**
Usrname	VARCHAR	Name of the user/Administrator
Pwd	VARCHAR	Secured password of the user/Administrator

Table 4.1

4.3.1.2 Table Name: **Register**

Description: It is used to hold the information of the new users.

Name	**Type**	**Description**
Usrname	Varchar	Name of the user
Pwd	Varchar	Password of the user
Addr	Varchar	Address of the customer
Phoneno	Number	PhoneNo of the customer
E-Mail	Varchar	E-mail id of the customer

Table 4.2

4.3.1.3 Table Name : **Up**

Description: Holds the information about the uploading files

Name	**Type**	**Description**
Did	Int	To get the designation id
Loc	Varchar	To view the location

Table 4.3

4.3.1.4 Table Name: **Ipaddr**

Description: Holds details about the IP address assigned to each server.

Name	**Type**	**Description**
Sip	VARCHAR	Server IP address
L1ip	VARCHAR	Listener1IP address
L2ip	VARCHAR	Listener2 IP address

Table 4.4

CHAPTER 5

USE-CASE DIAGRAM

5.1 USE CASE DIAGRAM

A **use case diagram** is used to represent a graphical overview of the functionality provided by a system in terms of actors, their goals, represented as use cases and any dependencies between those use cases. The use-case diagram for the project is shown in the figure 5.1

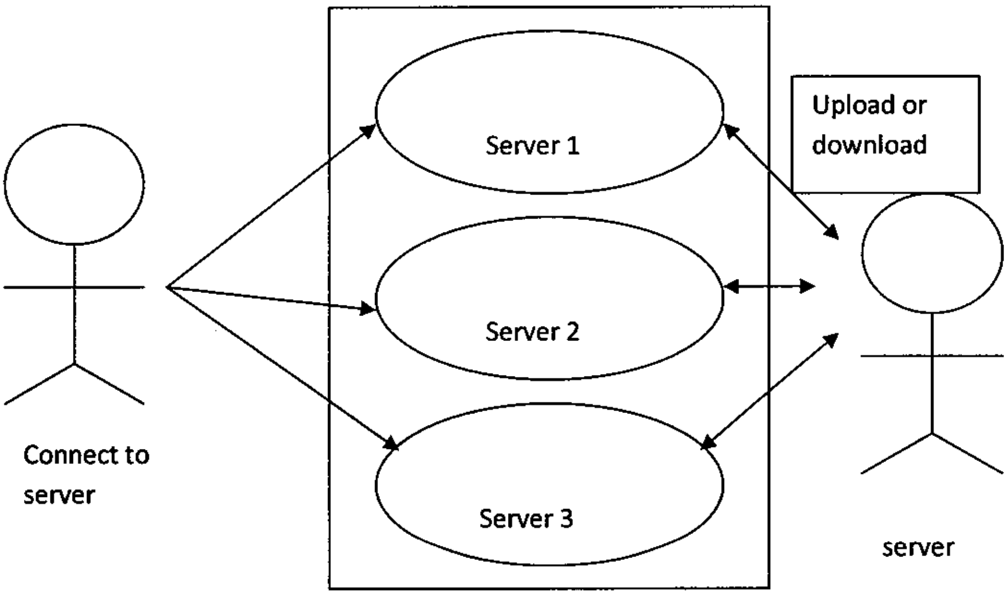
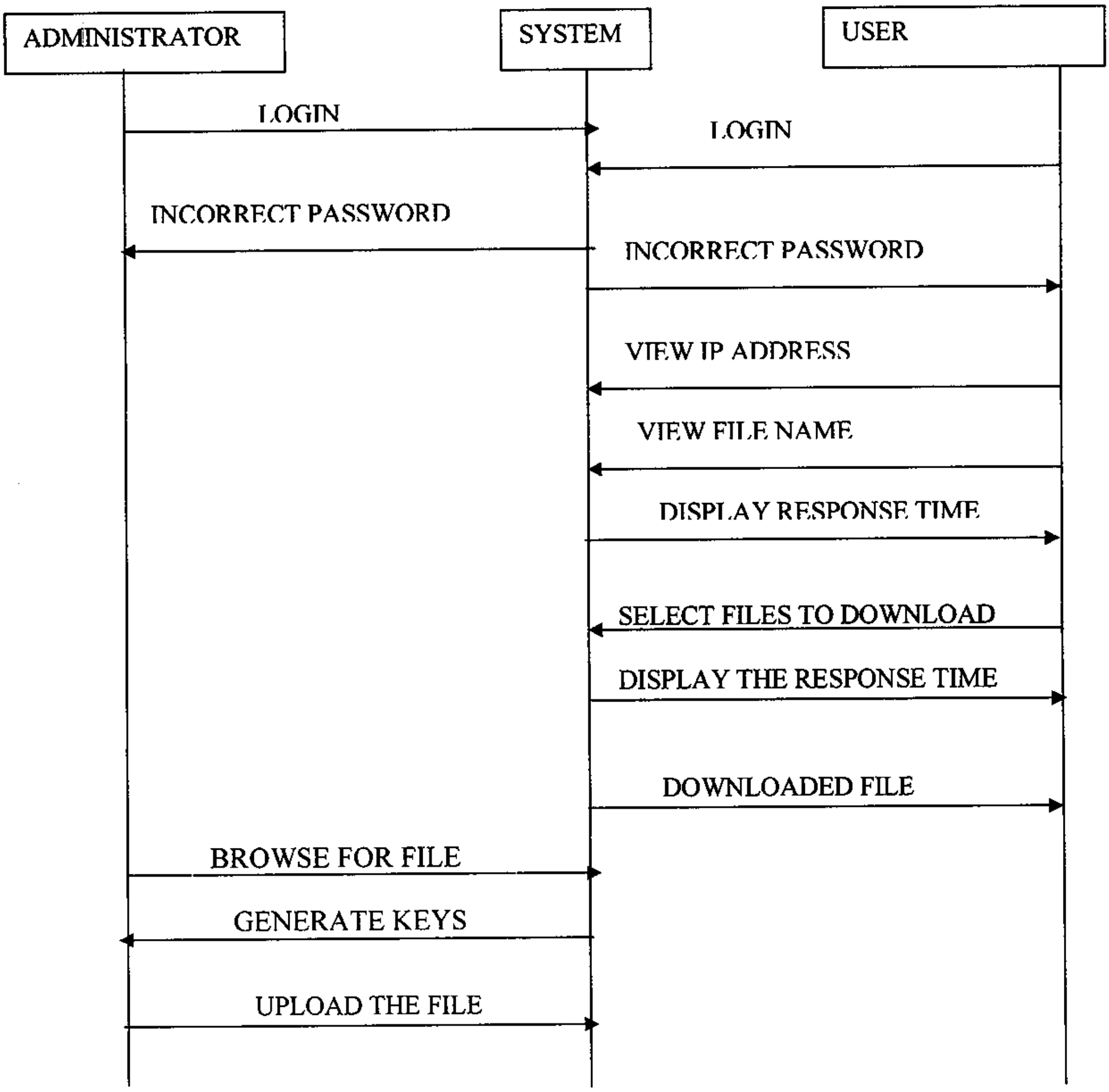


Figure 5.1 Use-case diagram

5.2 SEQUENCE DIAGRAM

A sequence diagram is a form of interaction diagram which shows objects as lifelines running down the page, with their interactions over time represented as messages drawn as arrows from the source lifeline to the target lifeline. Sequence diagrams are good at showing which objects communicate with which other objects; and what messages trigger those communications. The sequence diagram for the project is shown in the figure 5.2



5.3 DATA FLOW DIAGRAM

Data flow diagram shows the flow of data between different processes in the project. The data flow diagram for the project is shown in figure-5.3

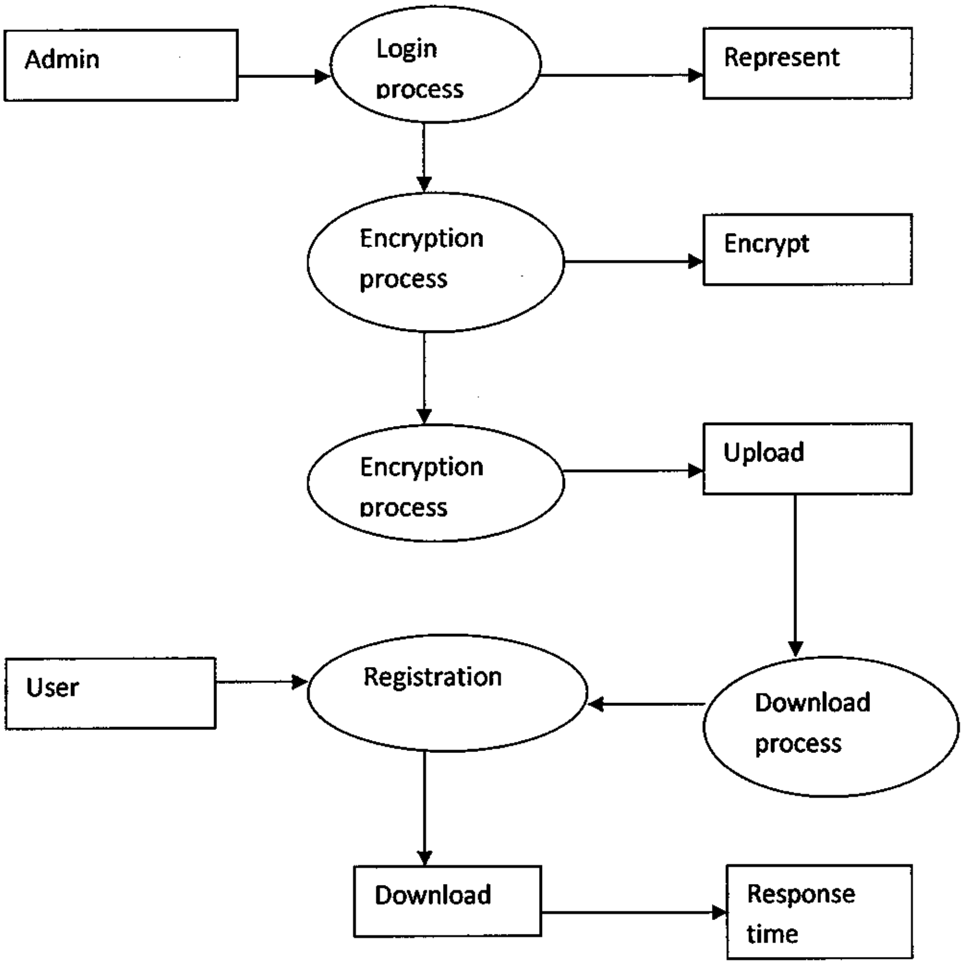


Figure 5.3 Data-Flow Diagram

CHAPTER 6

SYSTEM TESTING AND IMPLEMENTATION

Software Testing and implementation is the process done in the development stage of the software.

6.1 TEST PLAN

Testing is the process of executing a program with the indent of finding any errors. Testing is vital to the success of the system. Without proper testing, hidden errors will surface after some time of use and perhaps irreversible damage has been doe to valuable data. A successful test is one that uncovers as yet undiscovered errors.

S.NO	TEST CASE	EXPECTED RESULT	ACTUAL RESULT
1.	User id: admin Password:administrator	Invalid login	Invalid login
2.	User id: admin Password: admin	Valid login	Valid login
3.	If the administrator select the generate keys in the menu	Private and public key should be generated automatically	Public key and private key should be generated automatically with the extension .kez,.pke

4.	If the user clicks the download button	All files should be displayed which are available in the server	All files should be displayed which are available in the server
5.	If the user clicks the download button after selecting the file	Response time of the different server should be displayed	Response time of the different server should be displayed

6.2 TYPE OF TESTING

Testing is a critical element of software quality and assurance and represents the ultimate review of specification design and coding. It is a vital activity that has to be enforced in the development of any system. This could be done in parallel during all the phases of system development. The feedback received from these tests can be used for further enhancement of the system under consideration. The testing phase conducts test using the Software Requirement Specification as a reference and with the goal to see whether the system satisfies the specified requirements.

6.2.1. Unit Testing

Unit testing verification efforts on the smallest unit of software design, module. This is known as "Module Testing". The modules are tested separately. This testing is carried out during programming stage itself. In these testing steps, each module is found to be working satisfactorily as regard to the expected output from the module.

6.3.1.2 Integration testing

Integration testing is a systematic technique for constructing tests to uncover error associated within the interface. In the project, all the modules are combined and then the entire programmer is tested as a whole. In the integration-testing step, all the error uncovered is corrected for the next testing steps.

6.3.1.3 Validation Testing

To uncover functional errors, that is, to check whether functional characteristics confirm to specification or not specified.

6.3.1.4 Regression Testing

Regression testing is any type of software testing which seeks to uncover software regressions. Such regressions occur whenever software functionality that was previously working correctly, stops working as intended. Typically regressions occur as an unintended consequence of program changes. Common methods of regression testing include re-running previously run tests and checking whether previously fixed faults have re-emerged.

In this project, regression testing is an integral part of the extreme programming software development method. In this method, design documents are replaced by extensive, repeatable, and automated testing of the entire software package at every stage in the software development cycle.

In this project, regression testing has been performed by a software quality assurance person after the development person has completed work. However, defects found at this stage are the most costly to fix. This problem is being addressed by the rise of developer testing. Although developers have always written test cases as part of the development cycle, these test cases have generally been either functional tests or unit tests that verify only intended outcomes. Developer testing compels a developer to focus on unit testing and to include both positive and negative test cases.

6.3.1.5 System Testing

System testing is actually a serious of different tests, whose primary purpose is to fully exercise the computer-based system. This helps in verifying that all the system elements have been properly integrated and perform the allocated functions. It verifies the entire product after having integrated all software and hardware components, and validates it according to the original project requirement. The system testing takes into consideration the hardware, and the software.

6.3.1.6 Smoke Testing

Smoke testing is done by developers before the build is released or by testers before accepting a build for further testing, Smoke testing is the most cost effective method for identifying and fixing defects in software. A smoke test generally consists of a collection of tests that can be applied to a newly created or repaired computer program. In this sense a smoke test is the process of validating code changes before the changes are checked into the larger product's official source code collection or the main branch of source code.

In this project smoke testing is carried out very frequently to check the consistency before a build.

6.3 SYSTEM VERIFICATION

System Verification answers the question "Am I building the product right?" It includes the review of interim work steps and interim deliverables during a project to ensure they are acceptable. Verification also determines if the system is consistent, adheres to standards, uses reliable techniques and prudent practices, and performs the selected functions in the correct manner. In data access, it verifies whether the right data is being accessed, in terms of the right place and in the right way.

6.4 SYSTEM VALIDATION

Validation answers the question "Am I building the right product?" This checks whether the developer is moving towards the right product, whether the development is moving towards the actual intended product that was agreed upon in the beginning. Validation also determines if the system complies with the requirements and performs functions for which it is intended and meets the organization's goals and user needs. It is traditional and is performed at the end of the project. In data access, it checks whether we are accessing the right data, in terms of data required to satisfy the requirement.

6.5 SYSTEM IMPLEMETATION

Implementation literally means to put into effect or to carry out. The system implementation phase of the software deals with the translation of the design specification into the source code. Coding is done in this stage using an .net framework and programming language. Various types of bugs were discovered while debugging the modules. These were verified, tested and modified.

Once the working application was verified, tested and modified the system could be implemented in the user environment.

CHAPTER 7

CONCLUSION

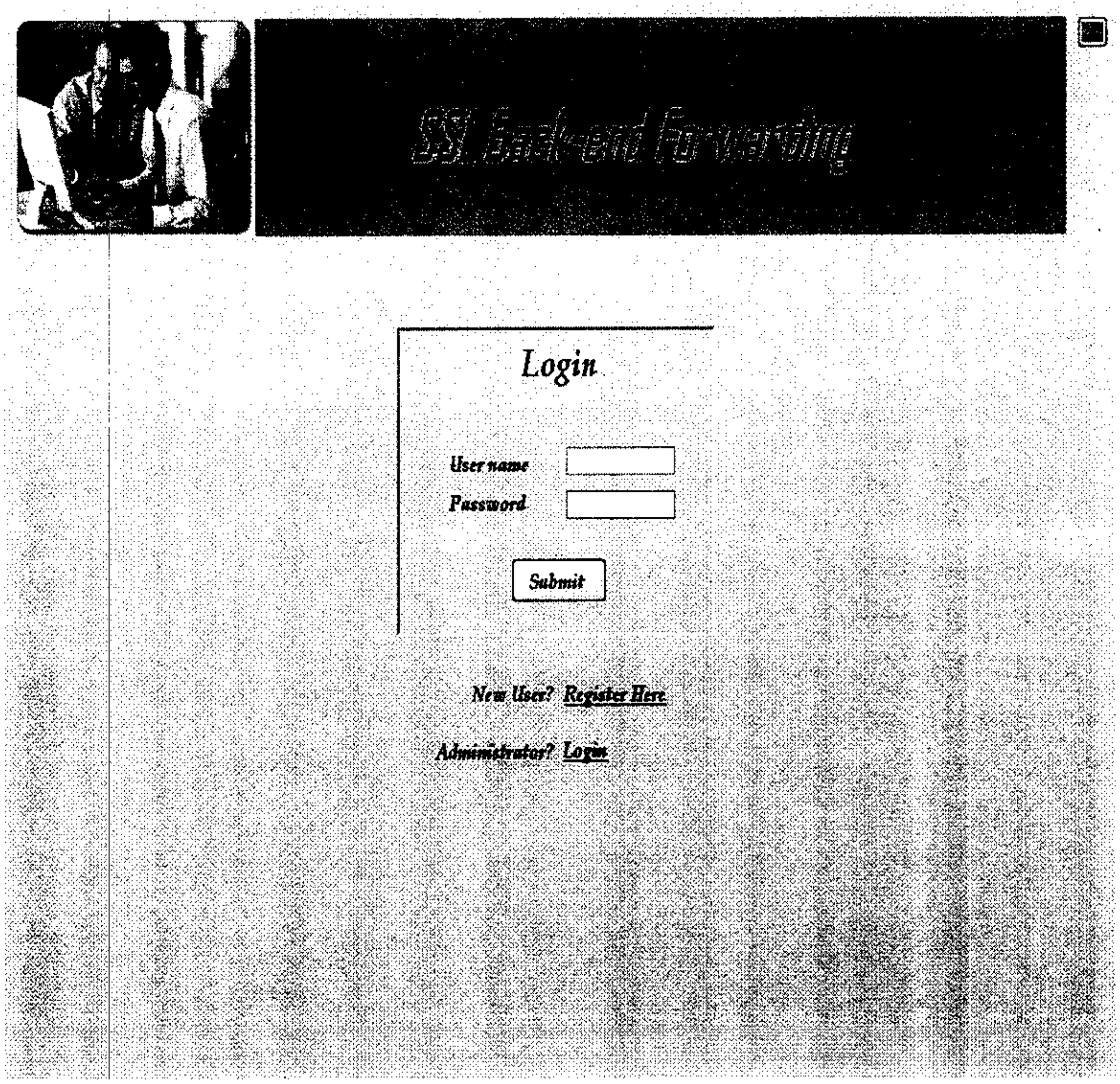
7.1 CONCLUSION

Finally, investigated the performance implications of the SSL protocol for providing a secure service in a cluster-based application server and proposed a back-end forwarding scheme for improving server performance through a better load balance. The proposed ssl_with_bf scheme exploits the underlying user-level communication in order to minimize the intracluster communication overhead. Comparisons between three application server models are done, RR, ssl_with_session, and ssl_with_bf, through simulation. The simulation model captures the VIA communication characteristics and the application server design in sufficient detail and uses realistic numbers for SSL encryption overheads obtained from measurements. Simulation with 16-node and 32-node cluster configurations with a variety of workloads provides the following conclusions: First, schemes with reusable sessions, deployed in the ssl_with_session and ssl_with_bf models, are essential for minimizing the SSL overhead. Second, the average latency can be reduced by about 40 percent with the ssl_with_bf model compared to the ssl_with_session model, resulting in improved throughput. Third, ssl_with_bf yields a better performance with the mixed clients, whereas the performance of the ssl_with_session model is degraded due to the increasing skew ness. Finally, ssl_with_bf is more robust than ssl_with_session in handling variable file sizes.

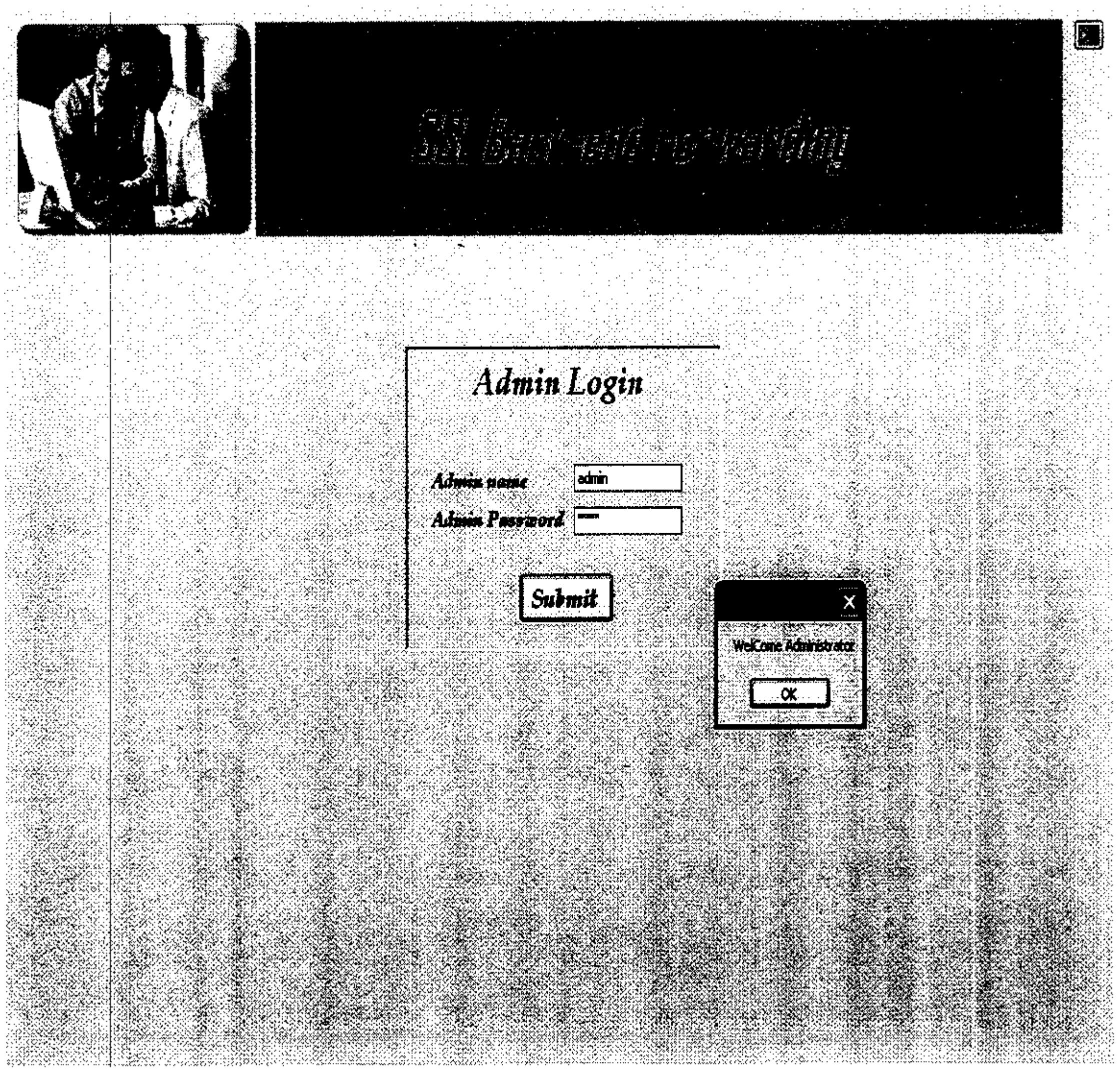
All of these results indicate that the proposed back-end forwarding scheme is a viable mechanism for improving the performance of secure cluster-based network servers.

APPENDICES

HOME PAGE:



ADMIN LOGIN:



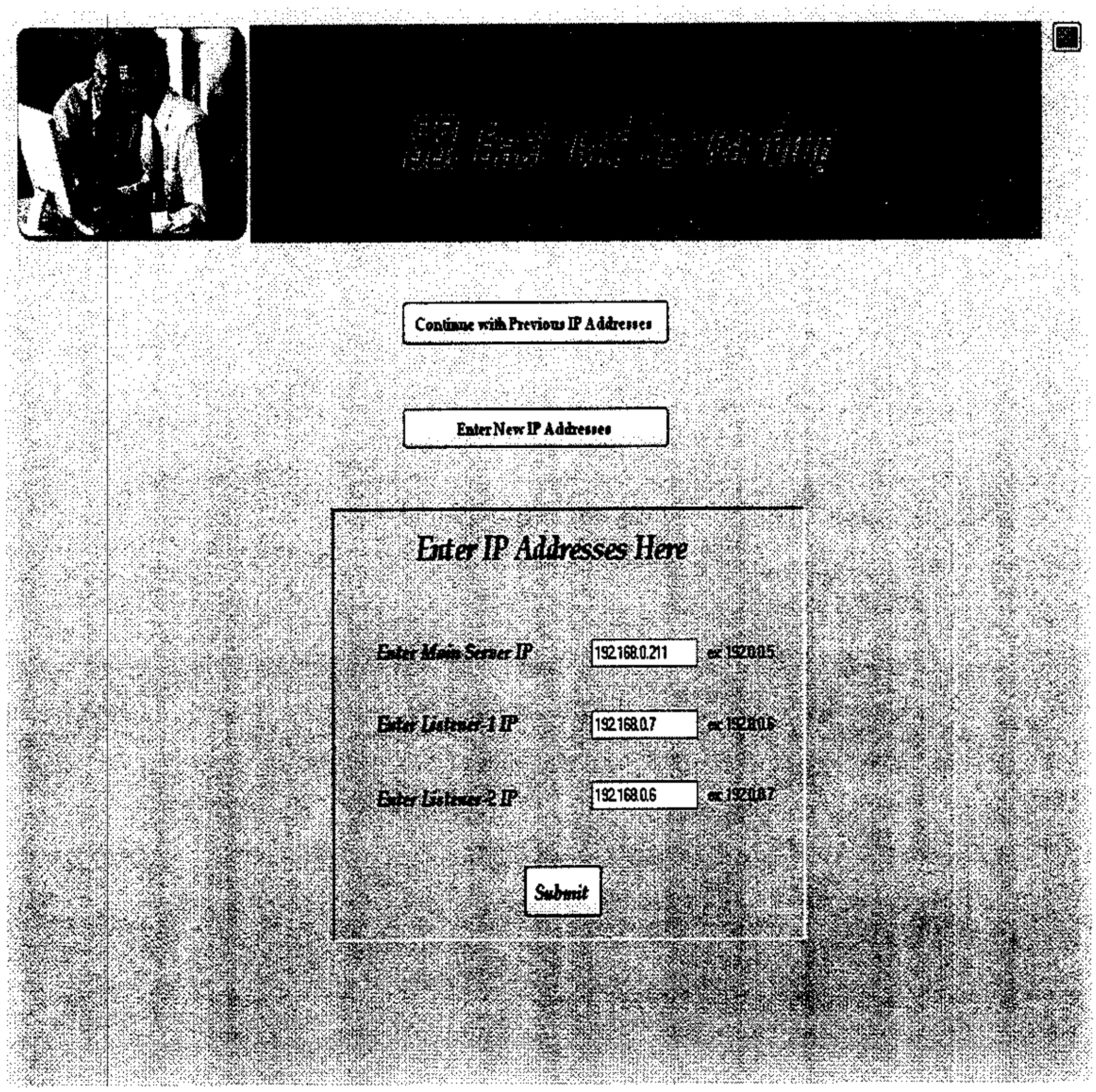
Admin Login

Admin name: admin

Admin Password: *****

WelCome Administrator

IP ADDRESS REPRESENTATION



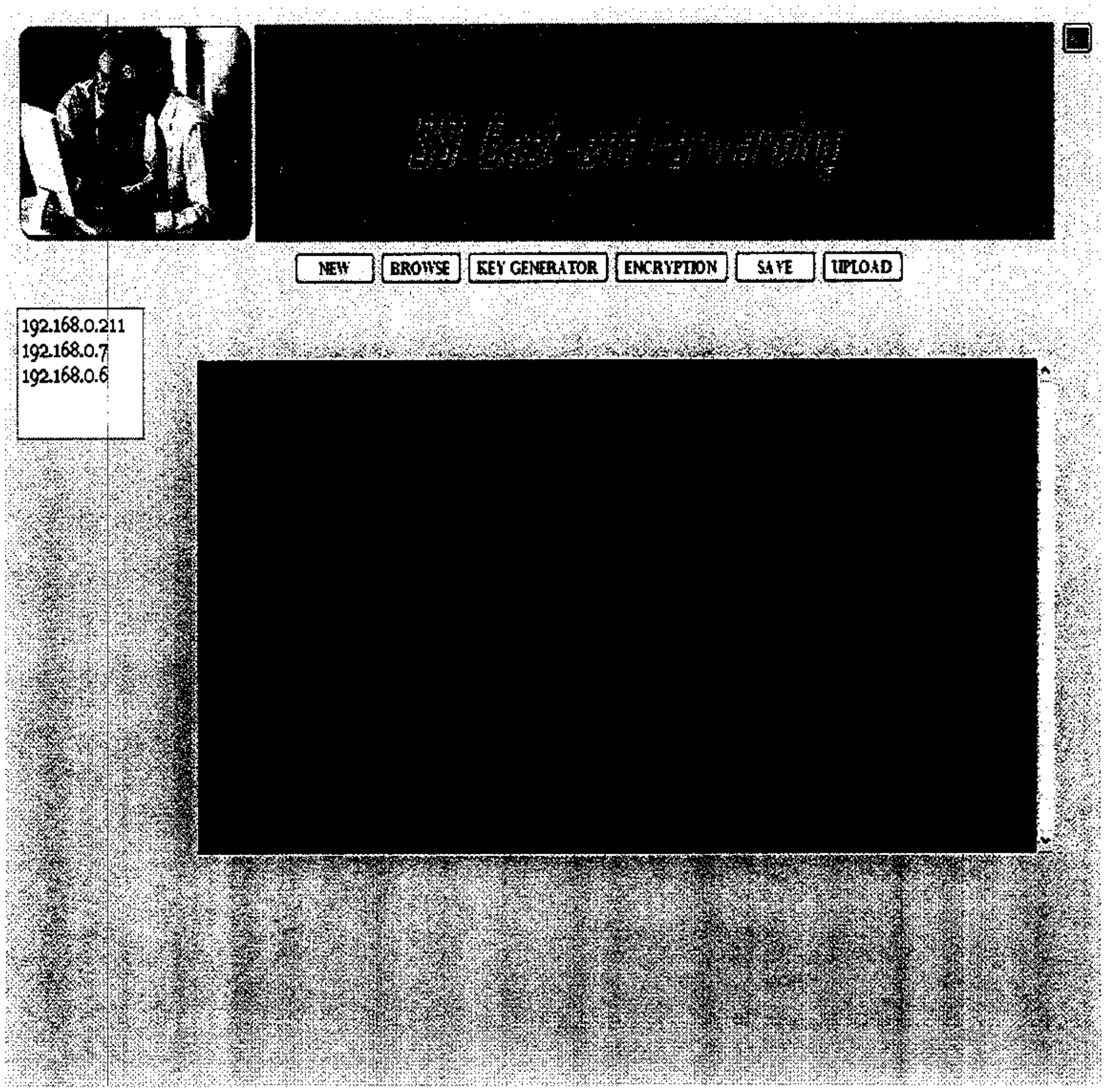
Enter IP Addresses Here

Enter Main Server IP 192.168.0.211 ex 192.0.0.5

Enter Listener-1 IP 192.168.0.7 ex 192.0.0.6

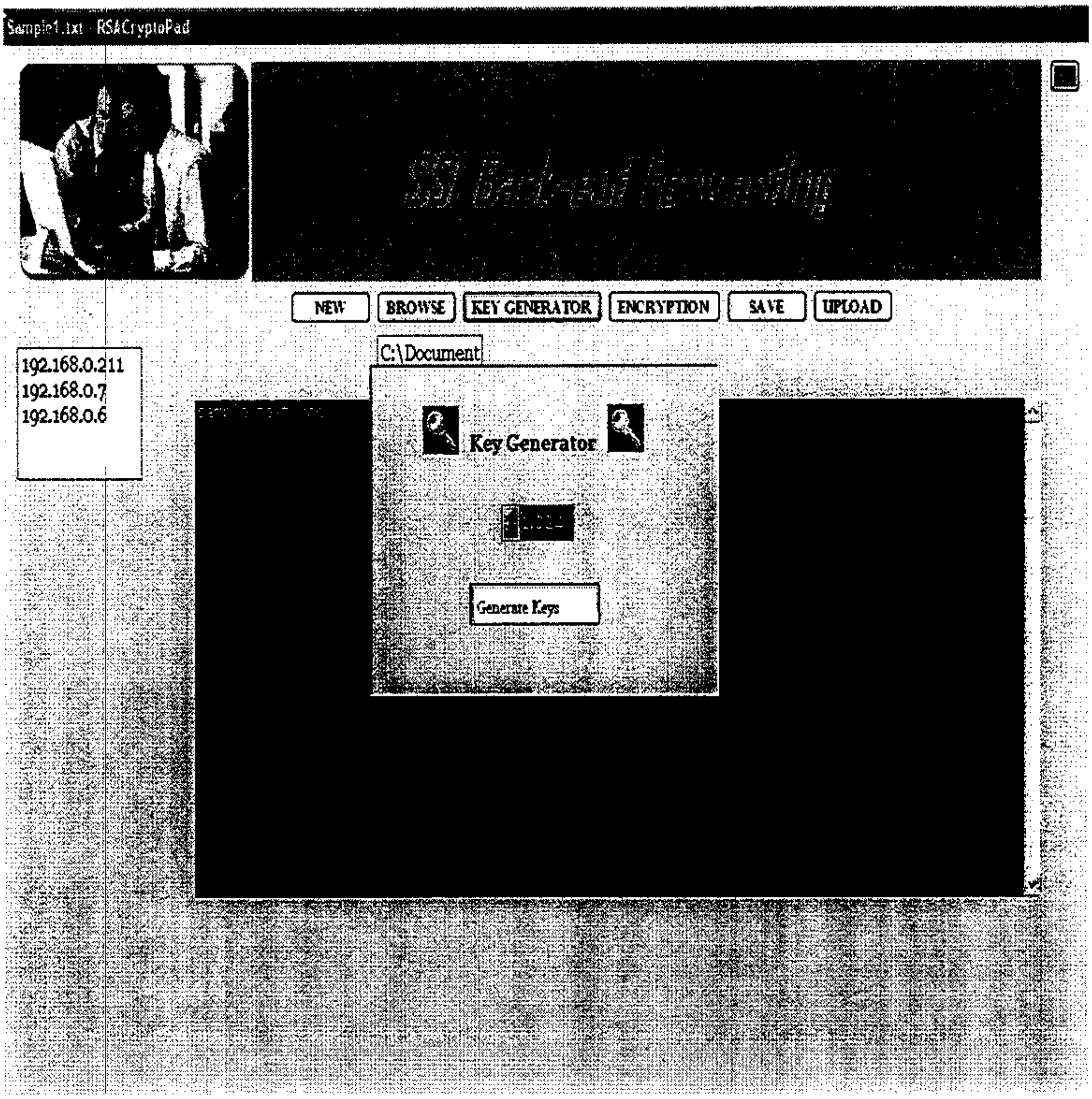
Enter Listener-2 IP 192.168.0.6 ex 192.0.0.7

FILE UPLOAD HOME



192.168.0.211
192.168.0.7
192.168.0.6

KEY GENERATION



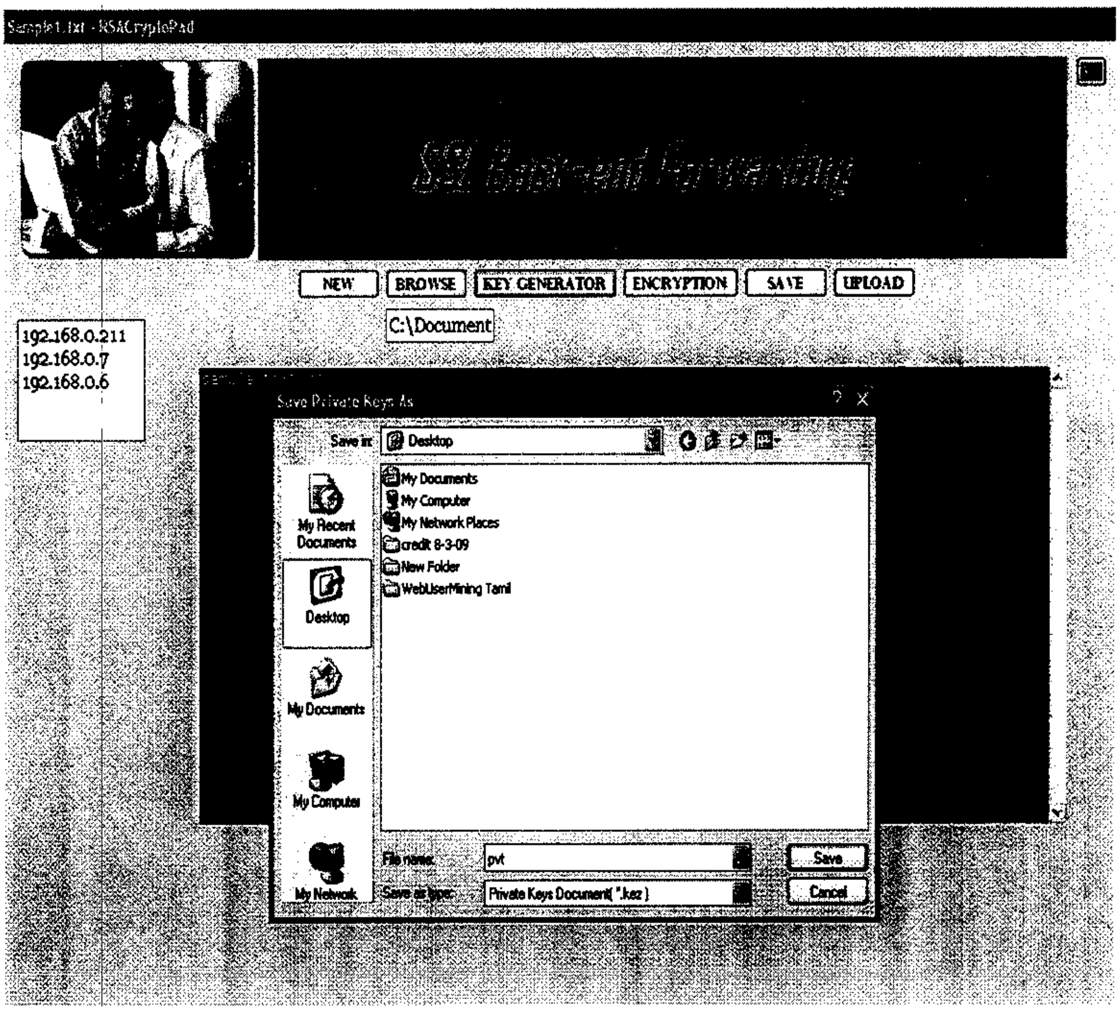
Sample1.txt - RSACryptoPad

192.168.0.211
192.168.0.7
192.168.0.6

C:\Document

1024

PRIVATE KEY



C:\Document

192.168.0.211
192.168.0.7
192.168.0.6

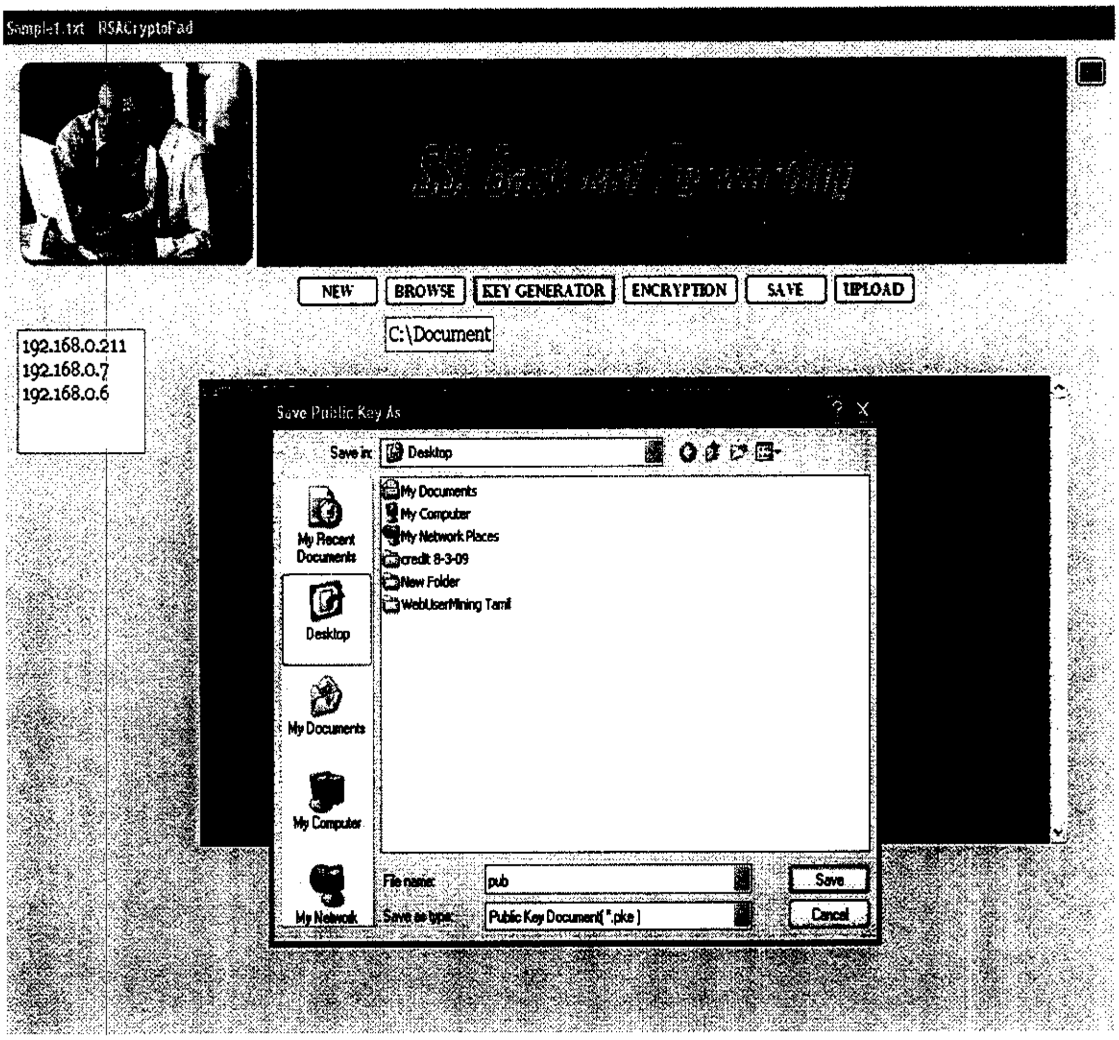
Save in: Desktop

My Documents
My Computer
My Network Places
credit 8-3-09
New Folder
WebUserMining Tamil

File name: pvt

Save as type: Private Keys Document(*.kez)

PUBLIC KEY



Sample1.txt RSACryptoPad

C:\Document

192.168.0.211
192.168.0.7
192.168.0.6

Save Public Key As

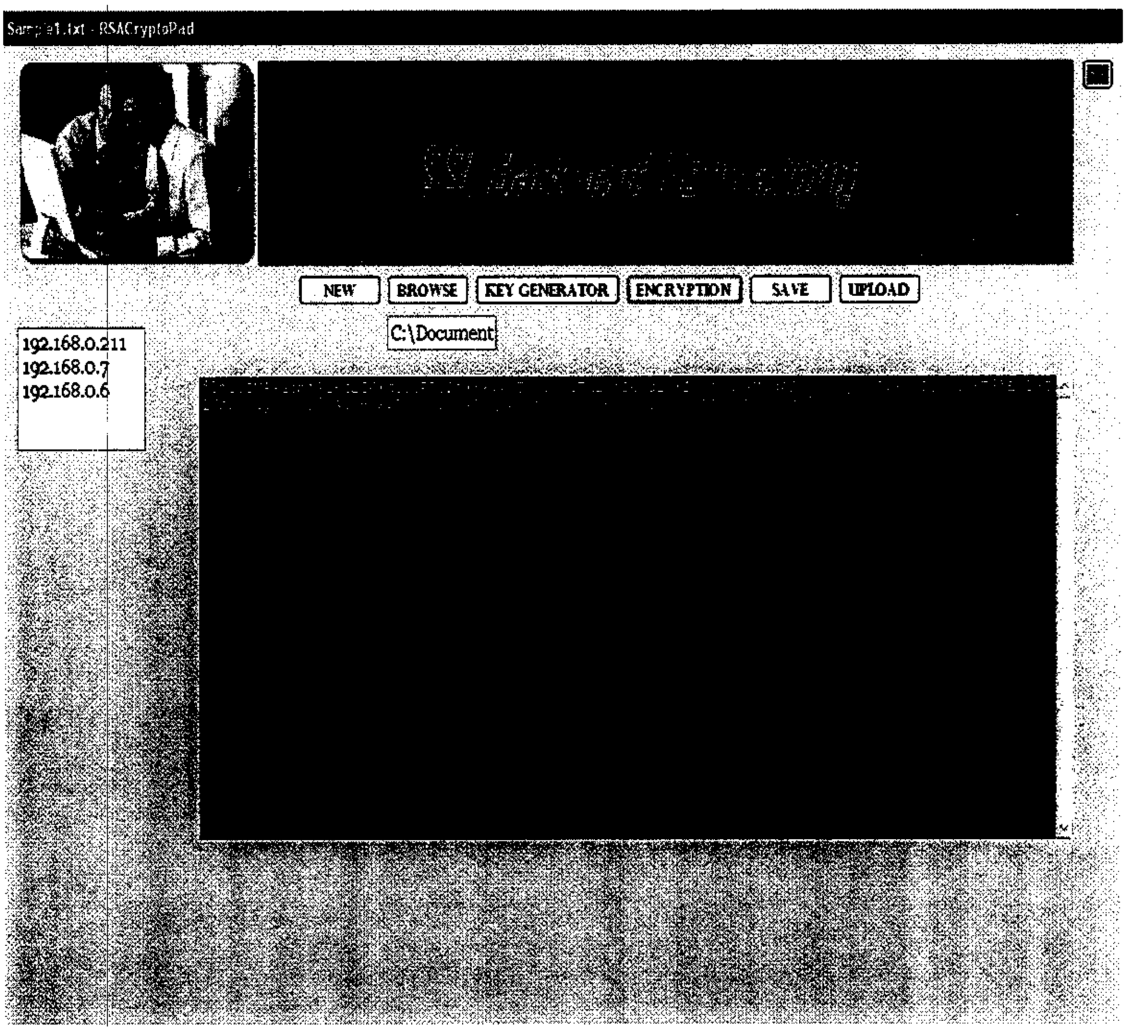
Save in: Desktop

My Documents
My Computer
My Network Places
credit 8-3-09
New Folder
WebUserMining Tamil

File name: pub

Save as type: Public Key Document(*.pke)

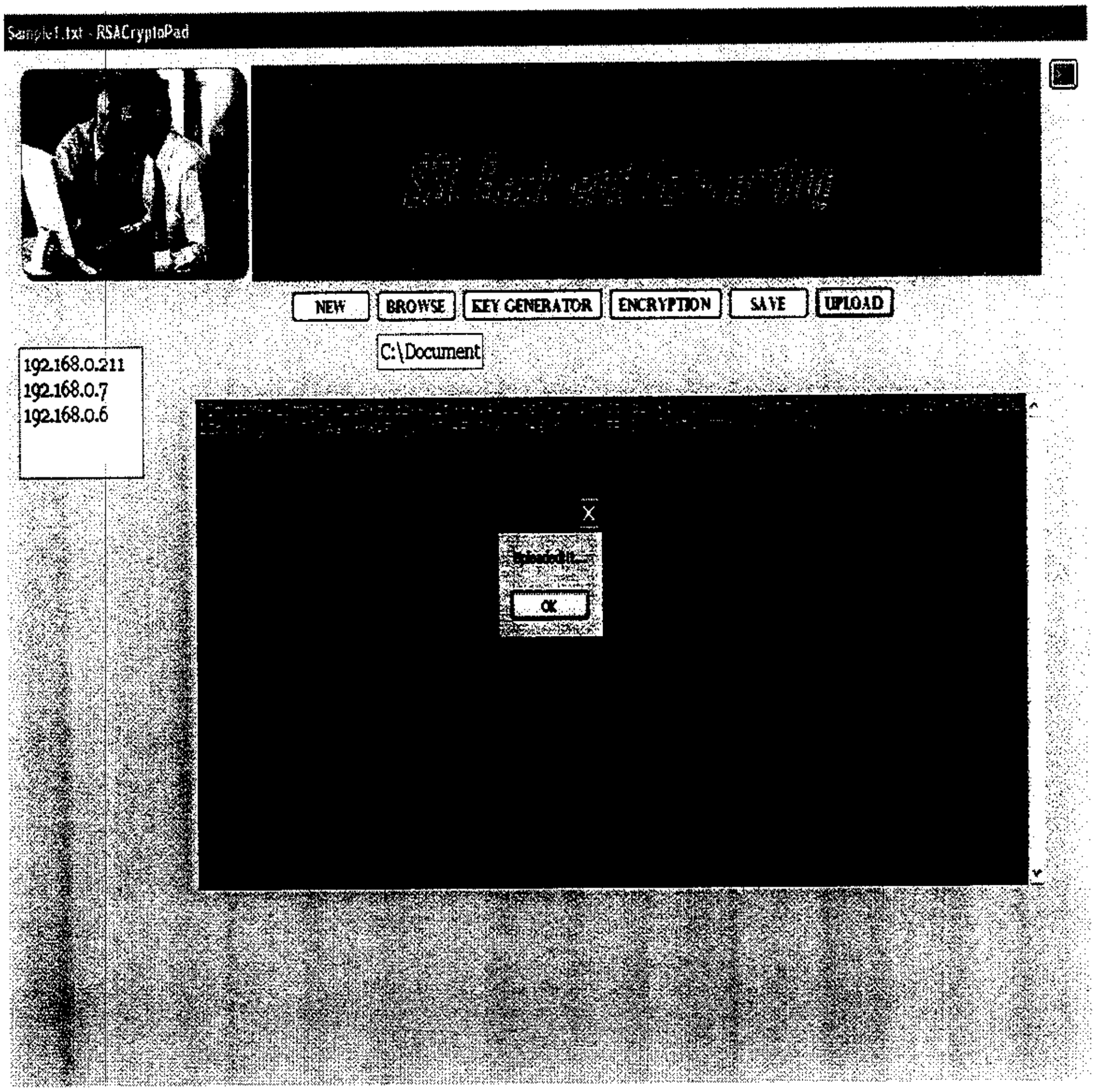
ENCRYPTION



C:\Document

192.168.0.211
192.168.0.7
192.168.0.6

UPLOADING FILE



Sample1.txt - RSACryptoPad

C:\Document

192.168.0.211
192.168.0.7
192.168.0.6

Uploaded It...

REFERENCES

1. S. Abbott, “On the Performance of SSL and an Evolution to Cryptographic Coprocessors,” Proc. RSA Conf., Jan. 1997.

2. M. Andreolini, E. Casalicchio, M. Colajanni, and M. Mambelli, “A Cluster-Based Web System Providing Differentiated and Guaranteed Services,” Cluster Computing, vol. 7, no. 1, pp. 7-19, 2004.

3. Hemlata “**SQL SERVER 2000 REFERENCES**”, First Edition, Cyber-Tech Publications.

4.Herbert Schmidt (2000),**”VIEW ON SQL QUERY ANALYSER**”, Four Edition, Tata McGraw-Hill.

5. M.F. Arlitt and C.L. Williamson, “Internet Web Servers: Workload Characterization and

Performance Implications,” IEEE/ACM Trans. Networking, vol. 5, Oct. 1997.