VIRTUAL PRIVATE NETWORK

By

S. Anandavalli

Reg No 71203621005

of

KUMARAGURU COLLEGE OF TECHNOLOGY
COIMBATORE

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

June, 2006

Kumaraguru College of Technology
Coimbatore-641006

Department of Computer Applications

Bonafide Certificate

Certified that this project report titled **Virtual Private Network** is the bonafide work of **Ms. S. Anandavalli (Reg No. 71203621005)** 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.

Project Guide **Head of the Department**

Submitted for the University Examination Held on 30.06.06.

30/6

Internal Examiner

30/6/06

External Examiner

TECHNOLOGIES ... *thoughts unwrapped*

TO WHOMSOEVER IT MAY CONCERN

This is to certify that **Ms. S. ANANDAVALLI. Reg no 71203621005**, final year **M.C.A, Kumaraguru College Of Technology Coimbatore**, has completed her project in this organization. She did the project entitled **"VIRTUAL PRIVATE NETWORK"** in **J2EE from January 2006 to May 2006** at our organization in partial fulfillment of the requirements for the award of M.C.A, Anna University. Her work was timely from the company's perception and useful to the company.

As part of the company's policy we don't let out any sort of coding or pseudo code out of the company's premises in printed or in electronic media.

For I MAATRIXX CONSULTING.
Merunaline.S
Human Resource Department

ACKNOWLEDGEMENT

I wish to express my sincere thanks to **Dr. K.K. Padmanabhan Ph. D.**, former principal, and **Dr. Joseph.V.Thanikal Ph.D.**, principal, Kumaraguru College of Technology, Coimbatore, for permitting me to undertake this project.

My deepest acknowledgement to **Dr. M. Gururajan Ph. D.**, Head of the Department, Department of Computer Applications, Kumaraguru College of Technology, Coimbatore, for his timely help and guidance throughout this project.

I am greatly indebted to my project guide **Mr. S. Ganesh Babu MCA**, Lecturer, Department of Computer Applications, Kumaraguru College of Technology, for his valuable guidance and inspiring words at every stage of this project.

I would like to express my gratitude to all the staff members for their timely help and guidance to complete the project successfully.

ABSTRACT

The project **Virtual Private Network** is a secured network through which the data will be transferred in a reliable manner. The Virtual Private Network has the ability of providing connection between the various branches of an organization in a secured way.

The existing system has only the head office. Due to the extension of the branch office the proposed system includes the software for managing the branch office and its security.

The project highlights the concept behind establishing the Virtual Private Network taking into consideration the aspects of Virtual Private Network namely Authentication, Authorization and Data Encryption using tunneling.

Tunneling is the logical path which is the portion of the connection in which the private data is encapsulated and sent. The tunneling is established through the Layer Two Tunneling Protocol which is configured.

This project also deals with developing the software for the branch office where it contains three modules namely Employee Module, Marketing Module and Training Module.

CONTENTS

LIST OF TABLES

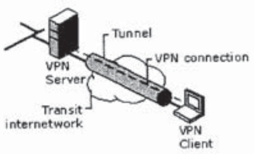
LIST OF FIGURES

CHAPTER 1

INTRODUCTION

A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

To emulate a point-to-point link, data is encapsulated, or wrapped, with a header that provides routing information allowing it to traverse the shared or public transit internetwork to reach its endpoint. To emulate a private link, the data being sent is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the encryption keys. The portion of the connection in which the private data is encapsulated is known as the tunnel. The portion of the connection in which the private data is encrypted is known as the virtual private network (VPN) connection.



1.1 Virtual private network connection

VPN technology also allows a corporation to connect to branch offices or to other companies over a public internetwork (such as the Internet), while maintaining secure communications. The VPN connection across the Internet logically operates as a wide area network (WAN) link between the sites.

In both of these cases, the secure connection across the internetwork appears to the user as a private network communication despite the fact that this communication occurs over a public internetwork—hence the name virtual private network.

The key feature of a VPN, however, is its ability to use public networks like the Internet rather than rely on private leased lines. VPN technologies implement restricted-access networks that utilize the same cabling and routers as a public network, and they do so without sacrificing features or basic security.

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.

VPN technology is designed to address issues surrounding the current business trend toward increased telecommuting and widely distributed global operations, where workers must be able to connect to central resources and must be able to communicate with each other.

With an Internet solution, a few Internet connections through Internet service providers (ISPs) and VPN server computers can serve the remote networking needs of hundreds or thousands of remote clients and branch offices.

1.1 PROJECT OVERVIEW

The Virtual Private Network has the ability of providing connection between the various branches of an organization in a secured way. This system connects the main office and the branch office. There was only main office before. Due to the extension of the branch office, this system includes the software for managing the branch office of the organization and virtual software to provide security.

The software which manages the branch office includes three modules namely

- **Employee Module**
  This module maintains official and personal details about the employee.
- **Marketing Module**
  This module maintains the client details of the branch office.
- **Training Module**
  This module maintains the training details of the branch office.

The virtual software which provides the security for the data which is transferred through the virtual private network has three main functions.

- **Authentication**
  The user who tries to communicate between the main office and the branch office is checked whether he belongs to that particular office.
- **Authorization**
  The designation of the employee is checked whether he can access to that particular resource.

- **Data Protection**
  The data protection is achieved by implementing the cryptographic algorithm (RSA Algorithm).

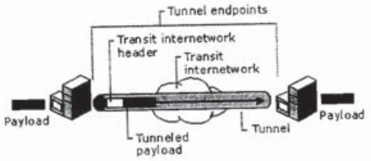
Virtual Private Network

The communication between the main office and the branch office of the HUNDRED PERCENT TECHNOLOGIES is done through the private network called, Virtual Private Network. The virtual path is established in the internet itself through the tunneling.

Tunneling Basics

Tunneling is a method of using an internetwork infrastructure to transfer data for one network over another network. Instead of sending a frame as it is produced by the originating node, the tunneling protocol encapsulates the frame in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate internetwork.

The encapsulated packets are then routed between tunnel endpoints over the internetwork. The logical path through which the encapsulated packets travel through the internetwork is called a tunnel. Once the encapsulated frames reach their destination on the internetwork, the frame is decapsulated and forwarded to its final destination. Tunneling includes this entire process (encapsulation, transmission, and decapsulation of packets).



The transit internetwork can be any internetwork-the Internet is a public internetwork and is the most widely known real world example.

The tunnel transfers the data through the Layer Two Tunneling Protocol (L2TP). The tunnels make it possible to use a public TCP/IP network, such as the Internet, to create secure connections between remote users and a private corporate network.

L2TP

The L2TP protocol defines mechanisms both for establishing and controlling the tunnel and for transferring data.

Functions of the L2TP Protocol

- Negotiate tunnel parameters
- Establish tunnels
- Authenticate users and data
- Encryption and Decryption of the data and addresses
- Manage security keys.
- Manage data transfer across the tunnel
- Manage data transfer inbound and outbound as a tunnel endpoint or router

Configuring L2TP:

- Set the Maximum Tunnel Idle Time
- Control the Retransmission Interval
- Control the Retransmit Limit
- Number of Tunnels established at a time
- Interval between the transmission
- These are the details to be considered and confirmed for this protocol.

This is how the data is encrypted and sent and at the receiver end it is decrypted.

1.2 GOALS OF THE PROJECT

The objectives of the project are

- Reduce the cost of communication between the different LANS.
- Improve the security through the virtual path
- Increase the reliability

CHAPTER 2

SYSTEM STUDY

System study is the process of gathering and interpreting the facts, diagnosing the problems, and using the information to recommend improvements to the system. The investigation into the system's operations brings out the current methods that the system is following and evaluates the effectiveness by using this information.

2.1 SOFTWARE REQUIREMENT AND SPECIFICATION

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

The Software Requirements Specification is based on the system definition high level requirements during initial planning are elaborated and more specific in order to characterize the features that the software product will incorporate the requirement specification is primarily concerned with functional and a performance aspect of the software product and emphasis is placed on specifying product characteristics without implying how the product will provide those characteristics

Desirable properties of a Software Requirements Specification

- Correct
- Complete
- Consistent
- Unambiguous
- Functional
- Verifiable

2.2 HARDWARE SPECIFICATIONS

CPU type	:	Pentium III
Memory	:	128 MB RAM
Hard disk	:	20 GB hdd
Key board	:	110 keys
Floppy Drive	:	1.44 MB fdd

2.3 SOFTWARE SPECIFICATIONS

Software	:	J2EE
Operating System	:	Windows'2k
Front end	:	HTML, Java Script
Server Side Scripting	:	Java Server Pages
Server	:	Apache Tomcat server 4.1
Back end	:	Oracle 8i

2.4 SOFTWARE OVERVIEW

Benefits of using java

Write Once, Run Anywhere

Sun identifies "Write once, run anywhere" as the core value proposition of the Java platform. Translated from business jargon, this means that the most important promise of Java technology is that you only have to write your application once--for the Java platform--and then you'll be able to run it anywhere.

Anywhere, that is, that supports the Java platform. Fortunately, Java support is becoming ubiquitous. It is integrated, or being integrated, into practically all major operating systems. It is built into the popular web browsers, which places it on virtually every Internet-connected PC in the world.

Security

Another key benefit of Java is its security features. Both the language and the platform were designed from the ground up with security in mind. The Java platform allows users to download un trusted code over a network and run it in a secure environment in which it cannot do any harm: it cannot infect the host system with a virus, cannot read or write files from the hard drive, and so forth. This capability alone makes the Java platform unique.

The Java 2 Platform takes the security model a step further. It makes security levels and restrictions highly configurable and extends them beyond applets. As of Java 1.2, any Java code, whether it is an applet, a servlet, a JavaBeans component, or a complete Java application, can be run with restricted permissions that prevent it from doing harm to the host system.

The security features of the Java language and platform have been subjected to intense scrutiny by security experts around the world.

when a new security bug is found. Remember, however, that no other mainstream platform can make security guarantees nearly as strong as those Java makes. If Java's security is not yet perfect, it has been proven strong enough for practical day-to-day use and is certainly better than any of the alternatives.

Network-centric Programming

Sun's corporate motto has always been "The network is the computer." The designers of the Java platform believed in the importance of networking and designed the Java platform to be network-centric. From a programmer's point of view, Java makes it unbelievably easy to work with resources across a network and to create network-based applications using client/server or multitier architectures. This means that Java programmers have a serious head start in the emerging network economy.

Dynamic, Extensible Programs

Java is both dynamic and extensible. Java code is organized in modular object-oriented units called classes. Classes are stored in separate files and are loaded into the Java interpreter only when needed. This means that an application can decide as it is running what classes it needs and can load them when it needs them. It also means that a program can dynamically extend itself by loading the classes it needs to expand its functionality.

The network-centric design of the Java platform means that a Java application can dynamically extend itself by loading new classes over a network. An application that takes advantage of these features ceases to be a monolithic block of code. Instead, it becomes an interacting collection of independent software components. Thus, Java enables a powerful new metaphor of application design and development.

Internationalization

The Java language and the Java platform were designed from

rather than tacked on as an afterthought. While most programming languages use 8-bit characters that represent only the alphabets of English and Western European languages, Java uses 16-bit Unicode characters that represent the phonetic alphabets and ideographic character sets of the entire world. Java's internationalization features are not restricted to just low-level character representation, however. The features permeate the Java platform, making it easier to write internationalized programs with Java than it is with any other environment.

Performance

Java programs are compiled to a portable intermediate form known as byte codes, rather than to native machine-language instructions. The Java Virtual Machine runs a Java program by interpreting these portable byte-code instructions. This architecture means that Java programs are faster than programs or scripts written in purely interpreted languages, but they are typically slower than C and C++ programs compiled to native machine language. Keep in mind, however, that although Java programs are compiled to byte code, not the entire Java platform is implemented with interpreted byte codes. For efficiency, computationally intensive portions of the Java platform--such as the string-manipulation methods--are implemented using native machine code.

Although early releases of Java suffered from performance problems, the speed of the Java VM has improved dramatically with each new release. The VM has been highly tuned and optimized in many significant ways. Furthermore, many implementations include a just-in-time compiler, which converts Java byte codes to native machine instructions on the fly. Using sophisticated JIT compilers, Java programs can execute at speeds comparable to the speeds of native C and C++ applications.

Programmer Efficiency and Time-to-Market

The final, and perhaps most important, reason to use Java is

Java and are usually amazed at how quickly they can get results with it. Studies have consistently shown that switching to Java increases programmer efficiency. Because Java is a simple and elegant language with a well-designed, intuitive set of APIs, programmers write better code with fewer bugs than for other platforms, again reducing development time.

Java and internet

Java is strongly associated with internet and known as internet programming language. Internet users can use java to create applet programs and run them locally using java enabled browser search as hot java. Applets can be downloaded from remote machine via internet and run it on local machine.

Java and World Wide Web

World Wide Web is an open ended information retrieval system designed to be used in the distributed environment. This system contains web pages that provide both information and controls. We can navigate to a new web page in any direction. This is made possible worth HTML java was meant to be used in distributed environment such as internet. So java could be easily incorporated into the web system and is capable of supporting animation graphics, games and other special effect. The web has become more dynamic and interactive with support of java. We can run a java program on remote machine over internet with the support of web.

CHAPTER 3

SYSTEM ANALYSIS

System analysis is concerned with investigating and analyzing, which is used to gain an understanding of the existing system and what is required.

Finally, systems analysis tells what the system should do to overcome the existing problems.

3.1 EXISTING SYSTEM

The organization has the main office and software for managing the main office. Since there was no branch office, there was no need for communication and network security.

3.2 PROPOSED SYSTEM

The branch office of the organization is to be extended. So this system is for managing the branch office and to provide the secure communication between the main office and the branch office through the Virtual Private Network. The virtual software provides all the features of the Virtual Private Network such as Authentication, Address Management and Encryption and Decryption.

Purpose

1. **Improve Security**

   The data has been transferred between the main office and the branch office in the secured way.

2. **Extend geographic connectivity**

   The distance between the main office and the branch office is not the problem. Even if the distance between the offices is long the data can be transferred reliably.

3. **Reduce operational costs versus traditional WAN**

   The operational costs are reduced compared to the Wide Area Network costs.

4. **Reduce transit time and transportation costs**

   Since the data is transferred through the internet the data transmission time and the transportation costs are low.

5. **Provide global networking opportunities**

   Since the data is transferred through the internet the interaction with the globe is also very easy.

3.3 MODULE FUNCTIONALITIES

The proposed system has the following modules in managing branch office.

- Employee Module
- Marketing Module
- Training Module

3.3.1 Employee Module

This module maintains the employee details of the branch office. The Employee Module maintains the employee details of the branch office, of HUNDRED PERCENT TECHNOLOGIES. This module is accessible only if the users are authorized. The official details and personal details of the each employee are maintained.

The following functions will be made available for Administration:

- Maintaining Employee Details
- Viewing Employee Details
- New Staff Registration
- Viewing the Personal Details of the Employee
- Viewing the Salary Details
- Updates the employee Details
- Deleting the employee's entry from the database

3.3.2 Marketing Module

This module maintains the client details of the branch office. This module is accessible to only the administrator.

The following functions will be made available for Marketing:

- Adding New clients
- Updates the Client Details
- Viewing the Clients of the branch office and their details
- Deleting the client from the list

3.3.3 Training Module

This module maintains the training details of the branch office. This module maintains both the Technical and Management training details of this branch office. This module is accessible only if the users are authorized.

The following functions will be made available for Training:

- Maintaining the technical training staff details and soft skill training staff details separately.
- Maintaining the list of soft wares to be trained.
- Updates the soft wares to be trained.
- Updates the staffs details
- Viewing the list of technical staffs based on the software they are specialized.
- Viewing the list of soft wares to be trained.
- Deleting the training course if it is not trained

This system develops the software for maintaining the branch office details and connects the main office and the branch office of the organization. The communication between the main office and the branch office of the organization is through the virtual private network. To establish the communication through the Virtual Private Network, the Virtual Software is needed.

The virtual software highlights the security concepts behind establishing the Virtual Private Network. It includes the following functions:

- Authentication
- Authorization
- Data Protection

The virtual software is included in both the main office and the branch office.

3.3.4 Authentication

This module mainly deals with ensuring the persons who are all related to the main office and its branch office. The virtual software in the main office ensures that the employees trying to communicate with the branch office from the main office are related to the main office. The virtual software in the branch office ensures that the employees trying to communicate with the main office from the branch office are related to the branch office.

It also provides audit and accounting records to show who accessed what information and when.

This module mainly deals with ensuring the persons who are all related to the own corporate VPN.

- The User Authentication verifies the VPN client's identity and restrict VPN access to authorized users only.
- It also provides the audit and accounting records to show who accessed what information and when

3.3.5 Authorization

This module mainly deals with the hierarchical level of the organization. The various employees have their own limits and boundaries to communicate. The employee's designation is checked for communication in both the main office and the branch office. In main office the employee's designation is checked whether they can communicate with the branch office. In branch office the employee's designation is checked whether they can communicate with the main office.

3.3.6 Data Protection

The data protection is achieved through the cryptographic algorithms which encrypt the data at the sender side and decrypt at the receiving end.

Data Encryption and Decryption

The data send from the main office to the branch office or vice versa are encrypted before sending. The place where the data is received, it is decrypted.

Encryption is the process of transforming plaintext into cipher text using the specified key. The reverse process of transforming cipher text into plaintext using a specified key is called decryption.

Rivest Shamir Adleman (RSA) Algorithm

The most famous of the public-key cryptosystem is RSA, which is named after its three developers Ron Rivest, Adi Shamir, and Leonard Adleman. At the time of the algorithm's development (1977), the three were researchers at the MIT Laboratory for Computer Science.

Key Generation

i. Generate two large prime numbers, p and q. Let n = pq.
   Let z = (p-1)(q-1).
ii. Choose a small number e, co prime to z. Find d, such that de % z = 1.
iii. Publish e and n as the public key. Keep d as the secret key.
iv. Encryption C = (P^e) % n. Decryption P = (C^d) % n whereas x % y means the remainder of *x* divided by *y*. Its security comes from the computational difficulty of factoring large numbers. To be secure, very large numbers must be used for p and q - 100 decimal digits at the very least.
v. Publish d and n as the public key. Keep e and n as the secret key.

Encryption C = (P^e) % n Decryption P = (C^d) % n where as x % y means the remainder of *x* divided by *y* .Its security comes from the computational difficulty of factoring large numbers. To be secure, very large numbers must be used for p and q - 100 decimal digits at the very least.

Encryption

i. Plaintext and public key (d and n values) are given as input.
ii. All the alphabets are assigned with the numerical values from A to Z.
iii. Plaintext letter is taken and corresponding numerical value is assigned.
iv. The assigned numerical value is multiplied 'e' number of times (to the power of 'e') – ie P^e.
v. Numerical value modulo 'n' is found ((P^e) mod n) and the resultant value will be the encrypted value for corresponding letter.

C = P^e % n

Where C is the Cipher text
P is the Plaintext alphabet value
e is the Encryption exponent
n is pq p,q → prime numbers

The special characters will not undergo any change while encryption or decryption. They are displayed as it is.

The receiver needs to construct two large prime numbers denoted p and q. The product of p and q is denoted n=pq. In practice, the prime numbers p and q each have about the same number of digits and are selected so that their product n is 33 or more digits long. The receiver then selects an integer *e* that has a multiplicative inverse modulo z=(p-1)(q-1). This is called the encryption exponent. The receiver then constructs the multiplicative inverse of *e* modulo (p-1)(q-1); That number is the decryption exponent and is denoted d.

The receiver's public key consists of two numbers – n and e. This is sender's public-key address. These two numbers are available to anyone who might want to send an encrypted message to receiver. The receiver keeps the decryption exponent d secret; it is his private key. The private key is used by receiver to decrypt any messages sent to him that have

For someone to cryptanalyze a message sent to receiver using his public key, they would have to be able to construct the private key d, which is the inverse of e modulo (p-1)(q-1). This can be easily done if p and q are known, but to get p and q, the cryptanalyst would need to be able to factor the other half of Josh's public key n. That is the problem. There is no efficient way to find q even if n is known (provided that n is large and p and q are approximately the same size).

If sender wants to send the message to the receiver using receiver's public key, first, the message must be converted to a string of numbers. Cipher text is obtained by raising each plaintext block to the exponent *e* modulo *n*.

$$p^e \bmod n = C$$

The message that sender transmits to receiver is the cipher text. For encryption, the letters are replaced by their corresponding numerical values.

Decryption

Decryption depends on Euler's corollary to Fermat's Little Theorem. Euler's corollary says that a^z. Because n=pq, this says that a^z = 1 mod n. Now e and d are inverses modulo z; i.e., ed=1 mod z. Another way of saying this is that ed is 1 plus a multiple of z; i.e., ed=1+k(z).

$$C^d \equiv (p^e)^d \equiv p^{ed}$$

$$\equiv p^{1+k(r-1)(s-1)} \equiv p^1 p^{k(r-1)(s-1)}$$

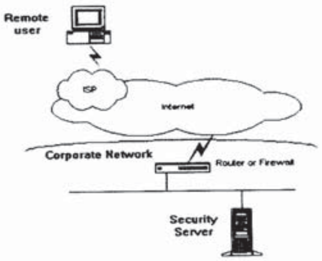
$$\equiv p\left(p^{(r-1)(s-1)}\right)^k \equiv p(1)^k \equiv p \bmod n \text{ that is, } C^d \bmod n = p$$

which is back to plaintext.

Working Process of Virtual Private Network

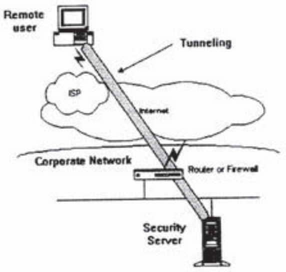
A remote employee wants to connect into the corporate network and access their company's internal web.

Step 1. The remote user dials into their local ISP and logs into the ISP's network as usual.



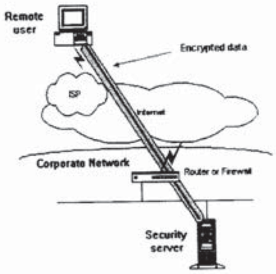
3.3.1 Communication between two Different Networks

Step 2. When connectivity to the corporate network is desired, the user initiates a tunnel request to the destination Security server on the corporate network. The Security server authenticates the user and creates the other end of tunnel.



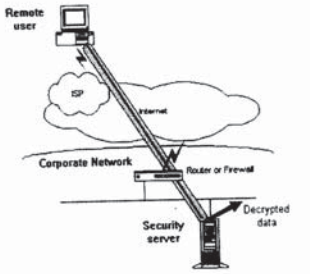
3.3.2 Tunneling in Communication

Step 3. The user then sends data through the tunnel which encrypted by the VPN software before being sent over the ISP connection.



3.3.3 Sending Encrypted Data

Step 4. The destination Security server receives the encrypted data and decrypts. The Security server then forwards the decrypted data packets onto the corporate network. Any information sent back to the Remote user is also encrypted before being sent over the Internet.

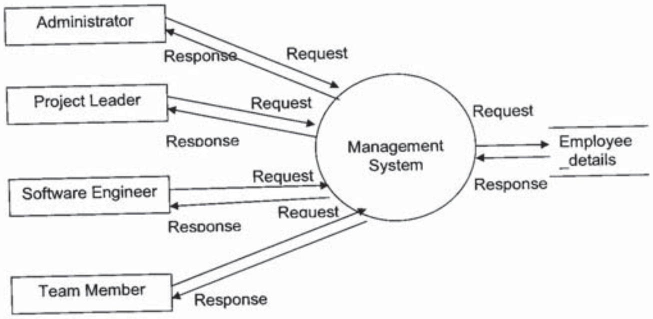


3.3.4. Data Decrypted at the receiving End

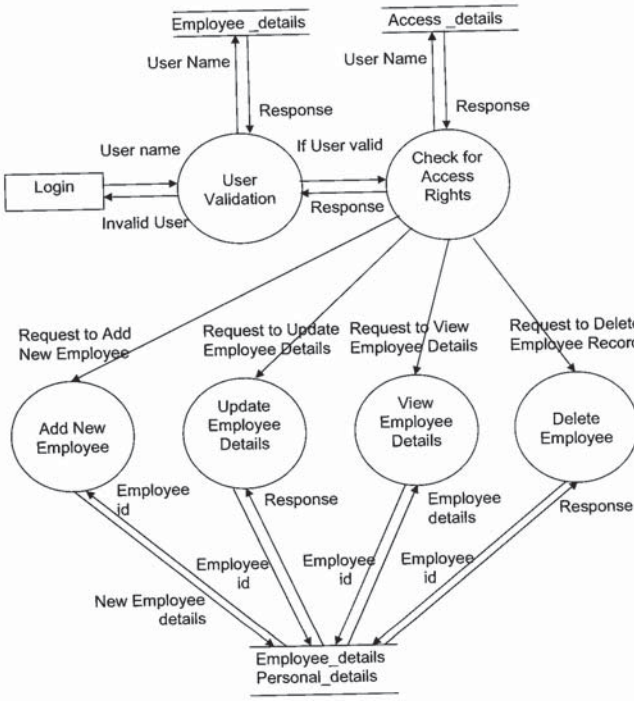
This is how the communication has been established between the main office and the branch office.

3.4. ANALYSIS MODEL

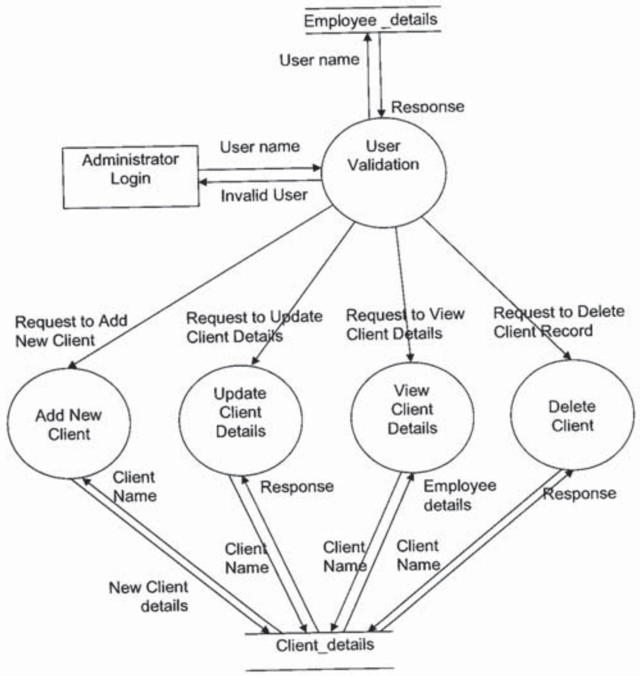
Data Flow Diagram - Level 0



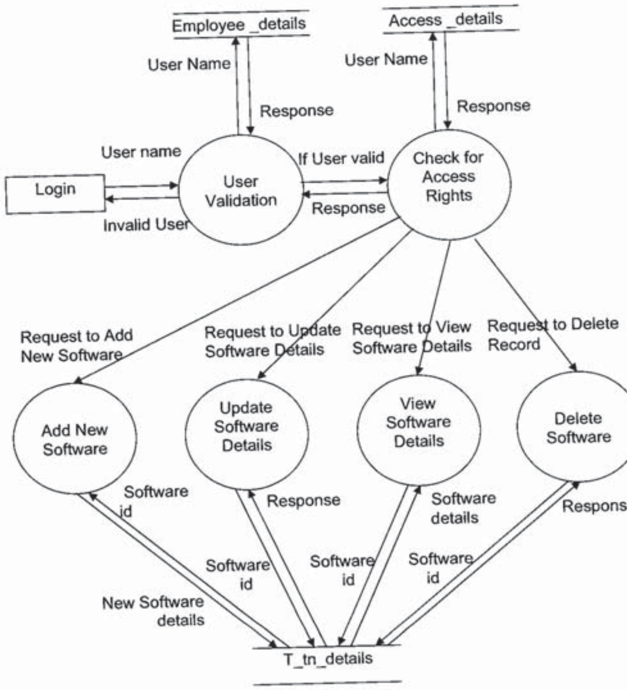
Level-1 Employee Module



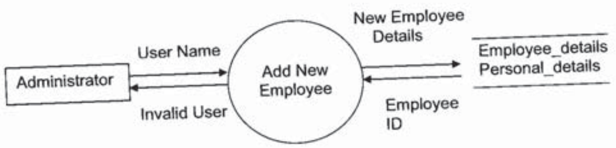
Level-1 Marketing Module



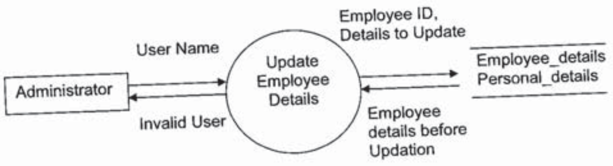
Level-1 Training Module



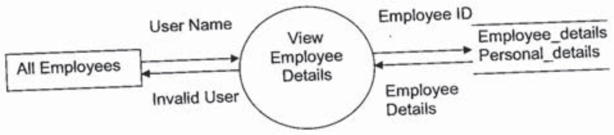
Level-2 Employee Module – Add New Employee Record



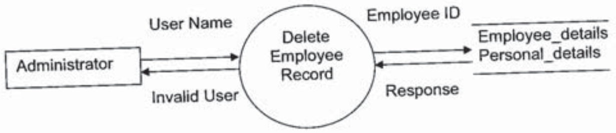
Level-2 Employee Module – Update Employee Details



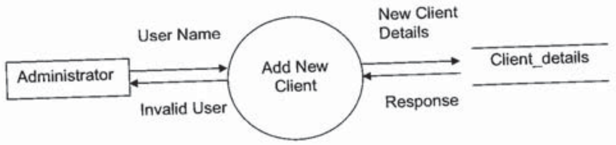
Level-2 Employee Module – View Employee Details



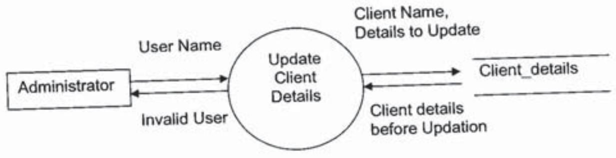
Level-2 Employee Module – Delete Employee Record



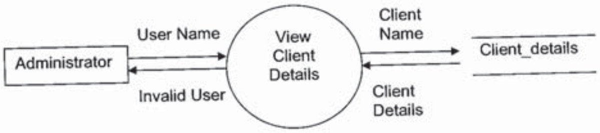
Level-2 Marketing Module – Add New Client Record



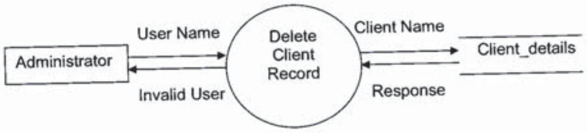
Level-2 Marketing Module – Update Client Details



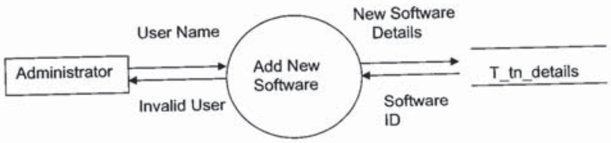
Level-2 Marketing Module – View Client Details



Level-2 Marketing Module – Delete Client Record



Level-2 Training Module – Add New Software



3.5 FEASIBLTY STUDY

Feasibility is the determination of whether or not a project is worth doing Feasibility study is high-level capsule version of the extra system analysis and the design process. The success of a system also lies in the amount of feasibility study done on it. There are three main feasibility tests performed. They are

Operational Feasibility

During feasibility analysis, operational feasibility study is necessary as it ensures that the project developed is successfully implemented in the organization. According to software engineering principles, operational feasibility or in other words usability should be high. A through analysis is done and found that the system is operational.

Technical Feasibility

Technical feasibility takes care of the technical issues that are to be tested to see whether the system is feasible. Technical feasibility makes a comparison between the level of technology available and the technology that is needed for the project. The level of technology is determined by factors such as the software tools available, the machine environment, platform etc since, the resource required for the development of the project is already available in the organization, and this project is technically feasible.

Economical Feasibility

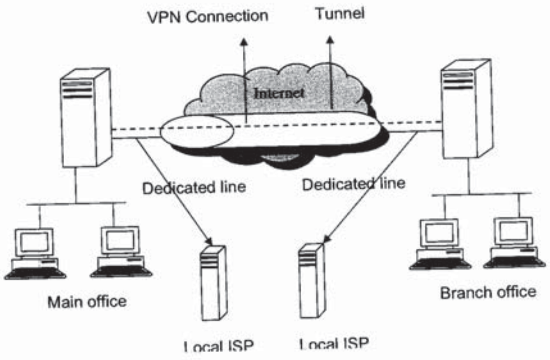
This is the most important aspect that has to be critical evaluated. The costs and benefits have to be estimated. Considering the cost factor, since the client is ready to pay a reasonable amount, which will be more than the cost of developing the system, the system will be economically feasible.

CHAPTER 4

SYSTEM DESIGN

4.1 OVERALL SYSTEM DESIGN

Virtual Private Network



4.2 INPUT DESIGN

Input to the system can be defined as the information that is to be provided to the system that will be used for further processing by the system to obtain meaningful information, which helps in decision making.

Input design is a process of converting user originated inputs to computer based format. The objectives followed while doing input design is controlling the data entered that is preventing the entry of invalid data, all the validation checks to be done on the data entered are specified

Module Inputs

Employee Module

- The Employee Name, Qualification, Department and Designation are given as inputs for adding employee's official details.
- The Date of birth, Mail ID, Contact Number and Address are given as inputs for adding employee's personal details.
- To update or view the employee details the Employee ID is obtained as input.

Marketing Module

- The client details of the organization such as Client Name, Address, Mail ID, Contact Number and Contact Person are given as inputs to add.
- To update or view the client details the Client Name is obtained as input.

Training Module

- The software name and the duration of the training are given as inputs to add in the technical trainer's details.
- The management skill name and the duration of the training are given as inputs to add in the management trainer's details.

- To update or view the training details the Software ID is obtained as input.

Input Screens are designed to accept input from the user. Here the screens are more users friendly. They are given in the Appendices.

4.2 OUTPUT DESIGN

Output from the system can be defined as the processed information that is generated by the system in a specified format using the information available.

Module Output

Employee Module

The Employee details are obtained as output if the employee ID is given.

Marketing Module

The Client details are obtained as output if the Client Name is given.

Training Module

The Training details are obtained as output if the Software ID is given.

4.3 TABLE DESIGN

The database of the project contains the following tables for various storing and retrieving various data required. The general theme is to handle information as an integrated whole, with a minimum of redundancy and improved performance.

4.3.1. Employee_details

Table Name	Employee_details
Description	Stores the official information for all the employees in the office

Table Header	Column Name	Data type	Size	PK
Employee_details	EmpId	VARCHAR2	15	Y
	Password	VARCHAR2	15	
	EmpName	VARCHAR2	25	
	Qualification	VARCHAR2	30	
	Designation	VARCHAR2	30	
	Department	VARCHAR2	30	

4.3.2 Personal_details

Table Name	Personal_details
Description	Stores the personal information for all the employees in the office

Table Header	Column Name	Data type	Size	PK
Personal_details	EmpId	VARCHAR2	15	Y
	Dob	DATE		
	MailID	VARCHAR2	40	
	Contact No	NUMBER	20	
	Address	VARCHAR2	70	

4.3.3 Salary_details

Table Name	Salary_details
Description	Stores the salary details for all the employees in the office

Table Header	Column Name	Data type	Size	PK
Salary_details	EmpId	VARCHAR2	15	Y
	BasicPay	NUMBER	6,2	
	Hra	NUMBER	3,2	
	ma	NUMBER	3,2	
	otherAllow	NUMBER	3,2	
	grossPay	NUMBER	6,2	
	Lic	NUMBER	3,2	
	Pf	NUMBER	3,2	
	netPay	NUMBER	6,2	

4.3.4 Client_detials

Table Name	Client_details
Description	Stores the client details of the branch office

Table Header	Column Name	Data type	Size	PK
[illegible]	ClientName	VARCHAR2	30	Y
	ContactPerson	VARCHAR2	25	
	ContactNo	NUMBER		
	Mail ID	VARCHAR2	40	
	Address	VARCHAR2	70	

4.3.5 T_tn_details

Table Name	T_tn_details
Description	Stores the list of soft wares to be trained

Table Header	Column Name	Data type	Size	PK
[illegible]	SId	NUMBER		Y
	Soft_t_name	VARCHAR2	30	
	Duration	NUMBER		

4.3.6 Tech_tra_details

Table Name	Tech_tra_details
Description	Stores all the technical trainers in the office and the software they train

Table Header	Column Name	Data type	Size	PK
[illegible]	EmpId	VARCHAR2	15	Y
	SId	NUMBER		

4.3.7 M_tn_details

Table Name	M_tn_details
Description	Stores the list of management trainings available

Table Header	Column Name	Data type	Size	PK
	MId	NUMBER		Y
	Mgnt_t_Name	VARCHAR2	30	
	Duration	NUMBER		

4.3.8 Mgnt_tra_details

Table Name	Mgnt_tra_details
Description	Stores all the soft skill trainers in the office and the software they train.

Table Header	Column Name	Data type	Size	PK
	EmpId	VARCHAR2	15	Y
	M_Id	NUMBER		

4.3.9 Module_details

Table Name	Module_details
Description	Stores the available modules of the managing system in the branch Office.

Table Header	Column Name	Data type	Size	PK
	ModuleId	NUMBER		Y
	ModuleName	VARCHAR2	30	

4.3.10 Access_details

Table Name	Access_details
Description	Maintains the accessibility of all the employees for each modules of the system

Table Header	Column Name	Data type	Size	PK
	EmpId	VARCHAR2	15	Y
	ModuleId	NUMBER		
	Add	CHAR	1	
	Update	CHAR	1	
	View	CHAR	1	
	Delete	CHAR	1	

These are the tables used for this system.

CHAPTER 5

SYSTEM TESTING

Software testing is a critical element of software quality assurance and represents the ultimate reviews of specification, design and coding .Testing presents an interesting anomaly for the software. Testing is vital to the success of the system. Errors can be injected at any stage during development. System testing makes a global assumption that if all the parts of the system are correct, the goal will be successfully achieved. During the testing, the program to be tested is executed with set of test data and the output of the program for the test data is evaluated to determine if the programs are performed as expected. A series of testing are performed for the application developed. The testing steps are

- Unit Testing
- Validation Testing
- Output Testing

5.1 UNIT TESTING

Unit testing focuses verification effort on the smallest unit of the software design, the module is known as module testing. Since the application has modules the testing is individually performed on each module. Using the detailed design description as a guide, important control paths are tested to uncover errors within the boundary of the module. This testing was carried out during programming stage itself. In this testing each module is found to be working satisfactorily as regards to the expected output from the module.

i. In the Employee Module if the new employee details are included it is tested whether it returns the Employee ID properly.

ii. In the Employee Module if the employee details are updated, the employee details are again viewed to check whether the details are updated properly.

iii. The Marketing Module can be accessed only if the user is administrator. This is also tested properly.

iv. In authentication function, the designation of the employees is checked for providing access rights.

v. In data protection function, it is checked whether the data has been encrypted properly. The testing is performed to verify all the characters such as alphabets, special characters and numbers are encrypted properly.

5.2 VALIDATION TESTING

At the culmination of the integration testing, software is completely assembled as a package. Interfacing errors have been uncovered and corrected and a final series of software test validation testing beings.

Software validation is achieved through a series of black box tests that demonstrate conformity with requirement. After validation test has been conducted, one or two conditions exist.

The function or performance characteristics confirm to specifications is accepted. A validation from the specification is uncovered and a deficiency created. Deviation or errors discovered at this step in this project is corrected prior to completion of the project with the help of the user by negotiating to establish a method for resolving deficiencies. The application has been tested by using validation testing and found to be working satisfactorily

i. In the Employee Module, the Employee Name, Qualification and the designation fields are tested. If the special characters or numbers are given the error message is displayed.
ii. In the Employee module, the Contact Number is checked whether all the characters are numbers. If not error message is displayed.
iii. In the Marketing Module, the Client Name and the Contact Person fields are checked. If any number or special character is given then error message is shown.
iv. In the Training Module the number of days of training field is checked for number. If a alphabet or special character is given then error message is displayed.

5.3 OUTPUT TESTING

After performing the validation testing, the next step is output testing of the application, since no application will be useful if it does not produce the required output in the specific format. The output is verified for the same values by working them out manually. The result generated by the application is compared with that of the results obtained manually to find out the correctness.

The main function of this system is to transfer data in a secure manner. The data which has been sent at one end is tested whether it is received at the other end properly.

CHAPTER 6

CONCLUSION AND FUTURE OUTLOOK

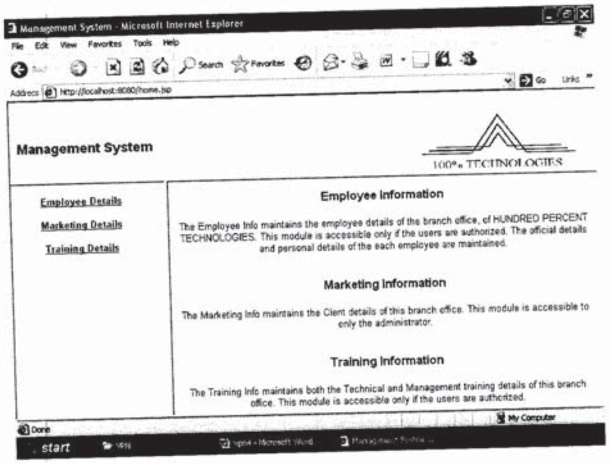
Thus the communication between the main office and the branch of HUNDRED PERCENT TECHNOLOGIES was carried out using **Virtual Private Network**. The system also manages the branch office details.

The system supports establishing only one tunnel. In future, the system can be extended for establishing many tunnels at a time.

APPENDICES

SCREEN SHOTS

Management System-Home Page



Management System - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Search Favorites
Address http://localhost:8080/home.jsp
Go Links
100% TECHNOLOGIES
Done
My Computer
start
vpn - Microsoft Word
Management System ...

Management System

Employee Details

Marketing Details

Training Details

Employee Information

The Employee Info maintains the employee details of the branch office, of HUNDRED PERCENT TECHNOLOGIES. This module is accessible only if the users are authorized. The official details and personal details of the each employee are maintained.

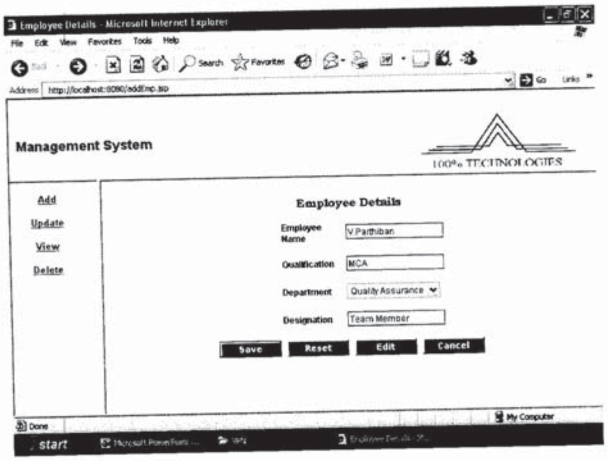
Marketing Information

The Marketing Info maintains the Client details of this branch office. This module is accessible to only the administrator.

Training Information

The Training Info maintains both the Technical and Management training details of this branch office. This module is accessible only if the users are authorized.

Adding New Employee's Details


Employee Details - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8080/addEmp.jsp
Go Links
100% TECHNOLOGIES
Done
My Computer
start

Management System

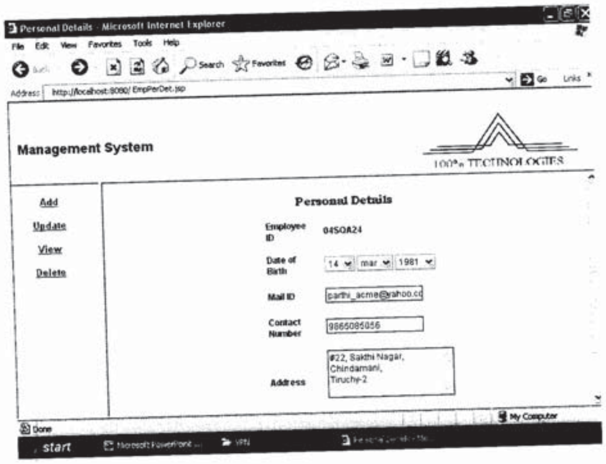
Add
Update
View
Delete

Employee Details

Employee Name	V.Parthiban
Qualification	MCA
Department	Quality Assurance
Designation	Team Member

Save Reset Edit Cancel

Adding New Employee's personal Details


Personal Details - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8080/ EmpPerDet.jsp
Go Links
100% TECHNOLOGIES
Done
My Computer
start
Microsoft PowerPoint ...
VPN

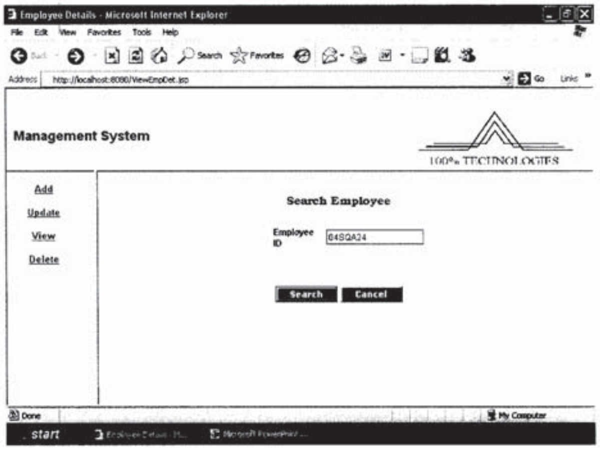
Management System

Add
Update
View
Delete

Personal Details

Employee ID	04SQA24
Date of Birth	14 mar 1981
Mail ID	parthi_acme@yahoo.co
Contact Number	9865085056
Address	#22, Sakthi Nagar, Chindamani, Tiruchy-2

Search to View Employee Details


Employee Details - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8080/ViewEmpDet.jsp
Go Links
100% TECHNOLOGIES
Done
My Computer
start
Microsoft PowerPoint ...

Management System

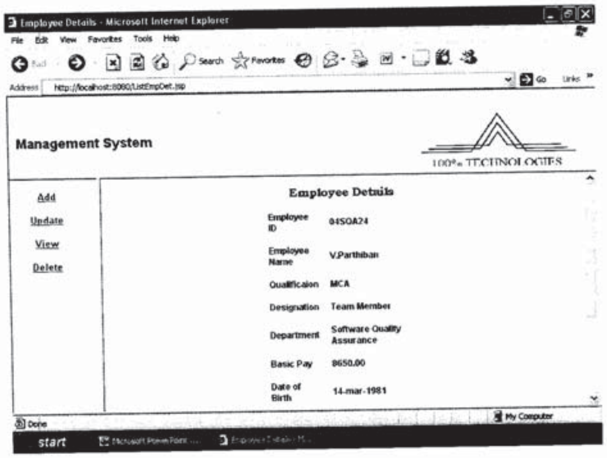
Add
Update
View
Delete

Search Employee

Employee ID: 04SQA24

Search Cancel

Viewing Employee Details


Employee Details - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8080/ListEmpDet.jsp
Go Links
100% TECHNOLOGIES
Done
My Computer
start
Microsoft PowerPoint ...

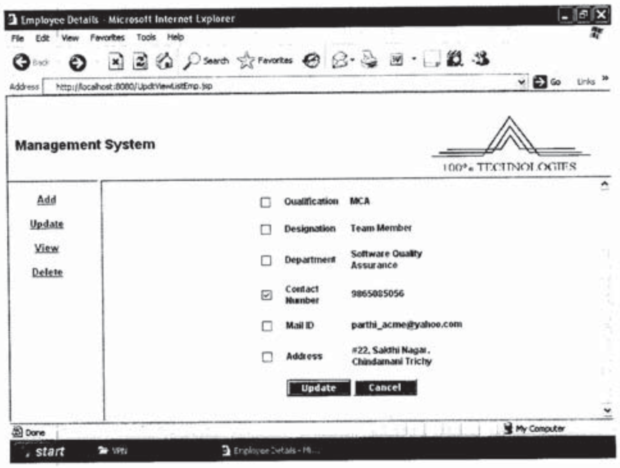
Management System

Add
Update
View
Delete

Employee Details

Employee ID	04SQA24
Employee Name	V.Parthiban
Qualificaion	MCA
Designation	Team Member
Department	Software Quality Assurance
Basic Pay	8650.00
Date of Birth	14-mar-1981

Updating Employee Details


Employee Details - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8080/UpdtViewListEmp.jsp
Go Links
100% TECHNOLOGIES
Done
My Computer
start VPN Employee Details - Mi...

Management System

Add
Update
View
Delete

□ Qualification MCA

□ Designation Team Member

□ Department Software Quality Assurance

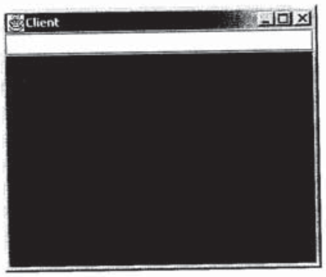
☑ Contact Number 9865085056

□ Mail ID parthi_acme@yahoo.com

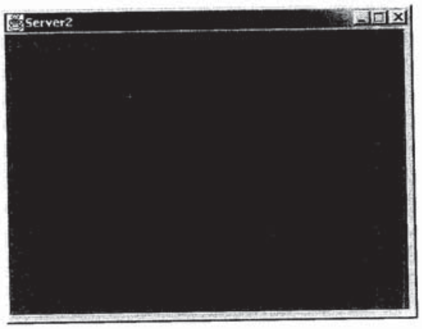
□ Address #22, Sakthi Nagar, Chindamani Trichy

Update Cancel

Attempting to obtain Virtual Connection



Server started at other end



REFERENCES

1. Bruce Schneier, (2001) 'Applied Cryptography', Second Edition, John Wiley and Sons Publications.

2. John Mairs,(2002) 'VPNs A Beginner's Guide', Tata McGraw-Hill Publishing Company Limited.

3. William Stallings, (2000) 'Data and Computer Communications', Seventh Edition, Asoke K. Ghosh Publications

WEBSITES

1. http://pkgsrc.se/wip/l2tp
   - Layer Two Tunneling Protocol Concepts
2. www.microsoft.com/windows2000/techinfo/howitworks.com
   - Virtual Private Network
3. www.virtualprivatenetwork.tunnel.com
   - Tunneling Concepts