DEVELOPMENT OF COMPUTER-BASED NETWORK SECURITY THROUGH THE USE OF FIREWALLS IN THE BANKING SYSTEM

BY

AKOLAWOLE TAOFEEQ OLAWALE
ND/23/COM/PT/0078

A PROJECT REPORT SUBMITTED TO THE

DEPARTMENT OF COMPUTER SCIENCE
INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGY, KWARA STATE POLYTECHNIC ILORIN

IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF NATIONAL DIPLOMA (ND) IN COMPUTER SCIENCE

***2025*□**

CERTIFICATION

This is to certify that this project was carried out by **Akolawole Taofeeq Olawale** with Matriculation Number **ND/23/COM/PT/0078** in the department of Computer Science, Institute of Information and Communication Technology, Kwara State Polytechnic, Ilorin.

------------------------------------ ----------------------

MR. ISIAKA, O.S. Date
(Project Supervisor)

-------------------------------- ----------------------

MR. OYEDEPO, F.S. Date
(*Head of Department*)

---------------------------------- ---------------------

External Supervisor Date

□

DEDICATION

This project is dedicated to the creator of the earth and the universe, the Almighty God. It is also dedicated to my parents, Mr. and Mrs. Akolawole of blessed memory.

□

ACKNOWLEDGEMENT

All praise is due to Almighty God, the Lord of the universe. I praise Him and thank Him for giving me the strength and knowledge to complete my HND programme and also for my continued existence on the earth.

I appreciate the utmost effort of my supervisor, **Mr. ISIAKA** whose patience, support and encouragement have been the driving force behind the success of this research work. He gave useful corrections, constructive criticisms, comments, recommendations, advice and always ensures that an excellent research is done. My sincere gratitude goes to Head of the Department **Mr. F. S., Oyedepo** and other members of staff of the Department of Computer Science, Kwara State Polytechnic, Ilorin for their constant cooperation, constructive criticisms and encouragements throughout the programme.

Special gratitude goes to my parents **Mr. and Akolawole** who exhibited immeasurable financial support, patience, support, prayers and understanding during the periods in which I was busy tirelessly working on my studies. Special thanks go to all my lovely siblings.

My sincere appreciation goes to my friends and classmates.

□

TABLE OF CONTENT

CHAPTER 2- LITURATURE REVIEW

CHAPTER 3- METHOLOGY AND ANALYSIS OF THE SYSTEM

CHAPTER 4- DESIGN AND IMPLEMENTATION OF THE SYSTEM

CHAPTER 5-CONCLUSION AND RECOMMENDATION

□

ABSTRACT

The degree of accidence of an organization that provides services to customers, such as banks, is determined by the speed and accuracy of the services performed in the banks, which include information processing, such as data entry. Data uses sorting data, updating data, and service data, among other things, that are better suited to computers. As a result, acquiring the latest business gadgets goes a long way toward keeping you one step ahead of your competitors, and most new banks being established go straight into bank security and computerization of fire walls. Finally, the reality of this project work is described as distributed computing in bank security processing, which is the computerization of bank security and fire wall in banking operations, particularly in the area of wire service operations.

□

CHAPTER ONE

GENERAL INTRODUCTION

1.1 INTRODUCTION

The increased use of computers and other related office equipment is finding increasing application in almost every field of human endeavor, particularly the financial sector. More and more banks are incorporating computer networks into their operations. Because these provide an easy way to access the organization's information and services. According to Akin (1992), computer networking entails collections within a framework of freedom office. They can, for example, work from home at any time. Because information has such a high value, organizations are now classifying their data and putting forth significant effort to protect it.

Networking is a vehicle for sharing information, whereas network security is a method of protecting the information. Information sharing is not limited by physical or geographical location, and today's information is available to all via the global network. Wire banking is a quick way to transfer money electronically from one person to another by using a bank or a nonbank provider such as Western Union or transfer Wise.

To become a part of this global network, an organization must first have its own Local area network (LAN), which is then linked to the internet via a Wide area network (WAN). Computer security focuses on two main issues: how to protect the computer's physical equipment and how to protect against unauthorized use of the computer's faculties by intruders. The goal of network security is to restrict access to corporate and government data stored on network services or transmitted over the LAN or WAN.

In Nigeria, a bank was established with the goal of providing banking services to the general public. Without banks, however, we would have to pay for everything in cash, which we would have to save somewhere. That is obviously dangerous. Servers and borrowers would have to meet in person, and a single transaction between a server and a borrower would be prohibitively expensive. Furthermore, the saver would be taking a significant risk: if the borrower is unable to repay, the saver would lose all of their savings. A bank lends money to a large number of people and businesses. If some borrowers are unable to repay their loans, the bank will absorb the losses, and savers will be unaffected.

1.2 STATEMENT OF THE PROBLEM

Banks in Nigeria must manage a large volume of information in order to evolve efficiently corporate management and improve customer services. The information required to carry out operations geared toward customer satisfaction must be highly secure and properly transmitted. Because banks use computer networks in their operations, there are bound to be security threats that impede work progress in the organization once the organization establishes its presence on the internet.

1.3 AIM AND OBJECTIVES OF THE STUDY

The work aims to define/provide a security system that prevents unauthorized users from accessing the network's protected areas. The project's objectives are as follows:

i. To provide a location for monitoring security for related events

ii. This system will also prevent potentially vulnerable services from entering or leaving the network.

iii. Establishment of a security network backbone for accessing critical information via wired service.

1.4 SIGNIFICANCE OF THE PROJECT

The world has become a global village, sharing everything through networking, and networking is the backbone of accessing vital information. Networks necessitate a high level of security, which includes the technical and administrative safeguards required to protect a computer-based system (hardware, personnel data) from the major hazards to which most computer systems are exposed, as well as to control access to information. Among the benefits are:

a) Network security and fire walls are useful in banking sectors and services.

b) It is beneficial to banks in other sectors that want to use network security and firewalls in their banks.

c) It demonstrates the importance of security in the banking sector.

1.5 SCOPE OF THE STUDY

This study provides an overview of security systems, networks, and firewalls, with a focus on firewalls. Network risks, threats, and vulnerabilities It also focuses on the development of security systems and network types.

1.6 ORGANISATION OF THE REPORT

The first chapter is an introduction to the project. It includes the study's background, a statement of the problem, the project's aim and objectives, the significance of the study, the scope and limitations of the study, the organization of the report, and the definition of technical terms. The second chapter examines some related literature as well as historical context. The third chapter discusses the system's methodology and analysis, research of the existing system, problems with the existing system, description of the proposed system, and advantages of the proposed system. The fourth chapter discusses system design, system output design, system input design, system implementation, programming language selection, and system documentation. The fifth chapter includes a summary, conclusion, and recommendation.

□

CHAPTER TWO

LITERATURE REVIEW

2.1 REVIEW OF THE RELATED PAST WORKS

Data communication, according to Raldlow (1986), is the transmission of digital data between two or more computers, and a computer network or data network is a telecommunications network that allows computers to exchange data. The physical connection between networked computing devices is made via cable media or wireless media. The Internet is the most well-known computer network.

According to Frederick (1999), interest in and knowledge of computer and network security is growing in tandem with the need for it. This interest is undoubtedly due to the Internet's continued expansion and an increase in the number of businesses migrating their sales and information channels to the Internet. There was no Internet at first. There were no networks. There was no e-mail, and people had to rely on postal mail or the telephone to communicate. Telegrams were sent by the extremely busy. Few people used derogatory names to refer to people they'd never met. Of course, the Internet has changed everything. The Internet, which began as the Advanced Research Projects Agency Network (ARPANET), was a small, almost closed community.

2.2 NETWORKING AND COMMUNICATION?

The transmission of digital data between two or more computers is referred to as data communication. The physical connection between networked computing devices is made via cable media or wireless media. The Internet is the most well-known computer network.

2.2.1 TYPES OF COMPUTER NETWORKS

Data in computer networks is transmitted in the form of packets. Packets are involved in everything you do on the Internet. Every Web page, for example, arrives as a series of packets, and every e-mail you send departs as a series of packets. Nodes are the devices that transmit or receive this data, such as a phone or a computer. Networks are classified into three types:

i Local Area Network (LAN): A LAN is a small network that is usually limited to a small geographical area. A LAN, for example, is a computer network that is only accessible to the residents of a building.

ii Wide Area Network (WAN): As the name suggests, these networks cover a wide geographical area. WANs are used to connect LANs and other types of networks so that users and computers in different regions can communicate with one another. The popular and well-known Internet is an example of a WAN.

iii Metropolitan Area Network (MAN): A MAN is a network that connects users to computer resources in a geographical area that is larger than a LAN but not as large as a WAN.

2.2.2 BASIC COMPONENTS OF COMPUTER NETWORK

i Servers: Servers are computers that store shared files, programs, and the network operating system. Servers provide all network users with access to network resources. There are numerous types of servers, and one server can perform multiple functions. File servers, print servers, mail servers, communication servers, database servers, print servers, fax servers, and web servers are just a few examples.

ii Clients - Clients are computers that connect to and use the network and its resources. Client computers are the network's customers (users), as they request and receive services from the servers.

iii Transmission Media - Transmission media are the facilities that allow computers in a network to communicate with one another. Transmission media are also known as channels, links, or lines.

iv Shared data - Shared data are files, printer access programs, and e-mail that file servers provide to clients.

v Shared printers and other peripherals - Shared printers and peripherals are hardware resources that servers make available to network users. Data files, printers, software, and any other items used by network clients are examples of resources provided.

vi Network Interface Card - Each computer in a network has a network interface card, which is a type of expansion card (NIC). The network interface card (NIC) prepares (formats) and sends data, receives data, and controls data flow between the computer and the network. On the transmit side, the NIC sends data frames to the physical layer, which sends the data to the physical link. The NIC on the receiver's side processes bits received from the physical layer and the message based on its contents.

vii Local Operating System - A local operating system allows personal computers to access files, print to a local printer, and have and use one or more on-board disk and CD drives.

viii Network Operating System - A network operating system is a program that runs on computers and servers and allows them to communicate with one another over a network.

ix Hub - A hub is a device that divides a network connection among several computers. It's similar to a distribution center. When a computer requests information from a network or a specific computer, the request is routed through a cable to the hub. The hub will receive the request and forward it to the rest of the network. Each computer in the network should then determine whether or not the broadcast data is for them.

x Switch - A switch is a type of telecommunications device that is classified as a computer network component. It uses physical device addresses in each incoming message to ensure that the message is delivered to the correct destination or port.

2.3 CONCEPT OF A FIREWALL

A firewall intercepts and controls traffic between networks that have varying degrees of trust. It is part of an organization's network perimeter defense and should enforce a network security policy. It provides an audit trail, according to Cheswick and Bellovin's definition. A firewall is an excellent place to support both strong user authentication and private or confidential communications between firewalls. Firewalls, as Chapman and Zwicky pointed out, are an excellent place to focus security decisions and enforce a network security policy. They can efficiently log internetwork activity and limit an organization's exposure. The "zone of risk" refers to the vulnerability to attack. If an organization connects to the Internet without a firewall (Figure 2.1), any host on the private network can access any resource on the Internet directly. To put it another way, every host on the Internet can attack every host on the private network. It is preferable to reduce the risk zone. Risk zone can be limited by using an internetwork firewall (Figure 2.2).

2.3.1 TYPES OF FIREWALL

Internet firewalls are classified into four types, or three types plus a hybrid. The specifics of these various types are not covered in this section because they are well covered in the literature.

i **Packet Filtering:** A packet filtering firewall is one type of firewall. Filtering firewalls examine packets using addresses and packet options. They operate at the IP packet level and make security decisions based on packet headers (really, "to forward or not to forward this packet, that is the question"). There are three types of filtering firewalls:

a) Static Filtering, which most routers use—filter rules that must be changed manually

b) Dynamic Filtering, in which an outside process changes the filtering rules dynamically based on router-observed events (for example, one might allow FTP packets in from the outside, if someone on the inside requested an FTP session)

c) Stateful Inspection, a technology similar to dynamic filtering but with a more granular examination of data contained in IP packets.

ii **Circuit Gateways:** Circuit gateways are network transport layer devices. Connections are once again authorized based on addresses. They, like filtering gateways, cannot (usually) examine data traffic flowing between networks, but they can prevent direct connections between networks.

iii **Application Gateways:** Application gateways, also known as proxy-based firewalls, operate at the application level and can examine data at the application data level. (We can think of this as the contents of the packets, though proxies do not operate with packets strictly speaking.) They can make decisions based on application data, such as FTP commands or URLs passed to HTTP. Application gateways are said to "break the client/server model."

iv **Hybrids:** Hybrid firewalls, as the name implies, combine elements from multiple types of firewalls. Hybrid firewalls are not a new concept. DEC SEAL, the first commercial firewall, was a hybrid that used proxies on a bastion host (a fortified machine labeled "Gatekeeper" in Figure 1) and packet filtering on the gateway machine ("Gate"). Hybrid systems are frequently built in order to quickly add new services to an existing firewall. Because each new service requires new proxy code, it is possible to add a circuit gateway or packet filtering to an application gateway firewall. Alternatively, proxies for the service or services could be used to add strong user authentication to a stateful packet filter.

CHAPTER THREE

METHODOLOGY AND ANALYSIS OF THE EXISTING SYSTEM

3.1 RESEARCH METHODOLOGY

This project's materials were gathered from the internet, textbooks, and personal interviews. This technique was used to enable the use of nonverbal information.

3.2 ANALYZING OF THE EXISTING SYSTEM

Unsecure methods of gathering customer data and transactions in the banking sector have been a major source of concern. This unsecured process had linked many banks' databases, particularly those dealing with wire service operations, which deal with the transfer of funds from one bank to another, either within the country or on an international level. However, unsecured network operations may result in a loss of trust and reliance between banks and their customers.

3.3 PROBLEM OF THE EXIXTING SYSTEM

The existing banking system, which lacks adequate security, has resulted in a slew of issues in the banking sector, including:

i. Loss of vital and important documents to fraudsters

ii. When large sums of money are involved, the bank's reputation may be jeopardized, and customers' trust in the bank may be shaken, potentially leading to a large number of customers withdrawing.

iii. It has a negative impact on the morale of other employees, especially when fraud goes undetected.

iv. Unchecked fraudulent practices are not only capable of destroying a whole bank, but can also destroy a nation's economy. v Other effects of fraud include the distraction of management's attention, an increase in operating costs, and the waste of time and resources spent on fraud prevention.

v. Bank fraud results in financial losses, which obviously reduces the industry's profit base.

3.4 DESCRIPTION OF THE PROPOSED SYSTEM

The researcher specifies which system will be used in implementation in the system proposal. To ensure adequate data security, security programs must also be written. Because some level of separation between an organization's internal network and the internet must be provided, the firewall approach is used. All information attacks are carried out via legal or illegal hardware interfaces connected to the network or the communication system used by the network. Fibre optics should be used in applications requiring high security due to their lack of emission, which makes them extremely difficult, if not impossible, to tap.

Because a firewall cannot function in isolation, the organization's security policy must be defined. This is in terms of the level of security and the data / information that needs to be safeguarded. A research investigation is an investigation undertaken to discover facts, obtain additional information, and so on through the planned and systematic collection, analysis, and interpretation of data. Methodology, on the other hand, refers to a structured approach to a specific job, such as system analysis and design. As a result, narrow your search to a specific job, such as system analysis and design. Thus, research methodology is the planned and systematic collection, analysis, and interpretation of data in order to arrive at a reliable solution to problems. It is also comprehensive. The primary source came from Diamond Bank Nigeria Ltd, where the bank's assistance with this project paid off.

3.5 ADVANTAGES OF THE PROPOSED SYSTEM

Firewalls have been used to deter network-related crimes due to threats to the confidentiality and integrity of sensitive data. However, the following are some of the benefits of the proposed system:

i Network security with a firewall aids in the protection of personal data of customers and employees on the network.

ii Network Security enables the protection of information shared on the network by customers and staff.

iii Network Security provides various levels of access. If several computers are connected to a network, some may have greater access to information than others.

iv By disconnecting private networks from the internet, they can be protected from external attacks. Network security protects them from virus attacks, for example.

CHAPTER FOUR

DESIGN AND IMPLEMENTATION OF THE SYSTEM

4.1 DESIGN OF THE SYSTEM

The implementation process is the process of putting theory into practice, i.e. the security system must be designed, and the system must access potential threats in order of importance. The significance of the threat must be defined by the security designer, and this must include a careful examination of the network system risk specifications. Threats and vulnerabilities should be investigated in order to fully understand the network's requirements.

4.1.1 OUTPUT SYSTEM

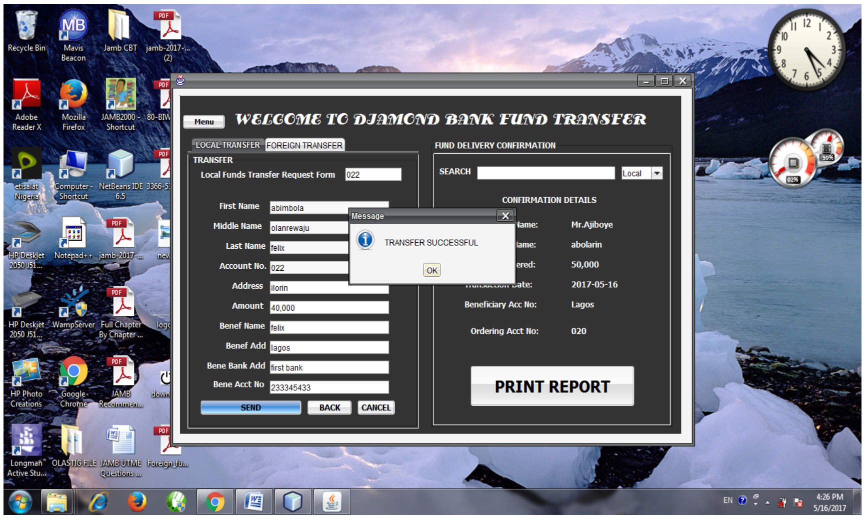
Forms are also part of the output design. The form includes the customer's personal information, a statement of account, a daily transaction list, and a transaction report.

a. Customers personal data: This file includes the fields branch name, transaction type, address, postal address, occupation data of account opening, postal address, occupation, date of account opening, hometown, town of residence, referees name and address, and secret code.

b. Customer’s statement of account: The following fields are included in this output: secret code, customer name and address, transaction type date, amount deposited, amount withdrawn and balance, frequency. At the end of each month, the bank generates this report and posts it to the customer's account for both saving and current transactions.

c. Banks daily transaction list: This file contains the following information: the branch, the secret code, the transaction type, the amount withdrawn, and the amount deposited. At the end of each day, the transaction list is displayed or printed so that the accountant can see the total amount withdrawn and total amount deposited. This aids in the balancing of the bank account.

d. Customer's transaction report: It contains the transaction type, the transaction amount, the data, the time, and the secret code.



TRANSFER

Local Funds Transfer Request Form: 022

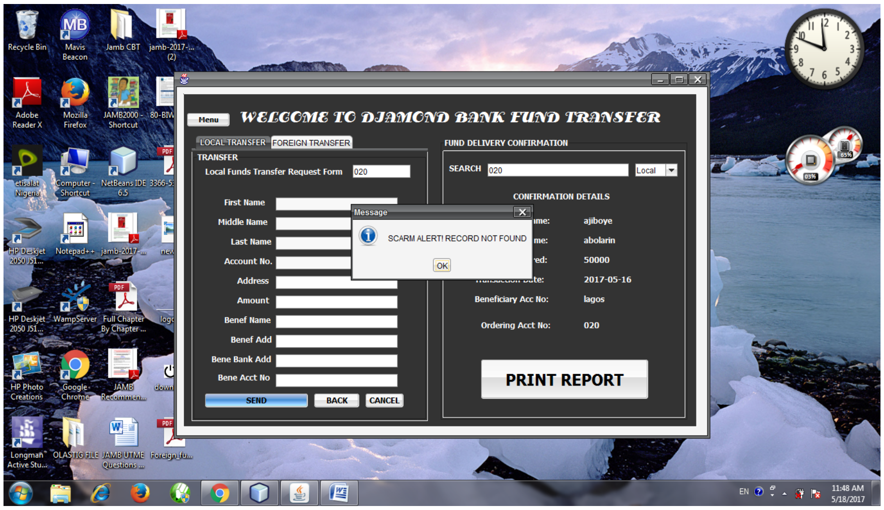
First Name: abimbola
Middle Name: olanrewaju
Last Name: felix
Account No.: 022
Address: ilorin
Amount: 40,000
Benef Name: felix
Benef Add: lagos
Bene Bank Add: first bank
Bene Acct No: 233345433

Message: TRANSFER SUCCESSFUL

SEARCH: Local

Mr.Ajiboye
abolarin
50,000
2017-05-16
Beneficiary Acc No: Lagos
Ordering Acct No: 020

Figure 4.1: Transaction Successful splash screen



TRANSFER

Local Funds Transfer Request Form: 020

First Name:
Middle Name:
Last Name:
Account No.:
Address:
Amount:
Benef Name:
Benef Add:
Bene Bank Add:
Bene Acct No:

Message: SCARM ALERT! RECORD NOT FOUND

SEARCH: 020 Local

ajiboye
abolarin
50000
2017-05-16
Beneficiary Acc No: lagos
Ordering Acct No: 020

Figure 4.2: Record no found splash screen

4.1.2 INPUT SYSTEM

The expected output will have a significant impact on the input consideration. The input design specifies the input data required to generate the required reports, including data extraction methods, data transaction and data preparation coding techniques, verification, and correction.

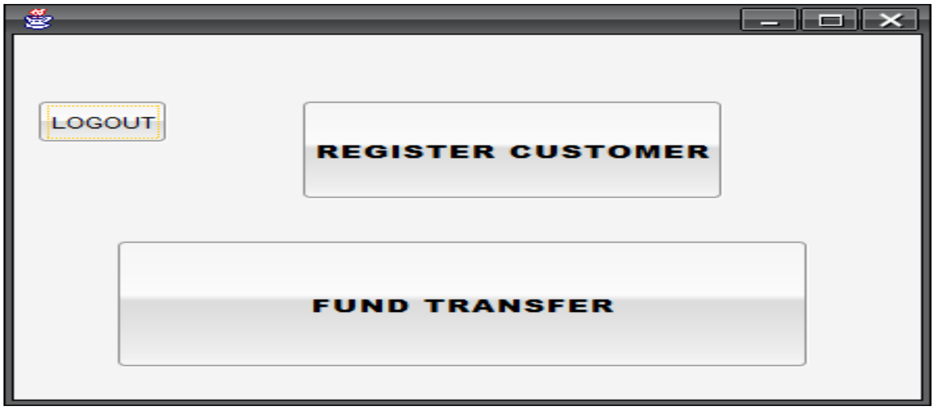


Figure 4.3: Options page

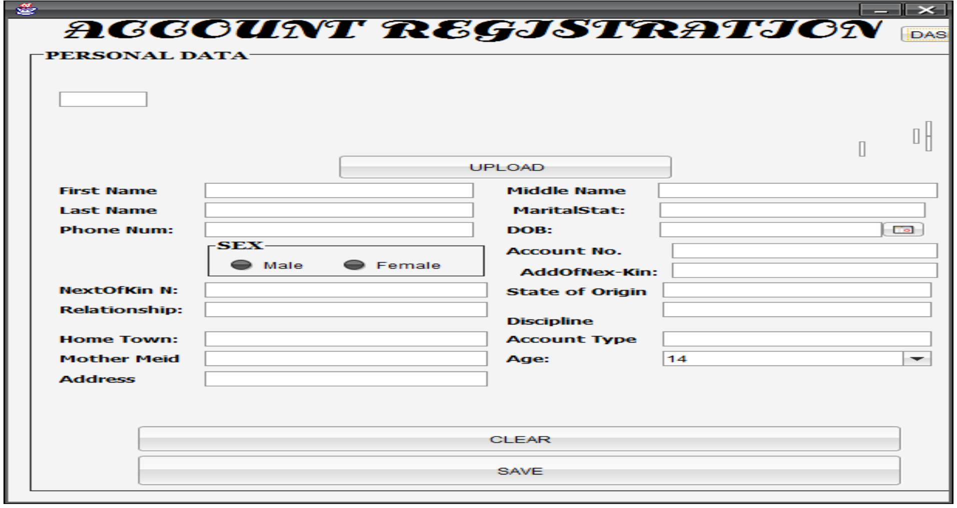


Figure 4.4: Customer Registration page

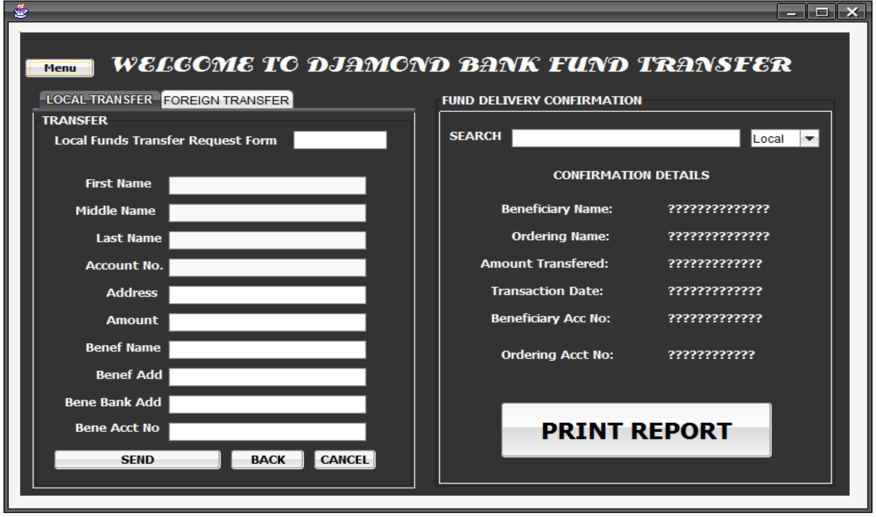


Figure 4.5: Foreign Transaction page

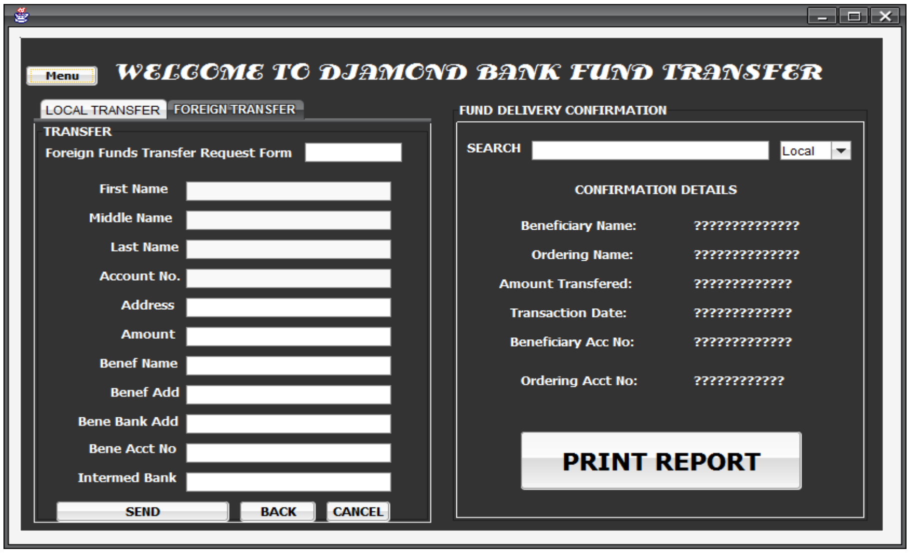
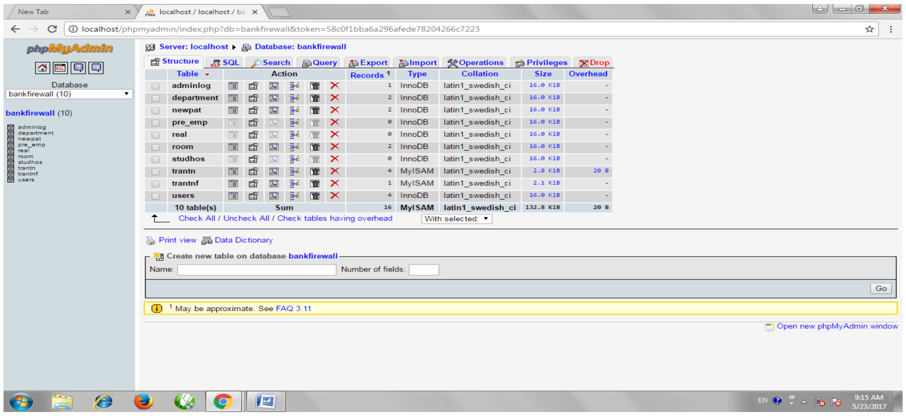


Figure 4.6: Local Transaction page

4.1.3 DATABASE DESIGN

During the early stages of architecture, it is critical to determine what the user requirements are and to create a table that is compatible with the requirements. For network security in the banking system, a database will be built using the entire source provided and the benefits obtained from PhpMyAdmin.


New Tab
localhost / localhost / ba
localhost/phpmyadmin/index.php?db=bankfirewall&token=58c0f1bba6a296afede78204266c7223
phpMyAdmin
Structure
SQL
Search
Query
Export
Import
Operations
Privileges
Drop
Print view
Data Dictionary
Go
Open new phpMyAdmin window
EN
9:15 AM
5/23/2017

Database: bankfirewall (10)

bankfirewall (10)

adminlog
department
newpat
pre_emp
real
room
studhos
trantn
trantnf
users

Server: localhost ▸ Database: bankfirewall

	Table	Action	Records [1]	Type	Collation	Size	Overhead
□	adminlog		1	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	department		2	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	newpat		2	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	pre_emp		0	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	real		0	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	room		2	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	studhos		0	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	trantn		4	MyISAM	latin1_swedish_ci	2.8 KiB	20 B
□	trantnf		1	MyISAM	latin1_swedish_ci	2.1 KiB	-
□	users		4	InnoDB	latin1_swedish_ci	16.0 KiB	-
	10 table(s)	Sum	16	MyISAM	latin1_swedish_ci	132.8 KiB	20 B

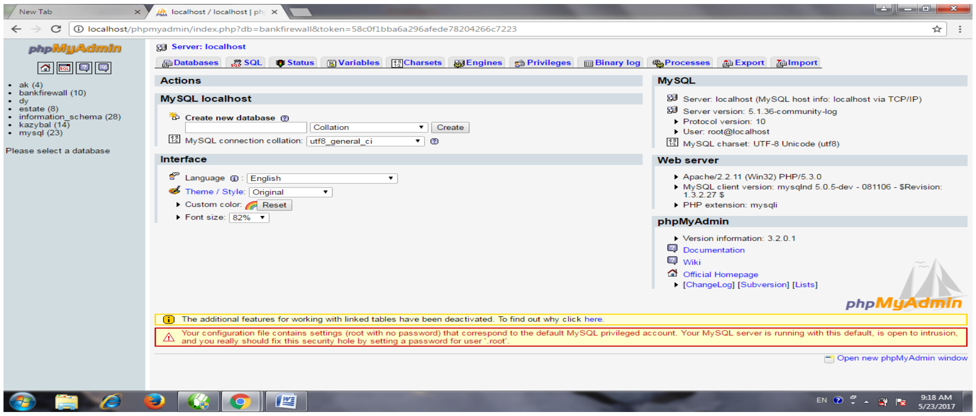
Check All / Uncheck All / Check tables having overhead With selected: ▾

Create new table on database bankfirewall

Name: Number of fields:

[1] May be approximate. See FAQ 3.11

Figure 4.8: Database



- ak (4)
- bankfirewall (10)
- dy
- estate (8)
- information_schema (28)
- kazybal (14)
- mysql (23)

Please select a database

Actions

MySQL localhost

Create new database Collation

MySQL connection collation: utf8_general_ci

Interface

Language: English

Theme / Style: Original

Custom color:

Font size: 82%

MySQL

Server: localhost (MySQL host info: localhost via TCP/IP)
Server version: 5.1.36-community-log
Protocol version: 10
User: root@localhost
MySQL charset: UTF-8 Unicode (utf8)

Web server

Apache/2.2.11 (Win32) PHP/5.3.0
MySQL client version: mysqlnd 5.0.5-dev - 081106 - $Revision: 1.3.2.27 $
PHP extension: mysqli

phpMyAdmin

Version information: 3.2.0.1

The additional features for working with linked tables have been deactivated. To find out why click here.

Your configuration file contains settings (root with no password) that correspond to the default MySQL privileged account. Your MySQL server is running with this default, is open to intrusion, and you really should fix this security hole by setting a password for user '.root'.

Figure 4.9: Database

4.1.4 PROCEDURE DESIGN

This is the bank's responsibility in terms of protecting its network resources. They are as follows:

a. Sensitive or confidential data should never be sent over the internet or network unless it is encrypted. Passwords and logo 10s are examples of sensitive data.

b. To determine where firewalls should be installed, the company should conduct a risk assessment. The firewall should be configured to allow outgoing internet access while strictly limiting incoming user access to the data/system.

c. No computer containing sensitive information should be allowed to connect to the internet unless it is protected by a firewall or other means.

d. Avoid using e-mail gateway commands, which crackers can use to probe for the user's address.

e. Remove compilers, editors, and other program development tools that could allow a cracker to install Trojan horse software or backdoors from the system(s).

f. Once downloaded into the system, all software available on the network must be scanned for computer viruses or Trojan horses.

g. All downloaded software should be loaded into flash drills rather than the hard disk. Before being installed on the land hard drive, the software will be scanned for Trojan horses and computer viruses.

h. Do not allow 100pholes in firewall systems to allow user-friendly systems or special entrance access.

i. Violations of standards, procedures, or practice will be brought to the management's attention for disciplinary action, including termination of appointment users should be made aware of the scope and limitations of their work.

4.2 IMPLEMENTATION OF THE SYSTEM

Because network security encompasses all types of business operations in the banking sector, defining the activities of different sections of the bank would be difficult. As a result, the program's goal is to use passwords to secure dates and files in the banking environment. For example, if a specific number of incorrect passwords are entered, the program quickly generates an error report and transfers control to a different part of the program. So, in order for this program to be fully implemented, banks must provide system analysis with the necessary information and activity requirements. This would aid in fully protecting their networks from cyber-attacks.

4.2.1 **CHOICE OF PROGRAMMING LANGUAGE**

The language used for system implementation/development is Web-based e-photo album for computer Science, and only a few tools have been used:

i. Language: JAVAIDE

ii. Database: MYSQL and PhpMyAdmin

iii. Application: Adobe Dreamweaver

iv. Web Server: XAMPP

4.2.2 HARDWARE SUPPORT

The hardware and software components of a computer system are broadly classified. The physical component of a computer system or computer peripherals is referred to as hardware. The developed web-based application cannot, of course, function in isolation. A variety of computer peripherals are required for the developed software to function properly. The following hardware components are required:

i A complete computer system

ii A minimum of 1.2GHz processor

iii 70MB of Available Hard Disk Space or more

iv At least 512MB of Random Access Memory (RAM)

v Mouse and Enhanced Keyboard

vi Printer e.g. laser jet

4.2.3 SOFTWARE SUPPORT

The term "software" refers to a collection of programs that are a set of instructions given to a computer to perform a specific task. The developed software can be either system software or application software; however, the developed software requires the assistance of other system software to run properly. The following software requirements are required for the proposed system to function properly:

i Microsoft Windows XP/VISTA/7

ii .net framework environment

iii .net framework 4.0

iv Microsoft SQL Server

4.2.4 CHANGE OVER TECHNIQUES

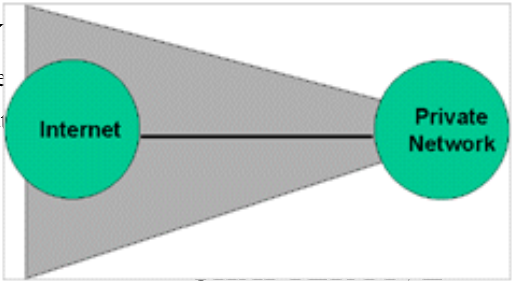
The method of changeover used for this work is parallel changeover, in which the old and new systems are both running at the same time with the same input. The outputs are compared, and any discrepancies are resolved, until the new system is proven to be satisfactory. The old system is disconnected at this point, and the new system takes its place.

4.3 SYSTEM DOCUMENTATION

Documentation was used as a process throughout the system development. The documentation ensures that the process involved in the development of the system, the system's content, the operational procedure, and the software's maintenance are communicated to the user in a concise manner. A well-documented system will guide the user through the process of installing the software.

4.3.1 DOCUMENTATION OF THE PROGRAM

Programming was defined as any sequence of operations required to achieve the desired results in any given computing task. It necessitates an understanding of the nature of computer programs as well as the programming language used to express problems. The program used here is the java programming language, which employs an interpreter to load and execute compliments on the java editor. Although the program does not include bank computations, a security policy has been implemented and tested against certain conditions that were raised during the program's execution.



4.3.2 MAI

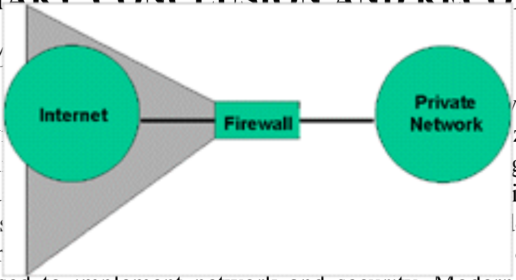
i Keeping the syste … system are not corrupted

ii Having up-to-da

□

Figure 2.1: Zone of Risk with a Firewall

SUMMARY CONCLUSION AND RECOMMENDATION



5.1 SUM

Based on … walls, it is clear that this topic encompasses a w … zations in order to protect their data and the envi … g cash and issuing bank drafts, transferring fund … ining accounts, and providing facilities for the … leeds. Local, metropolitan, and wide area networ … can connect. Several pieces of equipment are used to implement network and security. Moderns, multiplexors, magnetic link character recognition (MICR), and printers are examples of physical equipment used in the network and security implementation. To control the network's operations, software programs must be written.

Figure 2.2: Limit the Zone of Risk with a Firewall

5.2 CONCLUSION

After studying the use of computer network security and firewalls in a modern bank, highlighting the benefits and drawbacks of networks, it would be appropriate to suggest to other banks that they provide a better means of protecting their network. It's worth noting that most banks are already computerized, implying that the enabling platform for implementing the network already exists. However, before embarking on the project, a more detailed study should be commissioned and carried out. The study, which should be carried out by an expert network analyst, will allow the bank to decide on the best topology software, hardware, and network facilities to implement.

5.3 RECOMMENDATION

Looking at the types of attacks that are common in network environments, we can derive a relatively short list of high-level practices that can help prevent security disasters and mitigate damage in the event of a successful attack.

i Data Backup: Although it is not a very secure approach, banks should try to provide as many duplicate dates and information as possible. The backup policy should be dictated by operational requirements, and it should be closely coordinated with a disaster recovery plan: if one point fails, one can easily switch to another method of performing that particular operation without having to wait for the system to be repaired.

ii Avoid system with single point of failure: Any security that can be breached by breaking through any component is not particularly strong. A degree of redundancy in security is beneficial and can help to protect the organization from a minor security breach turning into a catastrophe.

□

REFERENCES

Abdullah J.I (2004). Introduction to the computer management tool. The motivation of the software is to eliminate the manual procedures

Ani C.O (2003). Programming with visual Microsoft basic computer studies for BTEC (2nd edition)

Andress, J. (2014). The Basics of Information Security.

Conway, R. (2004). Code Hacking: A Developer's Guide to Network Security. Developer's Guide to Network Security provides a hands-on approach to learning the vital security skills.

Chang, R. (2002). Defending Against Flooding-Based Distributed

Sawyer P. (1999). Using information technology 13th edition. A Practical Introduction to Computers & Communications. Brief Version

Vacca, R. (2009). Computer and information security handbook. Amsterdam: Elsevier.

Fredeck A. (1999). Firewalls and internet. Interest and knowledge about computer and network security is growing along with the need for it.

Oppliger, R. (1997). Internet Security: Firewalls and Beyond. Communications

FLOWCHARTS

FLOWCHART OF THE PROPOSED SYSTEM

TRANSFER FUND FLOWCHART

TRANSACTION RECORDS FLOWCHART

TRANSACTION TYPE FLOWCHART

PROGRAMME SOURCE CODE

```
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.KeyEvent;
import java.awt.event.WindowEvent;
import java.net.InetSocketAddress;
import java.net.Socket;
import java.util.Calendar;
import java.util.GregorianCalendar;
import java.util.logging.Level;
import java.util.logging.Logger;
import javax.swing.JButton;
import javax.swing.JOptionPane;
import javax.swing.UIManager;


/**
*
* @author OLASTIG2
*/
public class login extends db{
  /** Creates new form login */
  public login() {
     initComponents();
     dynamicdate();
     currentdate();
  }
        public void dynamicdate(){
   Calendar cal = new GregorianCalendar();
  int month = cal.get(Calendar.MONTH);
  int year = cal.get(Calendar.YEAR);
  int day = cal.get(Calendar.DAY_OF_MONTH);
  txt_date.setText(day+"/"+(month+1)+"/"+year);
   int second = cal.get(Calendar.SECOND);
  int minute = cal.get(Calendar.MINUTE);
  int hour = cal.get(Calendar.HOUR);
  txt_time.setText(hour+":"+(minute)+":"+second);
  Thread clock =new Thread() {
  public void run(){
    for(;;){
  Calendar cal = new GregorianCalendar();
  int month = cal.get(Calendar.MONTH);
        jButton1ActionPerformed(evt);
      }
    jLabel7.setText("ABOLARIN EMMANUEL ABIODUN");
    javax.swing.GroupLayout jPanel1Layout = new javax.swing.GroupLayout(jPanel1);
    jPanel1.setLayout(jPanel1Layout);
    jPanel1Layout.setHorizontalGroup(
      jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
      .addGroup(jPanel1Layout.createSequentialGroup()
        .addContainerGap()
        .addGroup(jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING, false)
          .addComponent(jLabel3, 0, 0, Short.MAX_VALUE)
          .addGroup(jPanel1Layout.createSequentialGroup()
            .addComponent(jLabel4)
            .addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.UNRELATED)
            .addComponent(txt_date, javax.swing.GroupLayout.PREFERRED_SIZE, 70,
javax.swing.GroupLayout.PREFERRED_SIZE)
            .addGap(18, 18, 18)
            .addComponent(jLabel6)
            .addGap(18, 18, 18)
            .addComponent(txt_time, javax.swing.GroupLayout.PREFERRED_SIZE, 62,
javax.swing.GroupLayout.PREFERRED_SIZE))
          .addComponent(jLabel7))
        .addGap(16, 16, 16)
        .addGroup(jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
          .addComponent(pa, javax.swing.GroupLayout.DEFAULT_SIZE, 209, Short.MAX_VALUE)
          .addComponent(jLabel2, javax.swing.GroupLayout.PREFERRED_SIZE, 112,
javax.swing.GroupLayout.PREFERRED_SIZE)
          .addComponent(jButton1, javax.swing.GroupLayout.DEFAULT_SIZE, 209, Short.MAX_VALUE)
          .addComponent(jButton2)
          .addComponent(combo, 0, 209, Short.MAX_VALUE)
          .addComponent(u, javax.swing.GroupLayout.Alignment.TRAILING,
javax.swing.GroupLayout.DEFAULT_SIZE, 209, Short.MAX_VALUE)
          .addComponent(jLabel5, javax.swing.GroupLayout.Alignment.TRAILING)
          .addComponent(jLabel1, javax.swing.GroupLayout.PREFERRED_SIZE, 78,
javax.swing.GroupLayout.PREFERRED_SIZE))
        .addContainerGap())
    );
    jPanel1Layout.setVerticalGroup(
      jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
      .addGroup(jPanel1Layout.createSequentialGroup()
        .addGroup(jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment.BASELINE)
          .addComponent(jLabel4)
          .addComponent(txt_date)
          .addComponent(txt_time)
          .addComponent(jLabel6)
          .addComponent(jLabel5))
        .addGroup(jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
          .addGroup(jPanel1Layout.createSequentialGroup()
            .addGap(22, 22, 22)
            .addComponent(jLabel1))
          .addGroup(jPanel1Layout.createSequentialGroup()
            .addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED)
            .addComponent(jLabel7)))
        .addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED)
        .addGroup(jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
          .addGroup(jPanel1Layout.createSequentialGroup()
            .addComponent(u, javax.swing.GroupLayout.PREFERRED_SIZE, 26,
javax.swing.GroupLayout.PREFERRED_SIZE)
```

```
                .addGap(23, 23, 23)
                .addComponent(jLabel2)
                .addGap(18, 18, 18)
                .addComponent(pa, javax.swing.GroupLayout.PREFERRED_SIZE, 24,
javax.swing.GroupLayout.PREFERRED_SIZE)
                .addGap(18, 18, 18)
                .addComponent(jButton1, javax.swing.GroupLayout.PREFERRED_SIZE, 38,
javax.swing.GroupLayout.PREFERRED_SIZE)
                .addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED)
                .addComponent(combo, javax.swing.GroupLayout.PREFERRED_SIZE,
javax.swing.GroupLayout.DEFAULT_SIZE, javax.swing.GroupLayout.PREFERRED_SIZE)
                .addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED,
javax.swing.GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE)
                .addComponent(jButton2, javax.swing.GroupLayout.PREFERRED_SIZE, 33,
javax.swing.GroupLayout.PREFERRED_SIZE))
              .addComponent(jLabel3, javax.swing.GroupLayout.PREFERRED_SIZE, 217,
javax.swing.GroupLayout.PREFERRED_SIZE))
            .addGap(25, 25, 25))
      );
      txt_date.getAccessibleContext().setAccessibleParent(this);
      javax.swing.GroupLayout layout = new javax.swing.GroupLayout(getContentPane());
      getContentPane().setLayout(layout);
      layout.setHorizontalGroup(
        layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
        .addGroup(layout.createSequentialGroup()
            .addContainerGap()
            .addComponent(jPanel1, javax.swing.GroupLayout.DEFAULT_SIZE,
javax.swing.GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE)
            .addContainerGap())
      );
      layout.setVerticalGroup(
        layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
        .addGroup(layout.createSequentialGroup()
            .addContainerGap()
            .addComponent(jPanel1, javax.swing.GroupLayout.DEFAULT_SIZE,
javax.swing.GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE)
              try {
        for (javax.swing.UIManager.LookAndFeelInfo info : javax.swing.UIManager.getInstalledLookAndFeels()){
      /* if("Nimbus".equals(info.getName())) {
          javax.swing.UIManager.setLookAndFeel(info.getClassName());
          break;
       }*/
            // UIManager.setLookAndFeel("com.jtattoo.plaf.smart.SmartLookAndFeel");
            UIManager.setLookAndFeel("com.jtattoo.plaf.acryl.AcrylLookAndFeel");
    }
      }  catch (javax.swing.UnsupportedLookAndFeelException e) {
    // handle exception
        java.util.logging.Logger.getLogger(db.class.getName());
  }

  }
      java.awt.EventQueue.invokeLater(new Runnable() {
        public void run() {
            new login().setVisible(true);
  private javax.swing.JLabel txt_date;


i
```