INTERNET BANKING IN NEPAL

(A Case Study on Nepalese Government Bank)

Submitted by :

Umesh Maharjan

Shanker Dev Campus

Roll No. 1163/062

T.U. Registration No : 5-1-29-013-96

Thesis Submitted to :

Office of the Dean

Faculty of Management

Tribhuvan University

In Partial Fulfillment of the Requirements of Degree of

Master in Business Studies (MBS)

Putalisadak, Kathmandu

September, 2009

RECOMMENDATION

This is to certify that the thesis entitled

INTERNET BANKING IN NEPAL

(A Case Study in Nepalese Government Bank)

Submitted by

Umesh Maharjan

has been prepared as approved by this department in the prescribed format of Faculty of Management. Thesis is forwarded for examination.

……	……	…….....……
Shree Bhadra Neupane	Prof. Bisheshwor Man Shrestha	Prof. Dr. Kamal Deep Dhakal
(Thesis Supervisor)	(Head, Research Dept.)	(Campus Chief)

……

Shankar Adhikari

(Thesis Supervisor)

VIVA-VOCE SHEET

We have conducted the viva voce examination of the thesis presented by

Umesh Maharjan

T.U. Regd. No: 5-1-29-013-96

Entitled :

INTERNET BANKING IN NEPAL

(A Case Study in Nepalese Government Bank)

and found the thesis to be the original work of student and written according to the prescribed format. We recommend thesis to be accepted as partial fulfillment of the requirements for Master's Degree in Business Studies (MBS)

Viva Voce Committee

Head of Research Department : …….

Member (Thesis Supervisor) : …….

Member (Thesis Supervisor) : …….

Member (External Expert) : …….

Tribhuvan University

Faculty of Management

DECLARATION

I here by declare that that thesis entitled "**INTERNET BANKING IN NEPAL : A Case Study on Nepalese Government Banks**" submitted to Shanker Dev Campus, Faculty of Management Tribhuvan University is my original work done in the form of partial fulfillment of the requirement for the Master's Degree in Business Studies (MBS) under the supervision of Mr. Shree Bhadra Neupane and Mr. Shankar Adhikari of Shanker Dev Campus.

Date : September 2009

……..

Umesh Maharjan

ACKNOWLEDGEMENT

I would like to acknowledge and extend my heartfelt gratitude to the Management of Shanker Dev Campus for providing Management Information System as specialization in Master in Business Studies which is also not providing by Central Campus of Tribhuvan University. And special thanks to my teachers Mr. Shankar Adhikari and Mr. Shree Bhadra Neupane who guided me during this thesis.

I have chosen the topic "**INTERNET BANKING IN NEPAL : A Case Study on Nepalese Government Bank**" which is not possible to complete without having support of Nepalese Government Bank so I would like to thanks both NRB and RBB for providing me visit there system and provide me information about them, my special thanks to Mr. Naresh Man Maharjan of Nepal Rastriya Bank.

I wish to express my greatest appreciation and gratitude to my teacher Mr. Roshan Regmi who provide me lots of information about Internet Banking and NBL.

Last not the least, all my well wishers, my family and my dear friends I am indebted by your support and courage through out this thesis and MBS.

Thank You
Umesh Maharjan
T.U. Regd. No: 5-1-29-013-96

Table of Contents

List of Tables

List of Figures

ABBREVIATIONS

2 FA	: 2-Factor Authentication
ATM	: Automated Teller Machine
BSA	: Bank Secrecy Act
CCA	: Controller of Certification Authority
CVC	: Central Vigilance Commissioner
DES	: Data Encryption Standard
DNA	: Deoxyribonucleic Acid
DNS	: Domain Name System
EACBP	: Examiners Are Curious, Bright People
ECS	: Electronic Clearing Services
EDI	: Electronic Data Interchange
EDPC	: Electronic Data Processing Center
FDIC	: Federal Deposit Insurance Corporation
FFIEC	: Federal Financial Institutions Examination Council
GB	: Giga Bytes
HLCIT	: High Level Commission for Information Technology
http	: Hyper Text Transfer Protocol
IBM	: International Business Machine
ICT	: Information and Communication Technology
ISACA	: Information Systems Audit and Control Association
ISP	: Internet Service Provider
IT	: Information Technology
MBS	: Master in Business Studies
MIS	: Management Information System
NBL	: Nepal Bank Limited
NCC	: National Computer Center
OCC	: Office of the Comptroller of the Currency
OFAC	: Office of Foreign Asset Control
OS	: Operating System
OTP	: One-Time Password
PC	: Personal Computer

PC	: Personal Computer
PFM	: Personal Financial Manager
PIN	: Personal Identification Number
PKC	: Public Key Cryptography
RAID	: Redundant Array of Independent Disks
RBB	: Rastriya Banijya Bank
RONAST	: Royal Nepal Academy for Science and Technology
SARs	: Suspicious Activity Reports
SKC	: Secret Key Cryptography
SQL	: Structured Query Language
SSL	: Secure Socket Layer
SWOT	: Strength, Weakness, Opportunity, Threat
TV	: Television
UAT	: User Acceptance Testing
URL	: Uniform Resource Locator
US	: United States
www	: World Wide Web

Chapter I
INTRODUCTION

1.1 Background

This research is the effort for study and analyzing the Internet Banking in Nepalese government Bank. Internet Banking can be defined as the use of technology to communicate instructions to and receive information from a financial institution where an account is held. Internet Banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business or obtain information on financial products and services through a public or private network, including the Internet.

Since the launch of Internet the large planet has become a smaller one. It has rendered enormous impacts on business sectors. Remarkable development in Information and Communication Technology (ICT) has introduced a global revolution in banking industry. The global trend in business arena set some challenge that cannot be fulfilled with the help of the traditional banking system.

The survey of current banking system in Nepal reveals the fact that it requires rapid modification and adaptation to keep harmony with the world economy business. It becomes more obvious by observing the increased number of customers in some modern bank while others are losing them.

The existing banking system in our country is slow and error-prone. In one hand, fails to meet the customers' demand and it causes some significant losses both for the banking authority and traders. E-Banking, on the other hand solves the above problems. Furthermore, it opens up some other salient aspects such as increased foreign trade and foreign investment.

Most plan allow customers to perform all routine transactions, such as account transfers, balance inquires, bill payments and stop payment requests everything but it's very easy to set up an account. We can access our account information anytime day or night and we can do it from anywhere. A few online banks update information in real time, while others do it daily.

1.2 Introduction of Origin and Growth of Bank in Nepal

The growth of banking in Nepal is not so long. In comparison with other developing or developed country, the institutional development in banking system of Nepal is far behind. Nepal had to wait for a long time to come to this present banking position. The origin of bank in Nepal and its beginning of growth is controversial.

Even though the specific date of the beginning of money and banking deal in Nepal is not obvious, it is speculated that during the reign of the King Manadev, the coin "Manank" and "Gunank" during the reign of the King Gunakamadev were in use.

After the establishment of Nepal Bank Limited on 30th Karkik, 1994 (1938), modern banking system started in Nepal. Under the Nepal Rastra Bank Act 2012 (1956), Nepal Rastra Bank was established in 2013(1957) Baisakh 14th in Nepal. But this act has been repealed and the Nepal Rastra Bank Act 2058(2002) has been enacted by the parliament. After its establishment, it issued the Nepali notes on 7th Falgun 2016 for the first time.

Gradually, bank develop their services in Nepal according to requirement of customers and to compete market so today we can transact via non cash elements : like Internet Banking, Credit Card, ATM Card and SMS banking etc.

1.3 Nepal's ICT Background

Nations worldwide have recognized development opportunities and challenges of the emerging information age characterized by Information and Communication Technologies (ICT). These technologies are driving national development efforts worldwide and a number of countries in both developing and the developed world are exploring ways of facilitating their development process through development, deployment and the exploitation of ICT within their economies and societies.

Nepal's journey into the world of information technology began some three decades back with the use of IBM 1401 for the population census, 1971. Royal Nepal Academy for Science and Technology (RONAST), for the first time, used the internet. Mercantile Private Limited started email services for commercial purpose in June 1994. In 1995 government purchased the machine for further data processing in

the Bureau of Statistics and established a separate organization called Electronic Data Processing Center (EDPC) and after 6 years it converted to National Computer Center (NCC).

Government has formed High Level Commission for Information Technology (HLCIT), which is playing the role of facilitator between private and public sector in the development of ICT in Nepal.

1.4 Introduction of Organizations

1.4.1 Rastriya Banijya Bank (RBB)

RBB is fully government owned, and the largest commercial bank in Nepal. RBB was established on January 23, 1966 (Magh 10, 2022 BS) under the RBB Act. RBB provides various banking services to a wide range of customers including banks, insurance companies, industrial trading houses, airlines, hotels, and many other sectors.

RBB has Nepal's most extensive banking network with over 118 branches. Through its branch network, RBB has been contributing to Nepal's economic development by providing banking services throughout the country.

RBB has many correspondent arrangements with major international banks all over the world that facilitate trade finance, bank-originated personal funds transfers and inter bank funds transfer via SWIFT. In a bid to promote remittance business, RBB works with Western Union and International Money Express, two leading person-to-person funds transfer networks.

In addition RBB runs various programmes i.e. Banking with the Poor, Micro Credit project for Women etc. to enhance the living standard of people as per the government directives. As well, RBB actively delivers various government programs to people living in remote parts of the country; these programs are intended to raise living standards.

1.4.2 Nepal Bank Limited (NBL)

Nepal Bank Limited, the first bank of Nepal was established in November 15, 1937 A.D (Kartik 30, 1994). It was formed under the principle of Joint venture (Joint venture between govt. & general public). NBL's authorized capital was Rs. 10 million & issued capital Rs. 2.5 million of which paid-up capital was Rs. 842 thousand with 10 shareholders. The bank has been providing banking through its branch offices in the different geographical locations of the country. Its vision statement is "To remain the leading financial institution of the country." Its mission statement is "Nepal Bank Limited seeks to provide an environment within which the bank can bring unique financial value and services to all customers. It will be a sound institution where depositors continue to have faith in the security of their funds and receive reasonable returns; borrowers are assured of appropriate credit facilities at reasonable prices; other service- seekers receive prompt and attentive service at reasonable cost; employees are paid adequate compensation with professional career growth opportunities and stockholders receive satisfactory return for their investment".

Its values statement: At Nepal Bank Limited, we believe that our banking should be based on:

- Respect, service and safety for the customers we serve
- Respect, reward and opportunity for the people with whom we work
- Respect, cooperation and support for the economic community of Nepal

NBL's objectives are :

- Continue to maintain leading share of banking sector with a significant presence in all major geographical areas in the country.
- Provide competitive and customer oriented banking services to all customers through competent and professional staff.
- Reclaim leadership within the national financial community.

1.5 Introduction of Internet Banking

“Internet banking” refers to systems that enable bank customers to access accounts and general information on bank products and services through a personal computer (PC) or other intelligent device (bankrate.com;2007).

Internet banking products and services can include wholesale products for corporate customers as well as retail and fiduciary products for consumers. Ultimately, the products and services obtained through Internet banking may mirror products and services offered through other bank delivery channels. Some examples of wholesale products and services include:

- Cash management.
- Wire transfer.
- Automated clearinghouse (ACH) transactions.
- Bill presentment and payment.

Examples of retail and fiduciary products and services include:

- Balance inquiry.
- Funds transfer.
- Downloading transaction information.
- Bill presentment and payment.
- Loan applications.
- Investment activity.
- Other value-added services.

Other Internet banking services may include providing Internet access as an Internet Service Provider (ISP). The OCC has determined that a national bank subsidiary may provide home banking services through an Internet connection to the bank’s home banking system and, incidental to that service, may also provide Internet access to bank customers using that service. Historically, banks have used information systems technology to process checks (item processing), drive ATM machines (transaction processing), and produce reports (management information systems). In the past, the computer systems that made the information systems operate were rarely noticed by

customers. Today, Web sites, electronic mail, and electronic bill presentment and payment systems are an important way for banks to reach their customers.

1.6 Statement of the Problem

Establishing Internet Banking infrastructure has been a challenging task for the developing countries like Nepal. In the context of Nepal there are ample of problems in Internet Banking some of them are given below :

- Computer and Banking Literacy : In aggregate here is low level of IT literacy. Very few people are computer literate in Nepal and very few people understand banking system or banking process even educated people also there.
- Infrastructure Development : Though banks reach with their services in rural area ISP or NTC services is not available there for internet services and vice versa.
- Security : Security of a transaction, authenticity of a deal, identification of a customer etc are important technological and systems issues, which are major sources of concern to e-banking. Customers are afraid from online attack. Various online attacks are also available.

1.7 Objectives of the Study

The main objectives of proposed research are to study, analyze and understand the Internet Banking of Nepal Bank Limited. Some of the other objectives are as follows :

- To identify the problems in existing Internet Banking services of Nepal
- Are public satisfy or not from Internet banking Services ? If not what will be the effective service delivery mechanism.
- To identify the prerequisites to get the Internet Banking services
- The research tell prerequisites to get Internet Banking services (for e.g. Computers, telephones, internet, customer should be account holder of bank)
- To examine the service delivery of different banks of Nepal
- The research includes various types of Internet Banking services provided by different banks' to general public.

1.8 Scope of the Study

The study will be mainly focused on three components of the study area :

- Social aspects : In social aspect the studied is focus on public participation according to their satisfaction, knowledge, beliefs, values etc.
- Technical aspects : This aspects is concerned with the technically how to develop system and technology used on projects.
- Economic aspects : In the economic analysis part, the study will focus on the possible areas of economic development by using this Internet Banking.

1.9 Limitation of the Study

This research is the small effort for study and analyzing the Internet Banking services of Nepal which has limited time so it cannot focus on all areas and may not be able to explore many fields. This research work is done within limited time frame during the MBS dissertation. There are so many constraints while doing the work such as inadequate time, load shedding, and resources etc. To understand methodology of Internet Banking service is very difficult because banks only provide surface level of information because of their security concern.

In spite of great effort, there are many limitations of this research work. The major limitations are as follows :

- In the field of E-banking, there are so many arenas like ATM, Tele Banking, Mobile Banking etc. but this research does not focus on all the e-banking services. Research works mainly focus on Internet Banking.
- Fund transfer is possible within the branch of bank. It means once cannot transfer amount from one bank to another bank.
- Banks have their own policy but there is no any standard policy for Internet Banking in Nepal.
- In the field of Internet Banking security is must but this research doe not cover all the aspects of security.
- General customers and corporate customers of Internet Banking system have same kinds of facilities.

1.10 Organization of the Study

This study is organized and decorated in seven chapters. Each chapter and unit will be on a prescribed format of thesis writing to the partial fulfillment of MBS program. Each unit gives the clear picture or roadmap of the study.

Chapter I : INTRODUCTION

This chapter deals with “Introduction of The Study”. In this chapter, separated unit for background, significances objective and limitation of the study has mentioned.

Chapter II : REVIEW OF THE LITERATURE

This chapter focused “Review of Literature”. In this chapter, various relevant such as different books, journals, article, websites and previous thesis mention has mentioned.

Chapter III : METHODOLOGY

Third chapter presented “Research Methodology”. In this chapter, research design, sources of the data, method of data collection and analysis has mentioned.

Chapter IV : ANALYSIS OF SYSTEM

This chapter deals with “Analysis of Internet Banking” and "Internet Banking Security". This chapter provides the different analysis like strength, weakness, opportunity, threat (SWOT) analysis and feasibility analysis of Internet banking. Security in Internet Banking comprises both the computer and communication security. Therefore this chapter consist different security principles, cryptographic key management, RAID etc.

Chapter V : CONCLUSION AND RECOMMENDATION

Fifth chapter presented with “Conclusions and Recommendation” of the Study.

Chapter II
LITERATURE REVIEW

The review of literature is the study of various literatures related to the topic. This chapter constitutes the review of literature in two aspects : the conceptual framework, and related studies from various books, journals, articles, research reports and thesis.

A literature review is an account of what has been published on a topic by accredited scholars and researchers.

2.1 Conceptual Background

Meaning of Bank

Bank is a "business establishment, in which money is kept for saving or commercial purpose or is invested, supplied for loans, or exchanged" [The American Heritage® Dictionary of English Language1]. Banking is "the business of operating a bank" [Cambridge Dictionary2]. A financial institution is a facilitator between the payer and the payee, a provider of credit and an intermediary between the investor and markets. The role of financial institutions is to transfer information and risk: they invest (transfer, buy and sell) wealth that they govern, from which they gain profit. Banking is mainly transference of money in electronic form, which is one reason why banking services are suitable for internet. In general level electronic banking service is the service provided by a bank or financial institution, which enables the management of banking transactions and other banking services by a bank to its customers, via a computer, television or mobile phone" or complicatedly "an electronic connection between bank and customer in order to prepare manage and control financial transactions". Also terms such as "Internet Banking", "e-banking" and "telebanking" are used as synonyms for electronic banking. For regular consumers the term "Internet Banking" means banking services that are accessed over the internet with various terminals, such as personal computer, mobile phone or TV.

“New technology sometimes requires complex understanding and mental capability, and thus the technology may be difficult to manipulate due to limited capability of firm employees. Finally technology readiness of firm plays a role in their attitudes

towards technology. Technology readiness is conceptualized as a combination of positive and negative feelings towards technology, roughly people's confidence that technology helps improve their lives, or simply makes things more difficult and less secure." (*Chircu and Kauffman; 2002:14*)

The main advantage of that I have found in these researches regarding internet banking is that its availability 24 hours a day and 7 days a week .The main disadvantages of associated with direct banking, however, included its complexity and the security risks involved in using it.

The main issues that preventing the adoption of internet banking included the convenience aspects of the service ease of use and its compatibility with customer existing lifestyles.

2.2 Internet Banking

"Internet banking" refers to systems that enable bank customers to access accounts and general information on bank products and services through a personal computer (PC) or other intelligent device. Internet banking allows you to manage your finances from home, work or from just about anywhere in the world.

According to Michael Karlin, the President and Chief Operation Officer of the world's first virtual bank, Security First Network Bank, the idea of Internet Banking is as follows :

1. You do not have to purchase any software, store any data on your computer, backup any information, since all transactions occur on the bank server over the infrastructure of the Internet.

2. You will be able to conduct your banking services anywhere you like but you need to have a computer and a modem, no matter where you are (e.g. at home, at office, or in a place outside the country).

3. You can use the banking services 24 hours a day, 7 days a week, and 365 days a year. You no longer have to reconcile a bank statement or manually track your ATM and paper checks.

Internet banking products and services can include wholesale products for corporate customers as well as retail and fiduciary products for consumers. Ultimately, the products and services obtained through Internet banking may mirror products and services offered through other bank delivery channels.

Some examples of wholesale products and services include:

- Cash management.
- Wire transfer.
- Automated clearinghouse (ACH) transactions.
- Bill presentment and payment.

Examples of retail and fiduciary products and services include:

- Balance inquiry.
- Funds transfer.
- Downloading transaction information.
- Bill presentment and payment.
- Loan applications.
- Investment activity.
- Other value-added services.

Other Internet banking services may include providing Internet access as an Internet Service Provider (ISP). Historically, banks have used information systems technology to process checks (item processing), drive ATM machines (transaction processing), and produce reports (management information systems). In the past, the computer systems that made the information systems operate were rarely noticed by customers. Today, Web sites, electronic mail, and electronic bill presentment and payment systems are an important way for banks to reach their customers. National banks have experimented with various forms of online banking for many years. Some of the early experiments involved closed systems where the customers accessed banks through a dial-in or cable TV connection. These systems limited a bank's potential customer base because they required out-of area customers to either incur long-distance charges on their phone bills or subscribe to a particular cable TV service to access the bank. With the widespread growth of the Internet, customers can use this technology

anywhere in the world to access a bank's network. The Internet, as an enabling technology, has made banking products and services available to more customers and eliminated geographic and proprietary systems barriers. With an expanded market, banks also may have opportunities to expand or change their product and service offerings.

2.3 Benefits of Internet Banking

2.3.1 Benefits for Banks

Internet banking offers many benefits to banks and their customers. The main benefits to banks are cost savings, reaching new segments of the population, efficiency, enhancement of the bank's reputations and better customer service and satisfaction (*Jayawardhena and Foley, 2000*).

According to global survey conducted by Booz-Allen and Hamilton (1997), the establishment of specialized Internet Banking requires only US$1-2 million, which is lower than branch-based banking setup. The traditional bank's running costs account for 50% to 60% of its revenues, while the running costs of Internet Banking is estimated at 15% to 20% of its revenues.
(*http://www.bah.com/viewpoints/insights/bank_brickless.htm*)

Mols(1998) conducted a survey in Denmark argued that Internet Banking might be useful for strengthening cross-selling and price differentiation. Internet banking makes it possible for banks to offer consumer a variety of services 22/7. Internet banking is attractive because the consumer are more satisfied with their banks, are less price sensitive have the highest intention to repurchase, and provide more positive word of mouth information than other bank customers.

2.3.2 Benefits for Customers

Internet banking offers also new value to customers. The emergence of the internet has had a significant impact on the diffusion of electronic banking. With the help of the Internet, banking is no longer bound to time or geography. Consumers all over the world have relatively easy access to their accounts 24 hours per day; seven days a week. It makes available to customers a full range of services including some services not offered at branches. The greatest benefit of Internet banking is that it is cheap or even free to customers. However, price seemed to be one factor militating against Internet banking (*Sathye; 1999*). Two important factors in the price debate are on the one hand geographical differences and on the other hand disparities between the costs of e.g. Internet connections and telephone call pricing. It has also been argued that electronic banks are more likely to change in response to customers' demand (*Brogdon;1999*). Internet banking has the advantage that the customer avoids traveling to and from a bank branch. In this way, Internet banking saves time and money, provides convenience and accessibility, and has a positive impact on customer satisfaction (*Karjauloto; 2001*). Customers can manage their banking affairs when they want, and they can enjoy more privacy while interacting with their bank. It has been claimed that Internet banking offers the customer more benefits at lower costs (*Mols; 1998*).

Internet banking is extremely beneficial to customers because of the savings in costs, time and space it offers, its quick response to complaints, and its delivery of improved services, all of which benefits make fore easier banking (*Turban et al.; 2000:23*).

To summarize, electronic banking in general and Internet banking in particular offer many benefits to both service providers and their customers.

2.4 Growth in Internet Banking

Numerous factors — including competitive cost, customer service, and demographic considerations — are motivating banks to evaluate their technology and assess their electronic commerce and Internet banking strategies. Many researchers expect rapid growth in customers using online banking products and services. The challenge for

national banks is to make sure the savings from Internet banking technology more than offset the costs and risks associated with conducting business in cyberspace.

Marketing strategies will vary as national banks seek to expand their markets and employ lower cost delivery channels. Bankers will need to understand the strategies used and technologies employed on a bank-by-bank basis to assess the risk. Evaluating a bank's data on the use of their Web sites, may help bankers determine the bank's strategic objectives, how well the bank is meeting its Internet banking product plan, and whether the business is expected to be profitable.

Some of the market factors that may drive a bank's strategy include the following:

Competition — Studies show that competitive pressure is the chief driving force behind increasing use of Internet banking technology, ranking ahead of cost reduction and revenue enhancement, in second and third place respectively. Banks see Internet banking as a way to keep existing customers and attract new ones to the bank.

Cost Efficiencies — National banks can deliver banking services on the Internet at transaction costs far lower than traditional brick-and-mortar branches. The actual costs to execute a transaction will vary depending on the delivery channel used. For example, according to Booz, Allen & Hamilton, as of mid- 1999, the cost to deliver manual transactions at a branch was typically more than a dollar, ATM and call center transactions cost about 25 cents, and Internet transactions cost about a penny. These costs are expected to continue to decline.

National banks have significant reasons to develop the technologies that will help them deliver banking products and services by the most cost-effective channels. Many bankers believe that shifting only a small portion of the estimated 19-billion payments mailed annually in the U.S. to electronic delivery channels could save banks and other businesses substantial sums of money. However, national banks should use care in making product decisions.

Management should include in their decision making the development and ongoing costs associated with a new product or service, including the technology, marketing, maintenance, and customer support functions. This will help management exercise

due diligence, make more informed decisions, and measure the success of their business venture.

Geographical Reach — Internet banking allows expanded customer contact through increased geographical reach and lower cost delivery channels. In fact some banks are doing business exclusively via the Internet — they do not have traditional banking offices and only reach their customers online.

Other financial institutions are using the Internet as an alternative delivery channel to reach existing customers and attract new customers.

Branding — Relationship building is a strategic priority for many national banks. Internet banking technology and products can provide a means for national banks to develop and maintain an ongoing relationship with their customers by offering easy access to a broad array of products and services.

By capitalizing on brand identification and by providing a broad array of financial services, banks hope to build customer loyalty, cross-sell, and enhance repeat business.

Customer Demographics — Internet banking allows national banks to offer a wide array of options to their banking customers. Some customers will rely on traditional branches to conduct their banking business. For many, this is the most comfortable way for them to transact their banking business. Those customers place a premium on person-to-person contact. Other customers are early adopters of new technologies that arrive in the marketplace. These customers were the first to obtain PCs and the first to employ them in conducting their banking business. The demographics of banking customers will continue to change. The challenge to national banks is to understand their customer base and find the right mix of delivery channels to deliver products and services profitably to their various market segments.

2.5 Types of Internet Banking

Understanding the various types of Internet banking products will help examiners assess the risks involved. Currently, the following three basic kinds of Internet banking are being employed in the marketplace:

- **Informational** — This is the basic level of Internet banking. Typically, the bank has marketing information about the bank's products and services on a stand-alone server. The risk is relatively low, as informational systems typically have no path between the server and the bank's internal network. This level of Internet banking can be provided by the bank or outsourced. While the risk to a bank is relatively low, the server or Web site may be vulnerable to alteration. Appropriate controls therefore must be in place to prevent unauthorized alterations to the bank's server or Web site.
- **Communicative** — This type of Internet banking system allows some interaction between the bank's systems and the customer. The interaction may be limited to electronic mail, account inquiry, loan applications, or static file updates (name and address changes). Because these servers may have a path to the bank's internal networks, the risk is higher with this configuration than with informational systems. Appropriate controls need to be in place to prevent, monitor, and alert management of any unauthorized attempt to access the bank's internal networks and computer systems. Virus controls also become much more critical in this environment.
- **Transactional** — This level of Internet banking allows customers to execute transactions. Since a path typically exists between the server and the bank's or outsourcer's internal network, this is the highest risk architecture and must have the strongest controls. Customer transactions can include accessing accounts, paying bills, transferring funds, etc.

2.6 Internet Banking Risks

Internet banking creates new risk control challenges for national banks. From a supervisory perspective, risk is the potential that events, expected or unexpected, may have an adverse impact on the bank's earnings or capital. The OCC has defined nine categories of risk for bank supervision purposes. The risks are credit, interest rate, liquidity, price, foreign exchange, transaction, compliance, strategic, and reputation. These categories are not mutually exclusive and all of these risks are associated with Internet banking.

- **Credit Risk -** Credit risk is the risk to earnings or capital arising from an obligor's failure to meet the terms of any contract with the bank or otherwise

to perform as agreed. Credit risk is found in all activities where success depends on counterparty, issuer, or borrower performance. It arises any time bank funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether on or off the banks balance sheet. Internet banking provides the opportunity for banks to expand their geographic range. Customers can reach a given institution from literally anywhere in the world. In dealing with customers over the Internet, absent any personal contact, it is challenging for institutions to verify the bonafides of their customers, which is an important element in making sound credit decisions. Verifying collateral and perfecting security agreements also can be challenging with out-of-area borrowers. Unless properly managed, Internet banking could lead to a concentration in out-of-area credits or credits within a single industry.

Moreover, the question of which state's or country's laws control an Internet relationship is still developing. Effective management of a portfolio of loans obtained through the Internet requires that the board and management understand and control the bank's lending risk profile and credit culture. They must assure that effective policies, processes, and practices are in place to control the risk associated with such loans.

- **Interest Rate Risk** - Interest rate risk is the risk to earnings or capital arising from movements in interest rates. From an economic perspective, a bank focuses on the sensitivity of the value of its assets, liabilities and revenues to changes in interest rates.

Interest rate risk arises from differences between the timing of rate changes and the timing of cash flows (repricing risk); from changing rate relationships among different yield curves affecting bank activities (basis risk); from changing rate relationships across the spectrum of maturities (yield curve risk); and from interest-related options embedded in bank products (options risk). Evaluation of interest rate risk must consider the impact of complex, illiquid hedging strategies or products, and also the potential impact that changes in interest rates will have on fee income. In those situations where

trading is separately managed, this refers to structural positions and not trading portfolios.

Internet banking can attract deposits, loans, and other relationships from a larger pool of possible customers than other forms of marketing. Greater access to customers who primarily seek the best rate or term reinforces the need for managers to maintain appropriate asset/liability management systems, including the ability to react quickly to changing market conditions.

- **Liquidity Risk -** Liquidity risk is the risk to earnings or capital arising from a bank's inability to meet its obligations when they come due, without incurring unacceptable losses. Liquidity risk includes the inability to manage unplanned changes in funding sources. Liquidity risk also arises from the failure to recognize or address changes in market conditions affecting the ability of the bank to liquidate assets quickly and with minimal loss in value.

  Internet banking can increase deposit volatility from customers who maintain accounts solely on the basis of rate or terms. Asset/liability and loan portfolio management systems should be appropriate for products offered through Internet banking. Increased monitoring of liquidity and changes in deposits and loans may be warranted depending on the volume and nature of Internet account activities.

- **Price Risk -** Price risk is the risk to earnings or capital arising from changes in the value of traded portfolios of financial instruments. This risk arises from market making, dealing, and position taking in interest rate, foreign exchange, equity, and commodities markets. Banks may be exposed to price risk if they create or expand deposit brokering, loan sales, or securitization programs as a result of Internet banking activities. Appropriate management systems should be maintained to monitor, measure, and manage price risk if assets are actively traded.

- **Foreign Exchange Risk** - Foreign exchange risk is present when a loan or portfolio of loans is denominated in a foreign currency or is funded by borrowings in another currency. In some cases, banks will enter into multi-

currency credit commitments that permit borrowers to select the currency they prefer to use in each rollover period. Foreign exchange risk can be intensified by political, social, or economic developments. The consequences can be unfavorable if one of the currencies involved becomes subject to stringent exchange controls or is subject to wide exchange-rate fluctuations.

Banks may be or exposed to foreign exchange risk if they accept deposits from non-U.S. residents create accounts denominated in currencies other than U.S. dollars. Appropriate systems should be developed if banks engage in these activities.

- **Transaction Risk** - Transaction risk is the current and prospective risk to earnings and capital arising from fraud, error, and the inability to deliver products or services, maintain a competitive position, and manage information. Transaction risk is evident in each product and service offered and encompasses product development and delivery, transaction processing, systems development, computing systems, complexity of products and services, and the internal control environment.

  A high level of transaction risk may exist with Internet banking products, particularly if those lines of business are not adequately planned, implemented, and monitored. Banks that offer financial products and services through the Internet must be able to meet their customers' expectations. Banks must also ensure they have the right product mix and capacity to deliver accurate, timely, and reliable services to develop a high level of confidence in their brand name.

  Customers who do business over the Internet are likely to have little tolerance for errors or omissions from financial institutions that do not have sophisticated internal controls to manage their Internet banking business. Likewise, customers will expect continuous availability of the product and Web pages that are easy to navigate.

  Software to support various Internet banking functions is provided to the customer from a variety of sources. Banks may support customers using

customer-acquired or bank-supplied browsers or Personal Financial Manager (PFM) software. Good communications between banks and their customers will help manage expectations on the compatibility of various PFM software products.

Attacks or intrusion attempts on banks' computer and network systems are a major concern. Studies show that systems are more vulnerable to internal attacks than external, because internal system users have knowledge of the system and access. Banks should have sound preventive and detective controls to protect their Internet banking systems from exploitation both internally and externally.

Contingency and business resumption planning is necessary for banks to be sure that they can deliver products and services in the event of adverse circumstances. Internet banking products connected to a robust network may actually make this easier because back up capabilities can be spread over a wide geographic area. For example, if the main server is inoperable, the network could automatically reroute traffic to a back up server in a different geographical location. Security issues should be considered when the institution develops its contingency and business resumption plans. In such situations, security and internal controls at the back-up location should be as sophisticated as those at the primary processing site. High levels of system availability will be a key expectation of customers and will likely differentiate success levels among financial institutions on the Internet.

National banks that offer bill presentment and payment will need a process to settle transactions between the bank, its customers, and external parties. In addition to transaction risk, settlement failures could adversely affect reputation, liquidity, and credit risk.

- **Compliance Risk -** Compliance risk is the risk to earnings or capital arising from violations of, or nonconformance with, laws, rules, regulations, prescribed practices, or ethical standards. Compliance risk also arises in situations where the laws or rules governing certain bank products or activities of the bank's clients may be ambiguous or untested. Compliance risk exposes

the institution to fines, civil money penalties, payment of damages, and the voiding of contracts.

Compliance risk can lead to a diminished reputation, reduced franchise value, limited business opportunities, reduced expansion potential, and lack of contract enforceability.

Most Internet banking customers will continue to use other bank delivery channels. Accordingly, national banks will need to make certain that their disclosures on Internet banking channels, including Web sites, remain synchronized with other delivery channels to ensure the delivery of a consistent and accurate message to customers.

Federal consumer protection laws and regulations, including CRA and Fair Lending, are applicable to electronic financial services operations including Internet banking. Moreover, it is important for national banks to be familiar with the regulations that permit electronic delivery of disclosures/notices versus those that require traditional hard copy notification. National banks should carefully review and monitor all requirements applicable to electronic products and services and ensure they comply with evolving statutory and regulatory requirements.

Advertising and record-keeping requirements also apply to banks' Web sites and to the products and services offered. Advertisements should clearly and conspicuously display the FDIC insurance notice, where applicable, so customers can readily determine whether a product or service is insured.

Regular monitoring of bank Web sites will help ensure compliance with applicable laws, rules, and regulations.

Application of Bank Secrecy Act (BSA) requirements to cyber banking products and services is critical. The anonymity of banking over the Internet poses a challenge in adhering to BSA standards. Banks planning to allow the establishment of new accounts over the Internet should have rigorous account opening standards. Also, the

bank should set up a control system to identify unusual or suspicious activities and, when appropriate, file suspicious activity reports (SARs).

The BSA funds transfer rules also apply to funds transfers or transmittals performed over the Internet when transactions exceed $3,000 and do not meet one of the exceptions. The rules require banks to ensure that customers provide all the required information before accepting transfer instructions. The record keeping requirements imposed by the rules allow banks to retain written or electronic records of the information.

The Office of Foreign Asset Control (OFAC) administers laws that impose economic sanctions against foreign nations and individuals. This includes blocking accounts and other assets and prohibiting financial transactions. Internet banking businesses must comply with OFAC requirements. A bank needs to collect enough information to identify customers and determine whether a particular transaction is prohibited under OFAC rules.

- **Strategic Risk -** Strategic risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes. This risk is a function of the compatibility of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals, and the quality of implementation. The resources needed to carry out business strategies are both tangible and intangible. They include communication channels, operating systems, delivery networks, and managerial capacities and capabilities. The organization's internal characteristics must be evaluated against the impact of economic, technological, competitive, regulatory, and other environmental changes.

  Management must understand the risks associated with Internet banking before they make a decision to develop a particular class of business. In some cases, banks may offer new products and services via the Internet. It is important that management understand the risks and ramifications of these decisions.

Sufficient levels of technology and MIS are necessary to support such a business venture. Because many banks will compete with financial institutions beyond their existing trade area, those engaging in Internet banking must have a strong link between the technology employed and the bank's strategic planning process.

Before introducing an Internet banking product, management should consider whether the product and technology are consistent with tangible business objectives in the bank's strategic plan. The bank also should consider whether adequate expertise and resources are available to identify, monitor, and control risk in the Internet banking business. The planning and decision making process should focus on how a specific business need is met by the Internet banking product, rather than focusing on the product as an independent objective. The bank's technology experts, along with its marketing and operational executives, should contribute to the decision making and planning process. They should ensure that the plan is consistent with the overall business objectives of the bank and is within the bank's risk tolerance. New technologies, especially the Internet, could bring about rapid changes in competitive forces. Accordingly, the strategic vision should determine the way the Internet banking product line is designed, implemented, and monitored.

- **Reputation Risk -** Reputation risk is the current and prospective impact on earnings and capital arising from negative public opinion. This affects the institution's ability to establish new relationships or services or continue servicing existing relationships. This risk may expose the institution to litigation, financial loss, or a decline in its customer base. Reputation risk exposure is present throughout the organization and includes the responsibility to exercise an abundance of caution in dealing with customers and the community.

  A bank's reputation can suffer if it fails to deliver on marketing claims or to provide accurate, timely services. This can include failing to adequately meet customer credit needs, providing unreliable or inefficient delivery systems, untimely responses to customer inquiries, or violations of customer privacy

expectations. A bank's reputation can be damaged by Internet banking services that are poorly executed or otherwise alienate customers and the public. Well designed marketing, including disclosures, is one way to educate potential customers and help limit reputation risk. Customers must understand what they can reasonably expect from a product or service and what special risks and benefits they incur when using the system. As such, marketing concepts need to be coordinated closely with adequate disclosure statements. A national bank should not market the bank's Internet banking system based on features or attributes the system does not have. The marketing program must present the product fairly and accurately. National banks should carefully consider how connections to third parties are presented on their Web sites. Hypertext links are often used to enable a customer to link to a third party. Such links may reflect an endorsement of the third party's products or services in the eyes of the customer. It should be clear to the customer when they have left the bank's Web site so that there is no confusion about the provider of the specific products and services offered or the security and privacy standards that apply. Similarly, adequate disclosures must be made so that customers can distinguish between insured and noninsured products.

National banks need to be sure that their business continuity plans include the Internet banking business. Regular testing of the business continuity plan, including communications strategies with the press and public, will help the bank ensure it can respond effectively and promptly to any adverse customer or media reactions.

2.7 Risk Management

Financial institutions should have a technology risk management process to enable them to identify, measure, monitor, and control their technology risk exposure. Risk management of new technologies has three essential elements:

- The planning process for the use of the technology.
- Implementation of the technology.
- The means to measure and monitor risk.

The OCC's objective is to determine whether a bank is operating its Internet banking business in a safe and sound manner. The OCC expects banks to use a rigorous analytic process to identify, measure, monitor, and control risk. Examiners will determine whether the level of risk is consistent with the bank's overall risk tolerance and is within the bank's ability to manage and control.

The risk planning process is the responsibility of the board and senior management. They need to possess the knowledge and skills to manage the bank's use of Internet banking technology and technology-related risks. The board should review, approve, and monitor Internet banking technology-related projects that may have a significant impact on the bank's risk profile. They should determine whether the technology and products are in line with the bank's strategic goals and meet a need in their market. Senior management should have the skills to evaluate the technology employed and risks assumed.

Periodic independent evaluations of the Internet banking technology and products by auditors or consultants can help the board and senior management fulfill their responsibilities. Implementing the technology is the responsibility of management. Management should have the skills to effectively evaluate Internet banking technologies and products, select the right mix for the bank, and see that they are installed appropriately. If the bank does not have the expertise to fulfill this responsibility internally, it should consider contracting with a vendor who specializes in this type of business or engaging in an alliance with another provider with complementary technologies or expertise.

Measuring and monitoring risk is the responsibility of management. Management should have the skills to effectively identify, measure, monitor, and control risks associated with Internet banking. The board should receive regular reports on the technologies employed, the risks assumed, and how those risks are managed. Monitoring system performance is a key success factor. As part of the design process, a national bank should include effective quality assurance and audit processes in its Internet banking system. The bank should periodically review the systems to determine whether they are meeting the performance standards.

2.8 Internal Controls

Internal controls over Internet banking systems should be commensurate with an institution's level of risk. As in any other banking area, management has the ultimate responsibility for developing and implementing a sound system of internal controls over the bank's Internet banking technology and products. Regular audits of the control systems will help ensure that the controls are appropriate and functioning properly. For example, the control objectives for an individual bank's Internet banking technology and products might focus on:

- Consistency of technology planning and strategic goals, including efficiency and economy of operations and compliance with corporate policies and legal requirements.
- Data availability, including business recovery planning.
- Data integrity, including providing for the safeguarding of assets, proper authorization of transactions, and reliability of the process and output.
- Data confidentiality and privacy safeguards.
- Reliability of MIS.

Once control objectives are established, management has the responsibility to install the necessary internal controls to see that the objectives are met. Management also has the responsibility to evaluate the appropriateness of the controls on a cost-benefit basis. That analysis may take into account the effectiveness of each control in a process, the dollar volume flowing through the process, and the cost of the controls.

According to the Information Systems Audit and Control Association (ISACA) the basic internal control components include:

- Internal accounting controls — Used to safeguard the assets and reliability of financial records. These would include transaction records and trial balances
- Operational controls — Used to ensure that business objectives are being met. These would include operating plans and budgets to compare actual against planned performance.

- Administrative controls — Used to ensure operational efficiency and adherence to policies and procedures. These would include periodic internal and external audits.

ISACA separates internal controls into three general categories. The three control categories can be found in the basic internal controls discussed above.

- Preventive Controls — Prevent something (often an error or illegal act) from happening. An example of this type of control is logical access control software that would allow only authorized persons to access a network using a combination of a user ID and password.
- Detective Controls — Identify an action that has occurred. An example would be intrusion detection software that triggers an alert or alarm.
- Corrective Controls — Correct a situation once it has been detected. An example would be software backups that could be used to recover a corrupted file or database.

Banks or service providers offering transaction-based Internet banking products need to have a high level of controls to help manage the bank's transaction risk. Examples of these controls could include:

- Monitoring transaction activity to look for anomalies in transaction types, transaction volumes, transaction values, and time-of-day presentment.
- Monitoring log-on violations or attempts to identify patterns of suspect activity including unusual requests, unusual timing, or unusual formats.
- Using trap and trace techniques to identify the source of the request and match these against known customers.

Regular reporting and review of unusual transactions will help identify:

- Intrusions by unauthorized parties.
- Customer input errors.
- Opportunities for customer education.

2.9 Issues in Internet Banking

Financial institutions, their card associations, and vendors are working to develop an Internet payment infrastructure to help make electronic commerce secure. Many in the banking industry expect significant growth in the use of the Internet for the purchase of goods and services and electronic data interchange. The banking industry also recognizes that the Internet must be secure to achieve a high level of confidence with both consumers and businesses.

Sound management of banking products and services, especially those provided over the Internet, is fundamental to maintaining a high level of public confidence not only in the individual bank and its brand name but also in the banking system as a whole. Key components that will help maintain a high level of public confidence in an open network environment include:

- Security
- Authentication
- Trust
- Nonrepudiation
- Privacy
- Availability

Security is an issue in Internet banking systems. The OCC expects national banks to provide a level of logical and physical security commensurate with the sensitivity of the information and the individual bank's risk tolerance. Some national banks allow for direct dial-in access to their systems over a private network while others provide network access through the Internet.

Although the publicly accessible Internet generally may be less secure, both types of connections are vulnerable to interception and alteration. For example, hardware or software "sniffers" can obtain passwords, account numbers, credit card numbers, etc. without regard to the means of access.

National banks therefore must have a sound system of internal controls to protect against security breaches for all forms of electronic access. A sound system of

preventive, detective, and corrective controls will help assure the integrity of the network and the information it handles.

Firewalls are frequently used on Internet banking systems as a security measure to protect internal systems and should be considered for any system connected to an outside network. Firewalls are a combination of hardware and software placed between two networks through which all traffic must pass, regardless of the direction of flow. They provide a gateway to guard against unauthorized individuals gaining access to the bank's network.

The mere presence of a firewall does not assure logical security and firewalls are not impenetrable: firewalls must be configured to meet a specific operating environment and they must be evaluated and maintained on a regular basis to assure their effectiveness and efficiency. Individuals who are technically competent must perform the installation, configuration, evaluation, and maintenance of firewalls. The specific risks involved may require a broad range of security controls.

Authentication is another issue in an Internet banking system. Transactions on the Internet or any other telecommunication network must be secure to achieve a high level of public confidence. In cyberspace, as in the physical world, customers, banks, and merchants need assurances that they will receive the service as ordered or the merchandise as requested, and that they know the identity of the person they are dealing with.

Banks typically use symmetric (private key) encryption technology to secure messages and asymmetric (public/private key) cryptography to authenticate parties. Asymmetric cryptography employs two keys — a public key and a private key. These two keys are mathematically tied but one key cannot be deduced from the other. For example, to authenticate that a message came from the sender, the sender encrypts the message using their private key. Only the sender knows the private key. But, once sent, the message can be read only using the sender's public key. Since the message can only be read using the sender's public key, the receiver knows the message came from the expected sender.

Internet banking systems should employ a level of encryption that is appropriate to the level or risk present in the systems. OCC is aware that stronger levels of encryption may slow or degrade performance and, accordingly, management must balance security needs with performance and cost issues. Thus, a national bank should conduct a risk assessment in deciding upon its appropriate level of encryption. The OCC does not mandate a particular strength or type of encryption. Rather, it expects management to evaluate security risks, review the cost and benefit of different encryption systems, and decide on an appropriate level of encryption as a business decision. Management should be able to explain the supporting analysis for their decision.

A common asymmetric cryptography system is RSA, which uses key lengths up to 1,024 bits. By using the two forms of cryptography together, symmetric to protect the message and asymmetric to authenticate the parties involved, banks can secure the message and have a high level of confidence in the identity of the parties involved.

Biometric devices are an advanced form of authentication. These devices may take the form of a retina scan, finger or thumb print scan, facial scan, or voiceprint scan. Use of biometrics is not yet considered mainstream, but may be used by some banks for authentication. Bankers should evaluate biometric activities based on management's understanding of risks, internal or external reviews, and the overall performance of these devices.

Trust is another issue in Internet banking systems. Public and private key cryptographic systems can be used to secure information and authenticate parties in transactions in cyberspace. A trusted third party is a necessary part of the process. That third party is the *certificate authority*.

A certificate authority is a trusted third party that verifies identities in cyberspace. Some people think of the certificate authority functioning like an online notary. The basic concept is that a bank, or other third party, uses its good name to validate parties in transactions. This is similar to the historic role banks have played with letters of credit, where neither the buyer nor seller knew each other but both parties were known to the bank. Thus the bank uses its good name to facilitate the transaction, for a fee. Banks also may need a way to validate themselves in cyberspace, as theft of

identity has taken place. According to GAO testimony (GAO/T-66D-99-34), perpetrators have copied legitimate brokerage-firm Web sites, altered addresses for customers to contact (and send checks), then put the fraudulent Web site back on the Internet. Except for the post office box and possibly the URL, everything on the Web site could appear legitimate. Banks will have to guard against a variety of frauds and scams as banking on the Internet becomes more prominent. A proper mix of preventive, detective, and corrective controls can help protect national banks from these pitfalls. Digital certificates may play an important role in authenticating parties and thus establishing trust in Internet banking systems.

Nonrepudiation is the undeniable proof of participation by both the sender and receiver in a transaction. It is the reason public key encryption was developed, i.e., to authenticate electronic messages and prevent denial or repudiation by the sender or receiver.

Although technology has provided an answer to nonrepudiation, state laws are not uniform in the treatment of electronic authentication and digital signatures. The application of state laws to these activities is a new and emerging area of the law.

Privacy is a consumer issue of increasing importance. National banks that recognize and respond to privacy issues in a proactive way make this a positive attribute for the bank and a benefit for its customers.

Public concerns over the proper versus improper accumulation and use of personal information are likely to increase with the continued growth of electronic commerce and the Internet. Providers who are sensitive to these concerns have an advantage over those who do not.

Availability is another component in maintaining a high level of public confidence in a network environment. All of the previous components are of little value if the network is not available and convenient to customers. Users of a network expect access to systems 24 hours per day, seven days a week.

Among the considerations associated with system availability are capacity, performance monitoring, redundance, and business resumption. National banks and

their vendors who provide Internet banking products and services need to make certain they have the capacity in terms of hardware and software to consistently deliver a high level of service.

In addition, performance monitoring techniques will provide management with information such as the volume of traffic, the duration of transactions, and the amount of time customers must wait for service. Monitoring capacity, downtime, and performance on a regular basis will help management assure a high level of availability for their Internet banking system.

It is also important to evaluate network vulnerabilities to prevent outages due to component failures. An entire network can become inoperable when a single hardware component or software module malfunctions. Often national banks and their vendors will employ redundant hardware in critical areas or have the ability to switch to alternate processing locations. The latter is often referred to as contingency planning.

2.10 Review of Web Pages

Some of the advantages of online banking through traditional banks are: (*http://www.investorguide.com/igu-article-513-banking-overview-of-online-banking-and-related-issues.html*)

- Most plans allow customers to perform all routine transactions, such as account transfers, balance inquiries, bill payments, and stop payment requests everything but withdrawing cash (at least for now). Some even let you apply for a loan or a credit card online.
- It's very easy to set up an account. With most plans, you can do this totally online, avoiding all paperwork.
- You can access your account information anytime, day or night, and you can do it from anywhere. A few online banks update information in real-time, while others do it daily.
- Once information has been entered, it doesn't need to be re-entered for similar subsequent checks, and you can even schedule future payments to occur automatically.

- Many banks allow for file transfer between their program and popular accounting software packages, making record-keeping a breeze.
- The fees tend to be about the same as with a typical checking account, but it works out to be cheaper since you don't have to pay for the stamps. As online banking continues to gain in popularity, the fees should diminish , since the banks will be able to pass to their customers the money they'd otherwise be spending on real estate and tellers.

For online-only banks, all of the advantages above still apply, and in addition:

- The costs can be even lower for online-only banks than for online banking with traditional banks.

Here are some of the disadvantages of online banking through traditional banks:

- It does take some time to set up and get used to (although all in all it's quite easy).
- Some banks only offer online banking in a limited area.
- When you pay online, you may have to put in a check request as much as two weeks before your payment is due. However, the bank may withdraw the money from your account the day that request is received, meaning you've lost up to two weeks of interest on that payment. (Be sure to ask about precisely when the money is withdrawn from your account.)

For online-only banks, all of the disadvantages above still apply, and in addition...

- Online-only banks don't have branches (by definition), so there's no teller to help you if you have questions (although nearly all do offer phone support), and you have to mail in your deposits (other than direct deposits).
- Traditional banks tend to have more extensive ATM networks than online-only banks.
- Some services that traditional banks offer are difficult or impossible for online-only banks to offer, such as traveler's checks and cashier's checks.

According to Federal Financial Institutions Examination Council "Financial institutions offering Internet-based products and services should have reliable and secure methods to authenticate their customers. The level of authentication used by

the financial institution should be appropriate to the risks associated with those products and services. Financial institutions should conduct a risk assessment to identify the types and levels of risk associated with their Internet banking applications. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. The agencies consider single-factor authentication, as the only control mechanism, to be inadequate in the case of high-risk transactions involving access to customer information or the movement of funds to other parties" (*http://www.ffiec.gov/press/pr031908.htm*).

Banstola (2007) published an article on "*Prospects and Challenges of E-banking in Nepal*" where he concludes :

Advances in information technology and telecommunications have certainly introduced new delivery channels for Nepalese commercial banks' products and services. These new delivery channels include automated teller machines (ATM's), mobile banking, Internet banking. Among these, the ATM's are the most widely accepted and highly utilized delivery channel. As per the information provided by banks, mobile banking seems to have good future prospects. PC banking is still not available in Nepal. However, about 35% of the respondents have Internet access at home and work and these represents a positive indication for PC-based banking and Internet banking in the future. At present, the strategies of the Nepalese banks tend to retain the existing customer through E-banking. E-banking adopters use the basic banking facilities such as cash receive and withdraw, balance enquiry, regular and schedule payment. Only few percentages use other facilities such as inter- account fund transfer, online purchasing. This is basically because of the security and confidentiality concern of the customers regarding these facilities of E-banking. Risk management, infrastructure development and policy formulation the three major challenges of E-banking in Nepal. Technological problems like connect break in service while withdrawing cash from ATM, poor mobile service are creating obstacles in development of E-banking in Nepal. An adequate level of infrastructure and human capacity building are required before banks adopt the full-fledged E-banking. In Nepal, E-banking is at its infancy right now and the system is not perfectly secure.

However, no e-banking frauds have been found yet. Lack of understanding of internet technology may be the reason. But, precaution must be taken.

Telecommunications industry and financial services sector are crucial components for E-banking. Nepal Telecom and now Mero mobile are two telecommunication industries which are operating their business throughout the county. But, the services are limited and the problems are more. The signification association found between age, education with use of E-banking means E-banking providers should target the younger age group as well as well educated persons. The cost analysis of most of the banks is seems to be either inadequate or not applied due to their narrow space of business transaction or lack of sufficient tools. This poor awareness in cost analysis of banking transaction may lead to loss in future in the field of E-banking. To be able to draw conclusions about profitability, some investigation into the income side has to be made as well.

2.11 Review of Thesis

Researcher reviewed some unpublished master degree thesis for identifying variables relevant for research. This works helps to avoid any repetition. Researchers found that majority of the master's degree thesis are concentrated in the case study approach of public organizations. However, researcher realizes that the review of old and new master degree thesis on different organization really useful to carry out this research study.

Thapa (2003) conducted a study entitled "*Future Prospective of Online Banking in Nepal*". He collected data based on the primary. The primary data were collected from structured interview. The analysis of data was presented on the tabular form, simple bar diagram and pie chart. The analysis of data has been done through various ways like percentage, average etc. and concluded that banks in future cannot survive without the support of Information Technology.

On his study he found that only 5% respondents are satisfied with the traditional banking system and rest 95% want immediate technical improvement in their service system. Respondents feel that the bank should imply online services to provide better facilities to them.

The findings of his study are:

- The bank should developed standard based solutions which consist of open system architecture, with scalability as its main feature for taking care of future volumes in growth.
- The IT industry should closely collaborate with the banking sector in providing such serves at cost-effective prices and should gear itself to meet the requirements of the banking and financial sector with a spirit of co-operation, and partnership in making the banking industry scale the heights of international excellence.
- In order to minimize frauds and security problems, the Central Vigilance Commissioner (CVC) should direct all banks to compulsorily offer Electronic Clearing Services (ECS) to their customers.

Bajracharya (2008) presented a dissertation on "*Internet Banking in Nepal*" and his finding are :

- Banks enhance the security level of virtual environment.
- Banks have to implement such policies which create secure environment for reliable transactions.
- Banks have to developed fast communication service with their' customers.
- The banks should minimize the level of perceived risk in e-transaction environment.
- Finally the banks should ensure their' customer that the customer data is secured and will not be shared or misused.

He conclude his dissertation by writing "The findings show that all respondents have greater level of worry regarding trust, do not have confidence to make any big financial transactions over internet, and have no satisfaction from Internet banking services".

Chapter III
METHODOLOGY

The following chapter on Methodology will describe research methods used in this study and explain the chosen methods. It will further describe the research purpose, research approach, and research strategy and data collection methods. Furthermore, this chapter describes the chosen sampling technique, the way the data for the study has been collected and techniques used to analyze the data.

3.1 Research Purpose

There are several techniques which could be used to carry out the research based on research problem area. When dealing with research problem, one can use any of three classification research.

3.1.1 Exploratory

Exploratory research is often conducted when problem is not well known or it has not been clearly defined as yet, or its real scope is as yet unclear. It allows the researcher to gather helps determine the best research design, data collection method and selection of subjects and sometimes it even concludes that the problem does not exit. Exploratory research is quite informal, when it relying on secondary researches such as reviewing available literature, data, or qualitative approaches such as informal discussions with consumers, employees, management or competitors, and more formal approaches through in-depth interviews, focus groups, projective methods, case studies or pilot studies .

3.1.2 Explanatory

This is a research type in which the primary goal is to understand the nature or mechanisms of the relationship between the independent and dependent variable. This approach is used when it’s necessary to show that one variable causes or determines the value of other variable. This research is good to use when there is no clear apprehension about what model that should be used and what qualities and relations that is important.

3.1.3 Descriptive

Descriptive research is used to obtain information concerning the current status of the phenomena to describe “what exists” with respect to variables or conditions in a situation. Descriptive research is used when the objective is to provide a systematic description that is as factual and accurate as possible or when the problem is well structured and there is no intention to investigate cause/effect relation. It provides the number of times something occurs, or frequency, lends itself to statistical calculations such as determining the average number of occurrences or central tendencies.

3.2 Research Approach

There are two types of research approaches, qualitative and quantitative. In the quantitative approach, results are based on numbers and statistics that are presented in figures, whereas in the qualitative approach where focus lies on describing an event with the use of words.

Although research on Internet banking services of Nepal is not very extensive compared to discussion of the benefits, most of the concepts in this study have been occasionally examined before, but mostly in the western context. Only a little research covers usually Singapore, Hong Kong or China, which are very developed economies and not representative of all Asian countries. Thus to gain practical knowledge of Internet banking in the Nepali context, this research is conducted as a qualitative study to explore the perception of Internet banking among Nepali firms. Hence the aim is not to make any simplification, but instead establish a closer contact with the contact with the objectives of prior research, which intend to provide us a deeper understanding of the participants’ attitudes and perceptions. Finally my intention with this research is to understand Internet banking first, describe and explore, and find detailed information about Internet banking services provided by different banks of Nepal, so qualitative approach is the most suitable method for my research.

3.3 Research Strategy

Research strategy is a general plan which shows that how this research will go on, and how researcher will answers the question that has been set by the researcher. It will contain clear objectives, derived from research question specify the source from

which researcher intend to collect data and consider the constraints that researchers will inevitably have such as access to data, time, location and money, ethical issues.

Qualitative research can be conducted using several strategies including: case study, experiments, surveys, histories, and analysis of archival information.

Following are the short description of above five research strategies:

3.3.1 Case Study

Case study refers to the collection and presentation of detailed information about a particular participant or small group. A case study is a written description of a problem or situation and typically examines the interplay of all variables in order to provide as complete an understanding of an event or situation as possible.

3.3.2 Experiments

The experimental method involves manipulating one variable to determine if changes in one variable cause changes in another variable. This method relies on controlled methods, random assignment, and the manipulation of variables to test a hypothesis. This strategy is used when the researcher need to compare two variables and examine their cause and effect relationships.

3.3.3 Survey

It's research technique in which information is collecting by interviews with a large number of respondents using a pre-designed questionnaire. This research technique has three important characteristics:

- **Purpose:** The purpose of survey research is to produce quantitative descriptions of some aspects of the study population. Survey analysis may be primarily concerned either with relationships between variables, or with projecting findings descriptively to a predefined population. Survey research is a quantitative method, requiring standardized information from and/or about the subjects being studied. The subjects studied might be individuals, groups,

organizations or communities; they also might be projects, applications, or systems.

- **Procedure:** The main way of collecting information is by asking people structured and predefined questions. Their answers, which might refer to themselves or some other unit of analysis, constitute the data to be analyzed.
- **Analyses:** Information is generally collected about only a fraction of the study population, but it is collected in such a way as to be able to take a broad view the whole population. Usually, the sample is large enough to allow extensive statistical analyses.

3.3.4 History

This method is deals with past, and is used when no relevant persons are alive to interview or report. This method is specifically used to describe the content, structure and function of the data which collected for research.

3.3.5 Analysis of Archival Information

The purpose of this technique is to describe the incidence or prevalence of a phenomenon. The use of the archival information is difficult when this topic is coming research area.

3.4 Sample Selection

Sampling is a survey-based research where researcher needs to analyze the sample about a population to answer the research questions or meet the research objectives. Once the problem has been carefully defined, the researcher needs to establish the sample that will outline the investigation to be carried out. It is necessary for researcher to clearly define the target population from whom sample will be taken. Sampling is important if budget and time constraints prevent research from surveying the entire population. Sample gives higher accuracy and fast result.

Sometimes, the entire population will be sufficiently small, and the researcher can include the entire population in the study. This type of research is called a census study because data is gathered on every member of the population.

Usually, the population is too large for the researcher to attempt to survey all of its members. A small, but carefully chosen sample can be used to represent the population. The sample reflects the characteristics of the population from which it is drawn.

Sampling technique can be classified into two types.

- Probability Sampling
- Non-Probability Sampling

3.4.1 Probability Sampling

In probability sampling, the sample is selected in such a way that each unit within the population has a known chance of being selected. It is this concept of "known chance" that allows for the statistical projection of characteristics based on the sample of the population. The advantage of probability sampling is that sampling error can be calculated. Sampling error is the degree to which a sample might differ from the population probability method includes:-

- Random sampling
- Systematic sampling
- Stratified sampling

3.4.2 Non-Probability Sampling

In non-probability sampling, the sample is selected in such a way that the chance of being selected of each unit within the population is unknown. Indeed, the selection of the subjects is random or subjective, since die researcher relies on his/her experience and judgment. As a result, there are no statistical techniques that allow for the measurement of sampling error, and the degree to which the sample differs from the population remains unknown and therefore it is not appropriate to project the sample characteristics to the population. Non-probability includes:-

- Convenience sampling
- Judgment sampling
- Quota sampling

- Snowball sampling

3.4.2.1 Convenience Sampling

Convenience sampling is used in exploratory research where the researcher is interested in getting an inexpensive approximation of the truth. As the name implies, the sample is selected because they are convenient. This non-probability method is often used during preliminary research efforts to get a gross estimate of the results, without incurring the cost or time required to select a random sample.

3.4.2.2 Judgment Sampling

Judgment sampling is a common non-probability method. The researcher selects the sample based on judgment. This is usually and extension of convenience sampling. For example, a researcher may decide to draw the entire sample from one "representative" city, even though the population includes all cities. When using this method, the researcher must be confident that the chosen sample is truly representative of the entire population.

3.4.2.3 Quota Sampling

Quota sampling is the non-probability equivalent of stratified sampling. Like stratified sampling, the researcher first identifies the stratums and their proportions as they are represented in the population. Then convenience or judgment sampling is used to select the required number of subjects from each stratum. This differs from stratified sampling, where the stratums are filled by random sampling.

3.4.2.4 Snowball Sampling

Snowball sampling is a special non-probability method used when the desired sample characteristic is exceptional. It may be extremely difficult or unavoidable to locate respondents in these situations. Snowball sampling relies on referrals from initial subjects to generate additional subjects. While this technique can dramatically lower search costs, it comes at the expense of introducing bias because the technique itself reduces the likelihood that the sample will represent a good cross section from the population.

Sampling in qualitative research involves two actions:

- Setting of boundaries: 'To define aspects of cases that we can study and connecting it directly to the research question".
- Creation of frame: "to help us uncover', confirm, or qualify the basic process or constructs that strengthen our study"

3.5 Data Collection Techniques

The study is mostly depends upon the primary as well as secondary sources of data which are given below:-

3.5.1 Primary Sources of Data

The research is mainly based on the primary sources of data, which are obtained from observation of the system of different Banks and filled questionnaires by employees of different Banks.

3.5.2 Secondary Sources of Data

The secondary source of data is also applied for the research. They are obtained from different books, journals, websites and field observations.

3.6 Questionnaire

The questionnaire consists of three pages and three sections. The first section gathers general question such as introduction.

The second section is about website such as website host and third section gathers data and physical security such as firewall, responsibility of system administrator etc.

3.7 Validity and Reliability

In order to reduce the possibility of getting incorrect answers, attention needs to be paid to validity and reliability.

3.7.1 Validity

Validity is concerned with whether the findings are really about what they appear to be about. Validity defined as the extent to which data collection method or methods accurately measure what they were intended to measure.

Following methods have been used to accomplish this proposed solution:

- Basic principles of existing banking system (Nepal)
- Study the major drawbacks of existing system by interviewing the current employees of different banks. Interviews are mostly taken by visiting bank.
- Study the existing IT infrastructure of Nepal in context of Bank by interviewing the bankers.
- Study the E-banking system from different resources that are available in different websites, books and online journals.
- Design proposed solution.
- Using sampling method to collect the data from different banks.

3.7.2 Reliability

Reliability refers to degree to which data collection method or methods will yield consistent findings, similar observations would be made or conclusions reached by other researchers or there is transparency in how sense was made from the raw data.

Chapter IV
ANALYSIS OF SYSTEM

4.1 Analysis of Internet Banking

Careful examination of something to see exactly how it operates is known as the analysis so in this chapter I tried to do that at best level. With the increasing development of technology, and with the benefit of using today's computer technology, online possibilities give the option of saving time and paper work. Both at work and private, one can manage the finances more quickly and efficiently (*bankrate.com; 2007*). Online banking creates additional opportunities and challenges for the banking industry.

In more detail, online banking is the performance of banking activities via the internet (*answers.com; 2007*). A good online banking system should not differ much from what a traditional brick and mortar bank offers. The great benefit of online banking is that it is free and the possibilities of accessing your bank whenever it is convenient for the customer, 24/7 and requires only a few mouse clicks for any transaction.

Furthermore a good online bank should offer high IT security. The object of having a good IT security is to eliminate or reduce significant threats against its system. The IT security comprises of three basic components : confidentiality, integrity and availability (*Bishop; 2005*).

Confidentiality : The system should be secure by ensured that the system will not be accessed to anyone who do not have the authority, the goal is to keep the information or resources hidden and this applies especially of the use of computers within government, medicine and law, there are different access control mechanism that support confidentiality.

Integrity : Integrity of data is about the level of trustworthiness of data or resources, the goal is to prevent improper or unauthorized change of data, important aspect is to protect a person's integrity, there are two kinds of integrity mechanism; prevention and detection, the prevention mechanism avoid any unauthorized attempts of changing the data by preserving the data, detection mechanism will discover when the

data's integrity is no longer trustworthy through analyzing and reporting the data status.

Availability : The information or resource should be accessible when desired, a system that is not available considered to be as bad as no system at all, in some aspects that data can also be intentionally arranged to deny accessibility due to security aspects.

4.2 Analysis of Internet Bank of RBB and NBL

As per response of questionnaire, RBB is providing the internet banking for the customer service while NBL is providing same facility for the convenience this might be the cause that RBB has more customer than the NBL. Both banks are satisfied with their services provided to the customers. In comparison to the normal customer of both banks the customer of internet banking is very nominal.

4.2.1 Users of Internet Banking

Name of Bank	**Number of User**
Rastriya Banijya Bank	Around 2000
Nepal Bank Limited	Around 1000

Table 1 : Users of Internet Banking

RBB has the around 2000 internet banking while its banking customers are more than 200000 whole around the country and the similar condition of internet banking user in NBL also, it has only around 1000 customer as internet banking which is very few in comparison to its normal customer. This is the main issue that how to increase number of internet banking customer and reduces the operating cost of the banks.

4.2.2 Services Provided as Internet Banking

Services	**RBB**	**NBL**
Balance Enquiry		
Transaction search		
Cheque book replenishment request		
Transfer within own accounts or within group accounts		
Statement download		
Loan information		
Insurance service over the internet		
Utility bill payments (Telephone, school/college fees, electricity etc)		near in future
Message to Branch		

Table 2 : Services Provided as Internet Banking

It shows that RBB is ahead in providing almost all the internet banking services. It may because the sound policy of RBB. This system allows individuals to perform banking activities like balance enquiry, statement download, inter-account fund transfer etc. from any place any time and any where via the internet. In comparison the RBB, NBL is not able to give all the services like transaction search, transfer within own accounts or within group accounts as Internet banking but they are trying to providing the services like utility bill payments, balance transfer and mobile bill payment which will be good part of Internet banking service provide by NBL. Both banks are not able to provide some services which we can find in international banks provide as Internet banking some are loan information and insurance service over the internet.

There is quite difference in users accessing time banks website also normally RBB's web site is visited mostly 11:00 am to 2:00 pm while NBL's website is visited mostly morning or after banking hour. In the concern of customers benefited also RBB can provide services to call customer who have registered while NBL have not tested yet.

4.2.3 Risk Management in RBB and NBL

Risk Management Factor	RBB	NBL
Regular Backup of web site information		
Firewall Protection		
Update of public web site		
Internet-banking Policy		
Lightening / power surge protection		
Advance Security Tools		
User ID and password Verification		
User ID, Password and PIN Verification		
Digital Certification		
Digital Signature	NA	NA
Biometric Verification	NA	NA
2FA	NA	NA
Encrypted data transfer		
Automatic log-off controls		

Table 3 : Risk Management in Banks

Both banks tried to managed their risk management as per possible as legalization in our country context so both banks are very much concern about the risk management. Both use firewall protection while RBB use Cisco's pix 525 series which is closed, hardware based and more secure than any other firewall and for application layer RBB use ISA 2006 which is very good product of Microsoft, NBL use LINUX firewall and FortiGate 100A. Where Cisco's pix 525 is known as better firewall in world, it is very expensive in comparison to others, it is capable to handle more than 2800000 simultaneous sessions. In comparison to RBB, NBL use lite firewall FortiGate 100A which is suitable for small business only and this one is suitable for NBL because of its low number of customers.

In RBB, Network and System Unit is responsible for installing, configuring and updating the firewalls as well as monitoring firewall activities and which is monitored daily, while in NBL system unit is responsible for it and there is continuous monitored and it has alert mechanism. This monitored mechanism is depend on the

device which they have installed and services they are using also mostly nowadays in all firewall there is continuous monitoring mechanism but Pix 525 series is little old firewall that's might be cause that RBB does not have continuous monitoring mechanism. Both banks blocked unused services at the firewall and only which are important to provide services only those ports are opened by both banks. Both banks have open only 80, 443 ports.

There must be internet banking policy before implementing it. Policy helps banks to organize, maintain and upgrade the system of internet banking. RBB and NBL both have very energetic and dynamic staffs to handle Internet Banking they have very sound Internet-banking policy. In the context of Nepal it is very important to have lighting /power surge protection because of necessary to provide 24/7 service which both banks have and they are able to manage it very well.

It is very important to test any services before they are launch to customer. Both banks tested their Internet Banking before launching. RBB use unit testing, black box testing and white box testing while NBL use user acceptance test which seems little concern towards customers' satisfaction.

RBB hosted their web site in their own office while NBL hosted their web site in vendor site they outsource some of their services while RBB do all their services by themselves. They both do regular backup of their web site information by their IT department as well as regular update of public web site. Both bank reviewed web site internally. Datacenter Unit Personnel is responsible to check links and programs for accuracy and functionality in RBB and which is done daily while IT department is responsible to check links and programs for accuracy and functionality in NBL and it is continuous process. Datacenter Unit Personnel is responsible for doing the implementation of the updates / patches and they are tested before putting into production in RBB while IT department is responsible for doing the implementation of the updates/ patches and they do UAT before putting into production in NBL.

It is very important to be up-to-date about addressing newly disclosed security threats to the computer operating system and application software. Because in normal condition 20 percents new threats cannot be detected by antivirus, anti spam, content filter and firewall also. So it is very important to be up-to-date which is possible by

paying service provider of firewall but RBB simply response yes they do but NBL response in this they use all possible tools and measures.

Both banks have safeguards in place to detect and prevent duplicate transactions which is essential in the sector of banking. Both banks employees can not access customers' passwords which is must in the electronic data interchange services. Nobody can access password and PIN code in EDI. RBB and NBL both use 128 bits level data encrypted which is quite impressive in security measures.

Digital Certification is an attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later. Both banks are using Verisign Digital Certificate as digital certificate but they are not using digital signature for security. The reason behind both banks' are not providing digital signature is lack of legal act in Nepal. There is not any mechanism till the date of digital signature in Nepal but it is on the way and the Controller of Certification Authority (CCA) is going to implement in near future may be start from next fiscal year. After that our banks are going to provide that service also.

Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures. The oldest form of biometric verification is finger printing. Biometric verification has advanced considerably with the advent of computerized databases and the digitization of analog data, allowing for almost instantaneous personal identification. Biometric Verification is also little far from our country context but in international banks we can find that also as risk management.

2-Factor Authentication (2FA) is the latest security initiative from OCBC that provides greater online protection for Internet and Mobile Banking users. With 2FA, users are required to input a One-Time Password (OTP), and this acts a 2nd level of user authentication. This technology is also not implementing by the RBB and NBL.

4.2.4 Database and Application Server in RBB and NBL

	RBB	**NBL**
Software	Pumori Plus III	NEWTON
Database Server	MS SQL Server	MS SQL Server
OS + Web Server	Windows 2000 server	Windows 2003 server
Storage Device		
Array		
Hot Swap		
Backup Policy	RAID 1+0	RAID 1+0
Disk Size		
For Total Banking	90 GB	80 GB
For Internet Banking	2 GB	2 GB

Table 4 : Database and Application Servers in Banks

For the banking software, RBB is using local product of Mercantile Pumori Plus III and NBL is using foreign product NEWTON which is supply here by 3i Infotech. Pumori Plus III is complete banking software solution for Microsoft Windows and Microsoft SQL Server while NEWTON is currently available for Red Hat Linux.

MS SQL is database server which is very powerful and product of Microsoft. With SQL Server 2005 developers can develop Web services in the database tier, making SQL Server a hypertext transfer protocol (HTTP) listener and providing a new type of data access capability for Web services-centric applications. Extend log shipping capabilities with the database mirroring solution. You will be able to use database mirroring to enhance availability of your SQL Server systems by setting up automatic failover to a standby server. With SQL Server 2005, database administrators are able to perform a restore operation while an instance of SQL Server is running. Online restore improves the availability of SQL Server because only the data being restored is unavailable; the rest of the database remains online and available. A new faster

recovery option improves availability of SQL Server databases. Administrators can reconnect to a recovering database after the transaction log has been rolled forward. There are lots of features of MS SQL these might be cause that both banks use MS SQL as database server.

Microsoft windows is such a huge product that even there are lots of options more than 80% of computer user use it. The Windows 2000 Server family has additional features, including the ability to provide Active Directory services (a hierarchical framework of resources), Distributed File System (a file system that supports sharing of files) and fault-redundant storage volumes. In Windows server there is inbuilt web server known as IIS. Here both RBB and NBL uses the windows server but RBB is using still windows 2000 server while NBL using windows 2003 server.

For storage devices both banks keep their disks in array, so that they are capable of doing hot swapping also. Hot swapping and hot plugging are terms used to separately describe the functions of replacing system components without shutting down the system. Hot swapping describes changing components without significant interruption to the system, while hot plugging describes changing or adding components which interact with the operating system. Both terms describe the ability to remove and replace components of a machine, usually a computer, while it is operating. For hot swapping once the appropriate software is installed on the computer, a user can plug and unplug the component without rebooting which is known as best practice to keep storage device.

RAID is an acronym for Redundant Array of Inexpensive (or Independent) Disks. A RAID array is a collection of drives which collectively act as a single storage system, which can tolerate the failure of a drive without losing data, and which can operate independently of each other. Both sample banks RBB and NBL used RAID10 which is technology that allowed computer users to achieve high levels of storage reliability from low-cost and less reliable PC-class disk-drive components, via the technique of arranging the devices into arrays for redundancy.

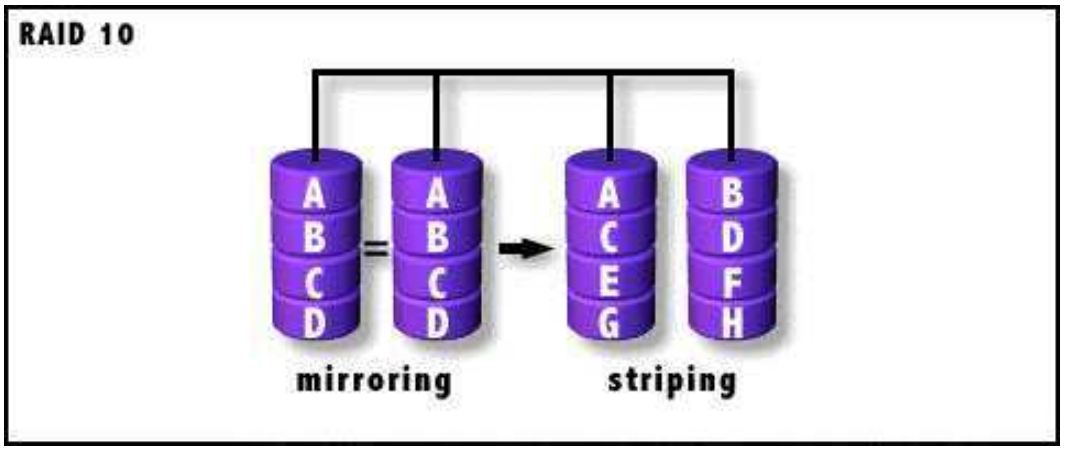

Figure 1 : Raid 10

RAID 10: Very High Reliability combined with High Performance. RAID Level 10 requires a minimum of 4 drives to implement.

Advantages:

- RAID 10 is implemented as a striped array whose segments are RAID 1 arrays. RAID 10 has the same fault tolerance as RAID level 1.
- RAID 10 has the same overhead for fault-tolerance as mirroring alone.
- High I/O rates are achieved by striping RAID 1 segments.
- Under certain circumstances, RAID 10 array can sustain multiple simultaneous drive failures.
- Excellent solution for sites that would have otherwise gone with RAID 1 but need some additional performance boost.

Disadvantages:

- Very expensive / High overhead.
- All drives must move in parallel to proper track lowering sustained performance.
- Very limited scalability at a very high inherent cost.
- Recommended Applications Database server requiring high performance and fault tolerance.

RAID 10 arrays are typically used in environments that require uncompromising availability coupled with exceptionally high throughput for the delivery of data located in secondary storage. In recent years a number of mutations of RAID 10 have been developed with similar capabilities. This paper presents one of the popular alternative implementations and discusses the relative advantages and disadvantages of RAID 10 and this alternative.

A RAID 10 array is formed using a two-layer hierarchy of RAID types. At the lowest level of the hierarchy are a set of RAID 1 sub-arrays i.e., mirrored sets. These RAID 1 sub-arrays in turn are then striped to form a RAID 0 array at the upper level of the hierarchy. The collective result is a RAID 10 array. The figure below demonstrates a RAID 10 comprised of two RAID 1 sub-arrays at the lower level of the hierarchy. They are sub-arrays A (comprised of disks A1 and A2) and B (comprised of disks B1 and B2). These two sub-arrays in turn are striped using the strips 1A, 1B, 2A, 2B, 3A, 3B, 4A, 4B to form a RAID 0 at the upper level of the hierarchy. The result is a RAID 10. Figure 1 illustrates a RAID 10 array, with each disk in the array participating in exactly one mirrored set, thereby forcing the number of disks in the array to be even.

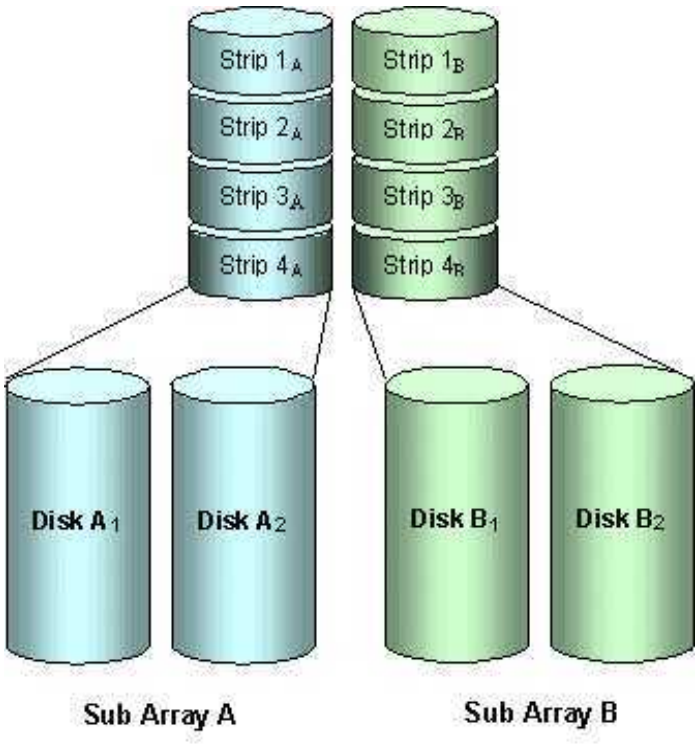

Figure 2 : RAID 10

Because of low number of customer in Internet Banking both bank has separated disk size very small in comparison to whole banking system. RBB have 90 GB disk space for total banking while NBL have 80 GB but both bank use or separated only 2 GB of disk space for Internet Banking.

4.3 Internet Banking Security Aspects

As in any other system, there are risks involved in Internet banking. However, potential risks are mitigated with banking institutions' continuous check on the security of the system and the care taken when using Internet banking services.

Security in Internet banking comprises both the computer and communication security. The aim of computer security is to preserve computing resources against abuse and unauthorized use, and to protect data from accidental and deliberate damage, disclosure and modification. The communication security aims to protect data during the transmission in computer network and distributed system.

4.3.1 Security Measures in the Bank Side

All banks that are providing internet-banking facility have the system consisting of the followings:

- Password controlled system entry.
- VeriSign issued Digital certification for the Bank's server.
- Secure Socket Layer (SSL) protocol for data encryption.
- Firewall setup.

4.3.2 Firewalls and Associated Controls

Management needs to understand the capabilities and functionality of the firewall and make sure that their systems are configured appropriately for the bank's business needs. Ongoing monitoring of the firewall ensures that the appropriate functions and utilities are activated to protect the institution and prevent attacks against known system weaknesses. Institutions that do not have the expertise to design, install, and test firewalls should seriously consider engaging professionals to perform this function. Due care should be exercised when selecting the vendors to perform these

functions and sound internal controls should be in place along with audits to verify the vendor's activities with the firewall. The institution should periodically engage an independent source to test the firewall for weaknesses. This includes annual, or more frequently as circumstances warrant, penetration testing to ensure controls are appropriate to the type and level of risk arising from the institution's Internet banking products and services.

A firewall is hardware and software placed between two networks. The intent is for all network traffic, regardless of the direction of flow, to pass through this firewall. The firewall then can check all traffic to make sure it is authorized and prevent unwanted traffic from entering the system. The firewall also can check the traffic to determine whether it contains any unauthorized attachments, such as viruses. Firewalls need to be efficient to catch any traffic that is unauthorized in order to prevent potential harm to the institution.

Network isolation is a function of firewalls. A domain name server converts publicly known addresses into internal addresses that are not publicly known. This is sometimes referred to as a "bastion host." The feature prevents intruders from gaining access to internal names and addresses on the bank's internal network. External devices attempting to access internal addresses are suspect and should be screened out.

Address screening is another of the functions of a firewall. This function is used to filter-out messages with inappropriate source addresses. For example, this function would screen out messages with internal system addresses. Messages that have not gone through a domain name server should not have internal addresses and would be suspect. Such traffic should not be allowed to pass through the firewall.

Application screening is a firewall function used to prevent inappropriate instructions from entering the system or an unauthorized access to the administrator level of the server. A "proxy server" is a device used to test the system's "rules" to prevent deviations from the established rules.

Message flow inspection or state full inspection is a function of a firewall used to detect inappropriate responses by the system. The system creates a database and looks

for inappropriate responses by a server to messages or inquiries. For example, if a request asks for account balance information and the response is to transfer funds, the "state full inspection" will recognize an inappropriate response and terminate the session.

Other controls normally work in tandem with firewalls. These controls include logical access controls and physical security. The reason these controls are important is that insiders represent the greatest threat to bank computer systems and data communications networks. Various studies reflect that nearly 70 percent of intrusions originate within the organization. Insiders have knowledge of the system or network and may have the opportunity to originate an unauthorized transaction either by accident or intent. Access to systems, networks, and information should be on a "need-to-know" basis.

Banks also need to provide protection from employee ignorance such as sharing passwords and running outside software without virus checking. A logical access control includes a user identification and a password. An individual's user ID might be J. Examiner. But each user should also have a unique password composed of at least 6-8 alphanumeric characters; more is better. It is important to avoid using passwords that are easily discerned. Names, addresses, or words found in the dictionary, any language, spelled forward or in reverse should be avoided. One option is to use mnemonics —something that is easy to remember but difficult to guess. An example of a mnemonic is the following phrase; "Examiners are curious, bright people." The mnemonic is EACBP. By adding some numbers and/or special characters, a password can be created that is easy to remember but difficult to discern.

Physical security also is an important control function in protecting a bank's data communications networks and internal accounting systems. Network hardware should be stored in secure locations so that it is accessible only to authorized personnel. This is a preventive control to protect the bank's assets and protect the institution from transaction, reputation, and strategic risk. Personal computers connected to a network should have sound logical access controls. This includes a password feature to access the network and time-out password controls to protect the network when a particular PC is unattended, even for brief periods of time.

Banks should consider the feasibility of centrally controlled modem pools. Controlling the placement and access to modems attached to a bank's network will help the bank limit access to only authorized individuals. Banks should specifically guard against unauthorized modems that employees may attach to their PCs which are connected to the bank's data communication network.

These unauthorized modems can be targets of "random dialing" efforts and can be a vulnerable entry point into the bank's network. Time of day controls can be used to restrict access to a bank's network to certain, preauthorized times. The objective is to limit the opportunity for after hours access except as authorized by the network administrator. Decisions on this type of control will be based on the types of business the bank is engaged in and the need for access to its internal networks.

Well-defined policies will help a bank develop a sound system of controls and ultimately reduce the vulnerability to penetration. Well-defined control objectives will help the systems administrator or vendors to properly configure the firewall. Such policies also will give auditors a standard to measure against when performing tests. Some considerations for bank firewall policies include:

- Communicating the bank's policy with respect to monitoring employee use of data communications networks, including electronic mail and the Internet.
- Requiring virus checking for all diskettes or downloads from other than authorized sources. Even diskettes received from other employees can be contaminated with a virus and should be scanned before use, especially on a PC connected to the bank's network.
- Determining the bank's policy for the access to PCs and the bank's network after hours for uses that are not related to work.
- Informing employees of the consequences of violating the institution's network usage policies.
- Limiting access to and use of administrator level capabilities of the firewall hardware and software.
- Requiring periodic review of the vulnerabilities of the bank's firewalls from known threats including, penetration testing.
- Regularly logging and reviewing all activity.

Sophisticated auditing techniques are appropriate to determine whether effective policies are in place and whether the system of controls over the bank's network is working as intended. The controls and audits of firewalls need to be performed on a regular basis. Firewall systems are dynamic and need regular reviews to ensure protection from newly identified vulnerabilities and system weaknesses.

Once the internal or external auditor gains a sound understanding of the bank's network configuration and types of business, he or she may decide to perform various tests to ensure the soundness of logical access controls. This might include testing default settings to determine whether only authorized firewall functions are permitted. The auditors might use audit software to scan the activity logs looking for anomalies or unusual activity. They might review the screening of employees who developed or installed the network. The auditors might also review the frequency of password changes for employees authorized access to a bank's data communications network.

Depending on the level of Internet banking employed, the bank will want to consider engaging outside experts to review their security measures and offer recommendations for enhancements. This type of review should be considered at least annually for transaction systems and somewhat less frequently for communicative and informational systems.

4.3.3 Cryptography

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, including:

- *Authentication:* The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
- *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
- *Non-repudiation:* A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as *plaintext*. It is encrypted into *ciphertext*, which will in turn (usually) be decrypted into usable plaintext. Cryptography is probably the most important aspect of communications security and is becoming increasingly important as a basic building block for computer security.

4.3.3.1 Types of Cryptographic Algorithms

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are (Figure 1):

- **Secret Key Cryptography (SKC)**: Uses a single key for both encryption and decryption
- **Public Key Cryptography (PKC):** Uses one key for encryption and another for decryption
- **Hash Functions:** Uses a mathematical transformation to irreversibly "encrypt" information

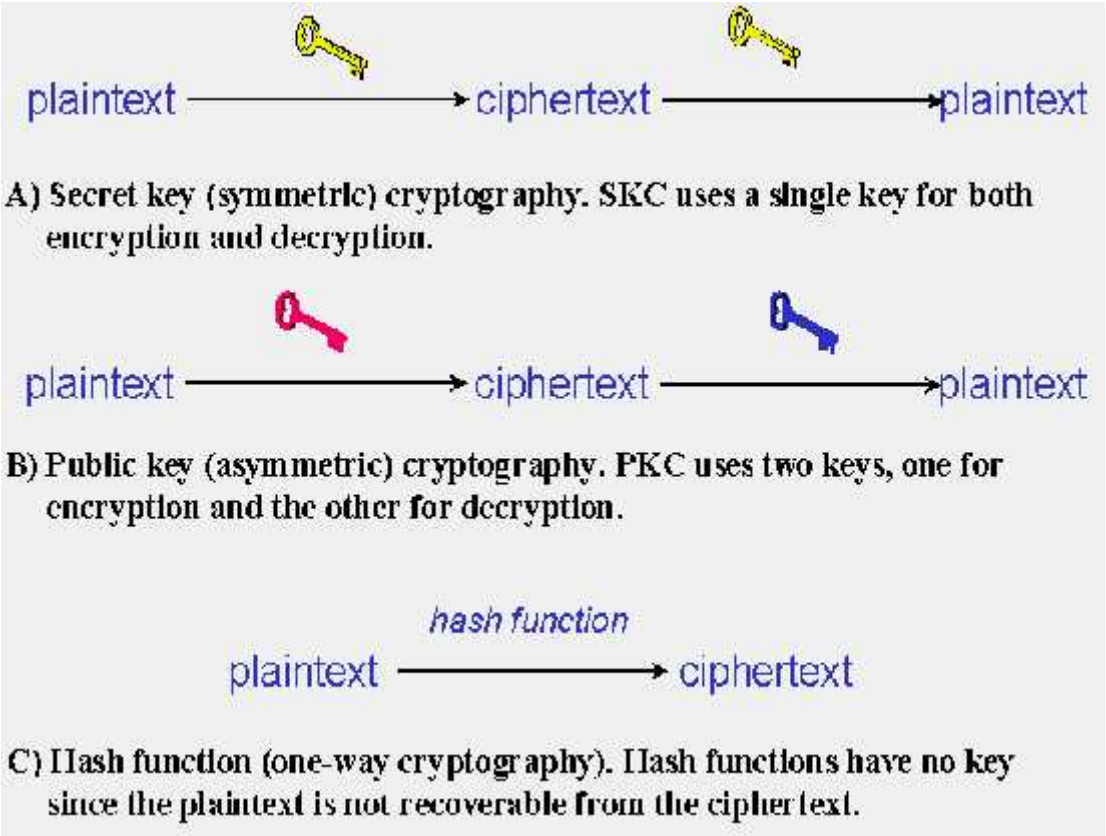

Figure 3 : Three Types of Cryptography : Secret Key, Public Key and Hash Function

Secret Key Cryptography, also known as Symmetric, requires both the sender and receiver to have the same key (the integers that drive the encryption algorithm). The diagram on the following page shows how the process works. The sender encrypts the message and the receiver decrypts the message using the same key. One of the most commonly used systems of this type is the Data Encryption Standard, or DES. The U.S. Government adopted this IBM- developed technology in 1977. It is widely used and operates on a minimum 56 bit (binary digit) base key. Some institutions will use Triple-DES where the message is encrypted three times to enhance its resistance to decoding.

The advantages of secret key cryptography are that it is secure, widely used, and fast. The disadvantages are that key administration is complex, requiring both parties to maintain absolute control over exchanging keys, it does not include a separate authentication mechanism, and there is no non repudiation (undeniable proof of participation of the sender and receiver). In addition, some cryptographic systems are subject to export restrictions from the U.S. government.

Public/Private Key Cryptography, also known as Asymmetric, employs two keys. As noted in the following diagram, in order to secure a message the sender performs the encryption using the recipient's public key. However, the receiver can only read the information using their private key. Often the literature refers to this technology as two key cryptography. A popular public key technology is RSA. Ron Rivest, Adi Shamir, and Leonard Adleman developed RSA in 1977. The primary use of RSA is for authentication and the secure exchange of encryption keys and digital signatures. Key length can vary from 40 to 1,024 bits.

Some of the advantages of public key cryptography over private key cryptography are that it simplifies key administration. For example, there is no requirement for a prior relationship between the sending and receiving parties. In addition, the key lengths can be much longer than DES. According to the vendors, this makes public key cryptography stronger. It also provides for non repudiation. The major disadvantage is that public key is much slower than private key cryptography. Thus, it is used primarily to authenticate messages rather than encrypt an entire message.

Hash functions, also called *message digests* and *one-way encryption*, are algorithms that, in some sense, use no key (Figure 1C). Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a *digital fingerprint* of a file's contents, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

Hash functions are sometimes misunderstood and some sources claim that no two files can have the same hash value. This is, in fact, not correct. Consider a hash function that provides a 128-bit hash value. There are, obviously, 2^{128} possible hash values. But there are a lot more than 2^{128} *possible* files. Therefore, there have to be multiple files — in fact, there have to be an infinite number of files! — that can have the same 128-bit hash value.

The difficulty is *finding* two files with the same hash! What is, indeed, very hard to do is to try to create a file that has a given hash value so as to force a hash value collision

— which is the reason that hash functions are used extensively for information security and computer forensics applications.

4.3.4 Types of Online Attacks

Banks and service providers need to guard against various types of online attacks. The object of an attack may vary. Attackers may try to exploit know vulnerabilities in particular operating systems. They also may try repeatedly to make an unauthorized entry into a Web site during a short time frame thus denying service to other customers.

Types of attacks may include:

- Sniffers — Also known as network monitors, this is software used to capture keystrokes from a particular PC. This software could capture logon IDs and passwords.
- Guessing Passwords — Using software to test all possible combinations to gain entry into a network.
- Brute Force — A technique to capture encrypted messages then using software to break the code and gain access to messages, user ID's, and passwords.
- Random Dialing — This technique is used to dial every number on a known bank telephone exchange. The objective is to find a modem connected to the network. This could then be used as a point of attack.
- Social Engineering — An attacker calls the bank's help desk impersonating an authorized user to gain information about the system including changing passwords.
- Trojan Horse — A programmer can embed code into a system that will allow the programmer or another person unauthorized entrance into the system or network.
- Hijacking — Intercepting transmissions then attempting to deduce information from them. Internet traffic is particularly vulnerable to this threat.
- Phishing — The act of sending spoofed e-mail messages falsely claiming to be from your banking institution to lure you into divulging personal information such as PIN or password for the purpose of identity theft. It often

contains a link to a website that contains logos, formatting, graphics and wordings that are convincing replicas of the banking institution's original site.

- Pharming — The act of exploiting the vulnerability of the Domain Name System (DNS) server software that allows a hacker to acquire the domain name of banking institution's original site and redirect traffic from the banking institution's site to a fraudulent site.
- Man-in-the-middle — This attack is an attack in which fraudsters are able to read, insert and modify messages between you and your banking institution without either party knowing that the link has been compromised.

4.4 Network Infrastructure of Internet Banking in Nepal

The security of the Nepalese Bank Internet banking application is addressed at three levels. The first concern is the security of customer information as it is sent from the customer's PC to the Web server. The second area concerns the security of the environment in which the Internet banking server and customer information database reside. Finally, security measures are in place to prevent unauthorized users from attempting to log into the online banking section of the Web site.

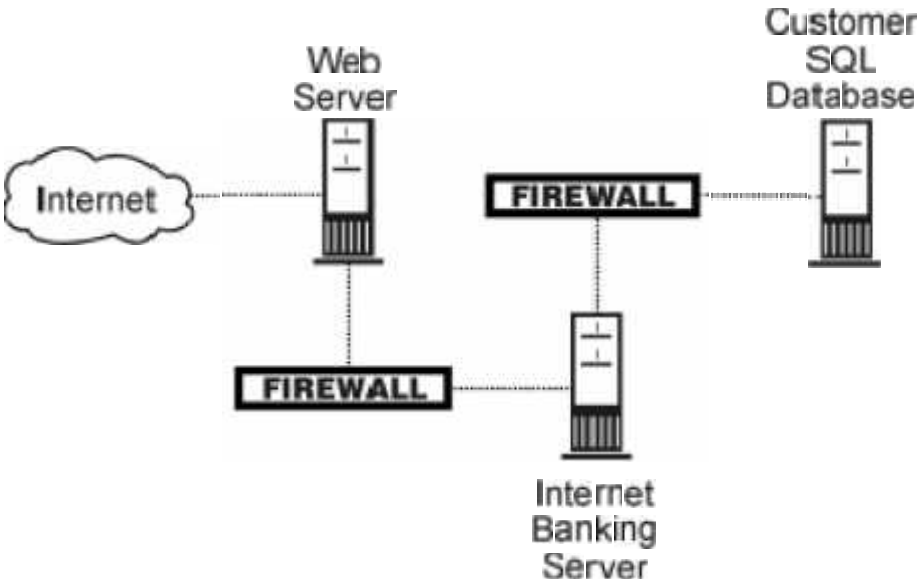

Figure 4 : Sample of System Architecture of Internet Banking

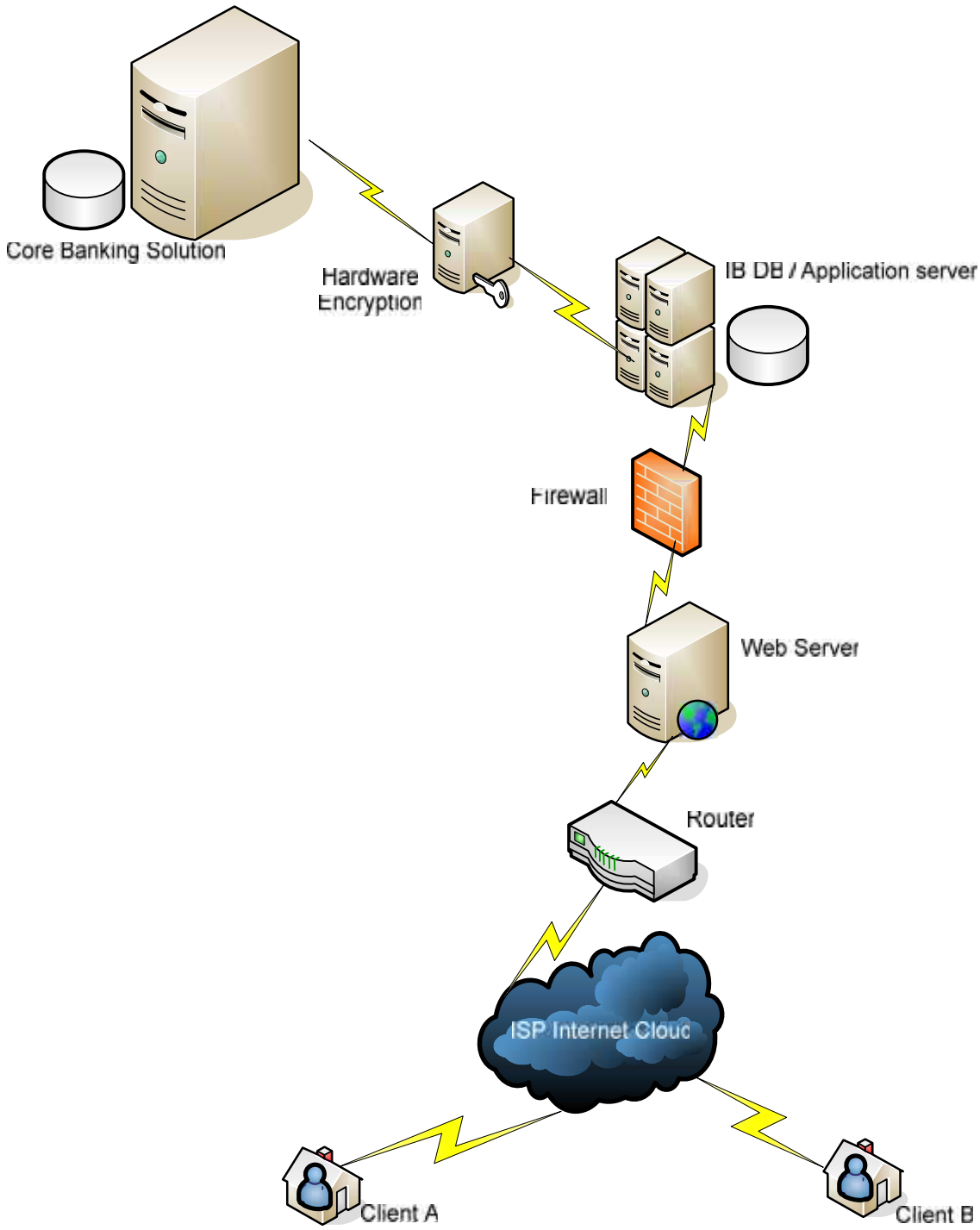

Figure 5 : Network Infrastructure of Internet Banking in Nepal

Data security between the customer browser and banks Web server is handled through a security protocol called Secure Sockets Layer (SSL). SSL provides data encryption, server authentication, and message integrity for a Internet connection. In addition, SSL provides a security "handshake" that is used to initiate the connection. This handshake results in the client and server agreeing on the level of security they will use and fulfills any authentication requirements

for the connection. Currently both RBB and NBL's online banking application supports data encryption at the highest level (128 bit). In order to get this level of encryption, you will need a browser that supports it. Both versions 3 and 4 of the most popular browsers support 40-bit encryption as a default, and have complete versions as well as patches that will support the stronger 128-bit encryption.

Requests for online banking information are passed on from the Web server to the Internet banking server. The Internet banking application is designed using a three-tiered architecture. The three-tiered architecture provides a double firewall, completely isolating the Web server from the customer information SQL database.

The World Wide Web interface receives SSL input and sends requests through a firewall over a dedicated private network to the Internet banking server. The World Wide Web interface is the only process capable of communicating through the firewall to the Internet banking server. Therefore, only authenticated requests communicate with the Internet banking server.

A security analyzer constantly monitors login attempts and recognizes failures that could indicate a possible unauthorized attempt to log into an account. When such trends are observed, steps will be taken automatically to prevent that account from being used.

Security concerns have been addressed from every angle within the architecture of the Internet banking application. Implementation of the SSL security protocol on the Web server and customer browser ensures authenticated data has been received from the customer. The three-tiered approach of the Internet banking application creates a double firewall which performs information requests over dedicated networks designed to handle specific functions. Placing all business logic and event logging within the Internet banking server creates a controlled environment which allows quick incorporation of Internet security technologies as they evolve. Finally, the security analyzer monitors login attempts in order to prevent unauthorized logins.

Use Cases

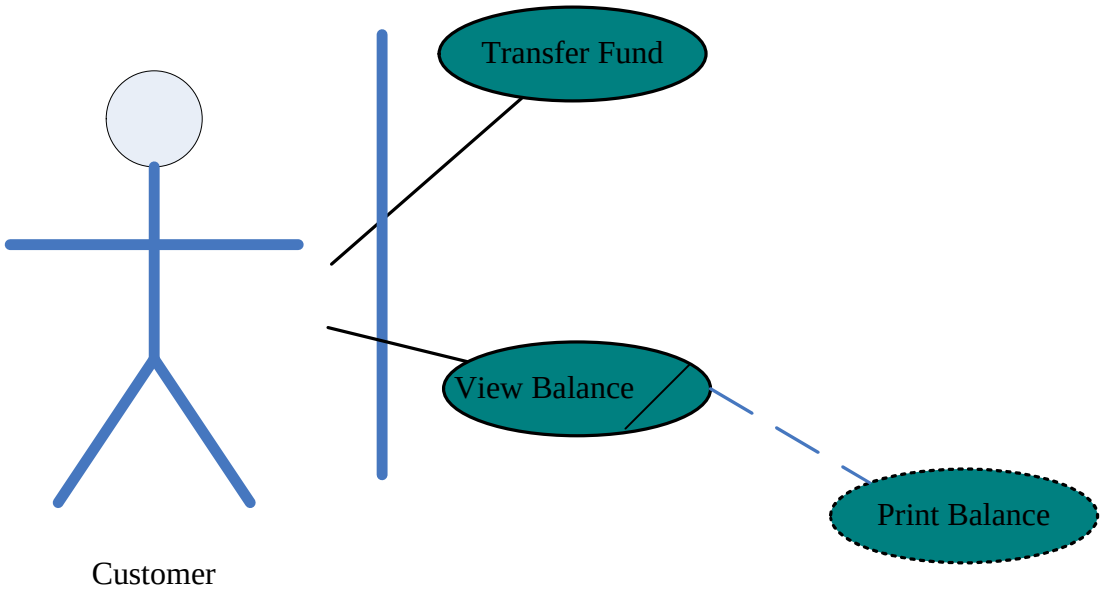

Figure 6 : Uses cases for Transaction

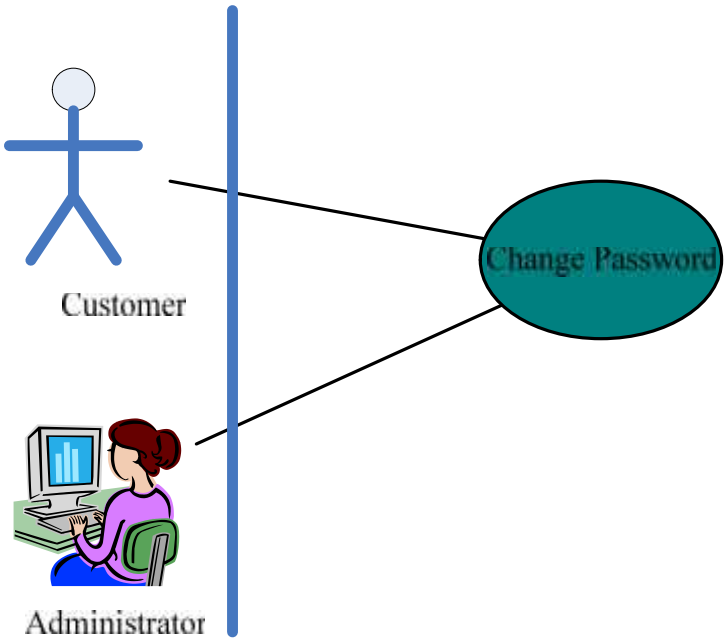

Figure 7: Use cases for Manipulation

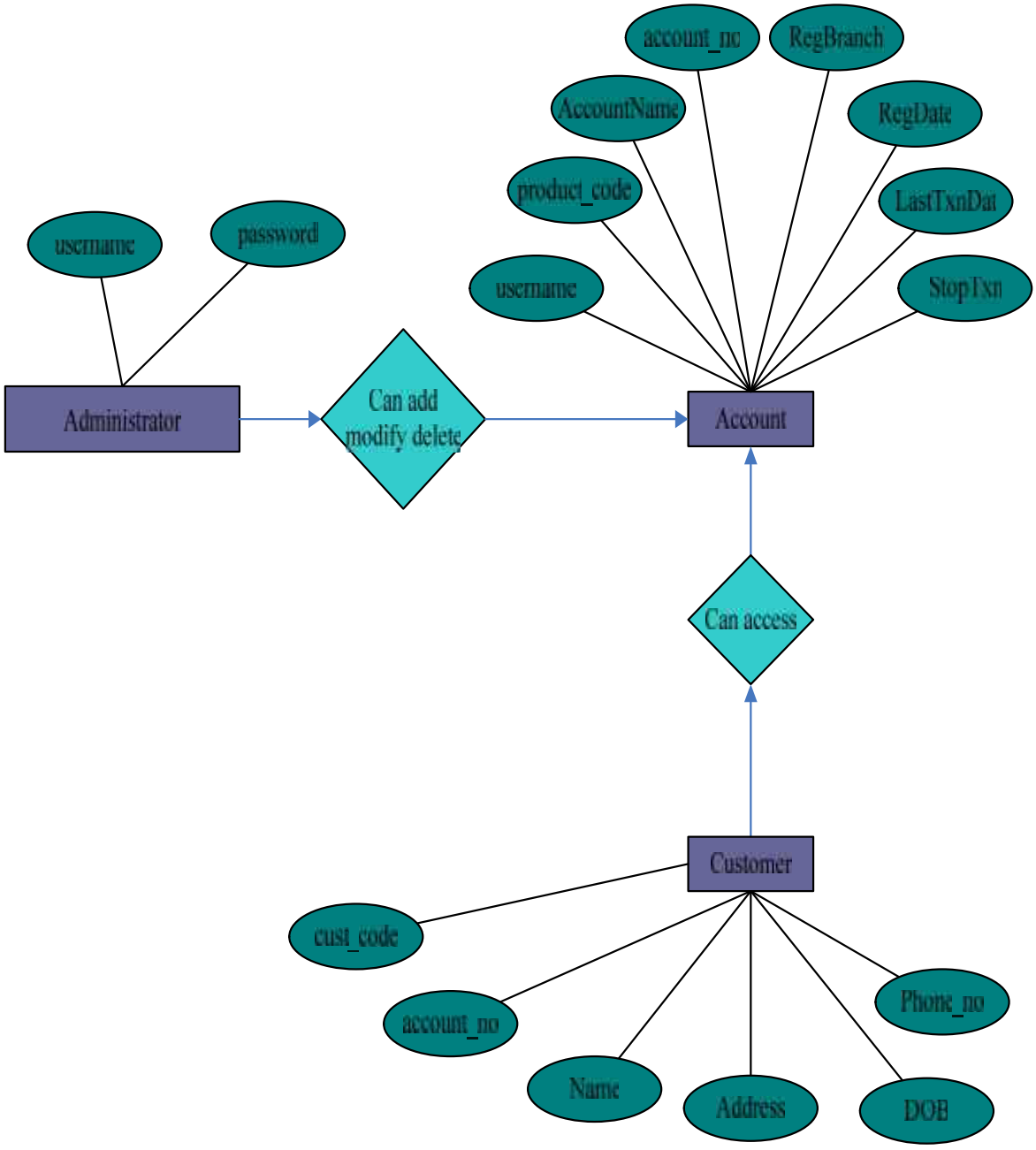

Figure 8: ER Diagram of Internet Banking

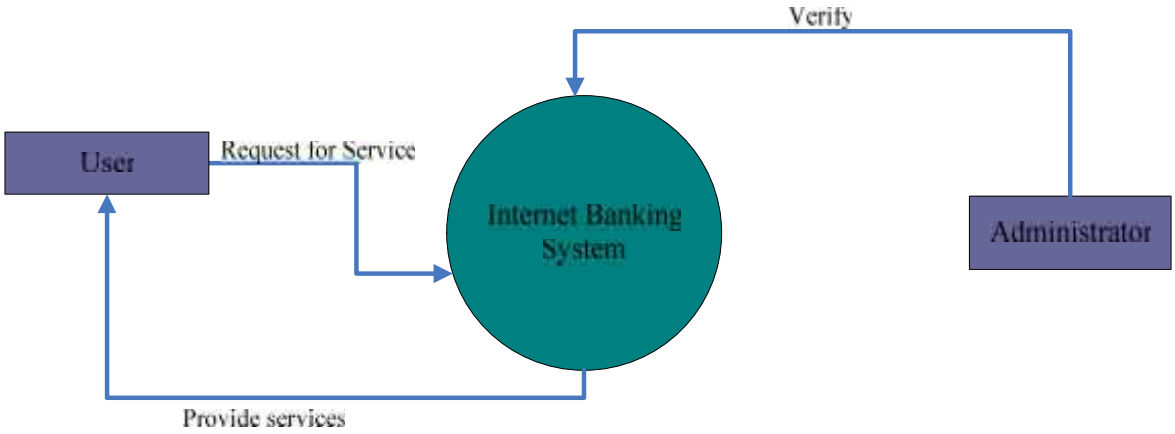

Figure 9 : Context Diagram

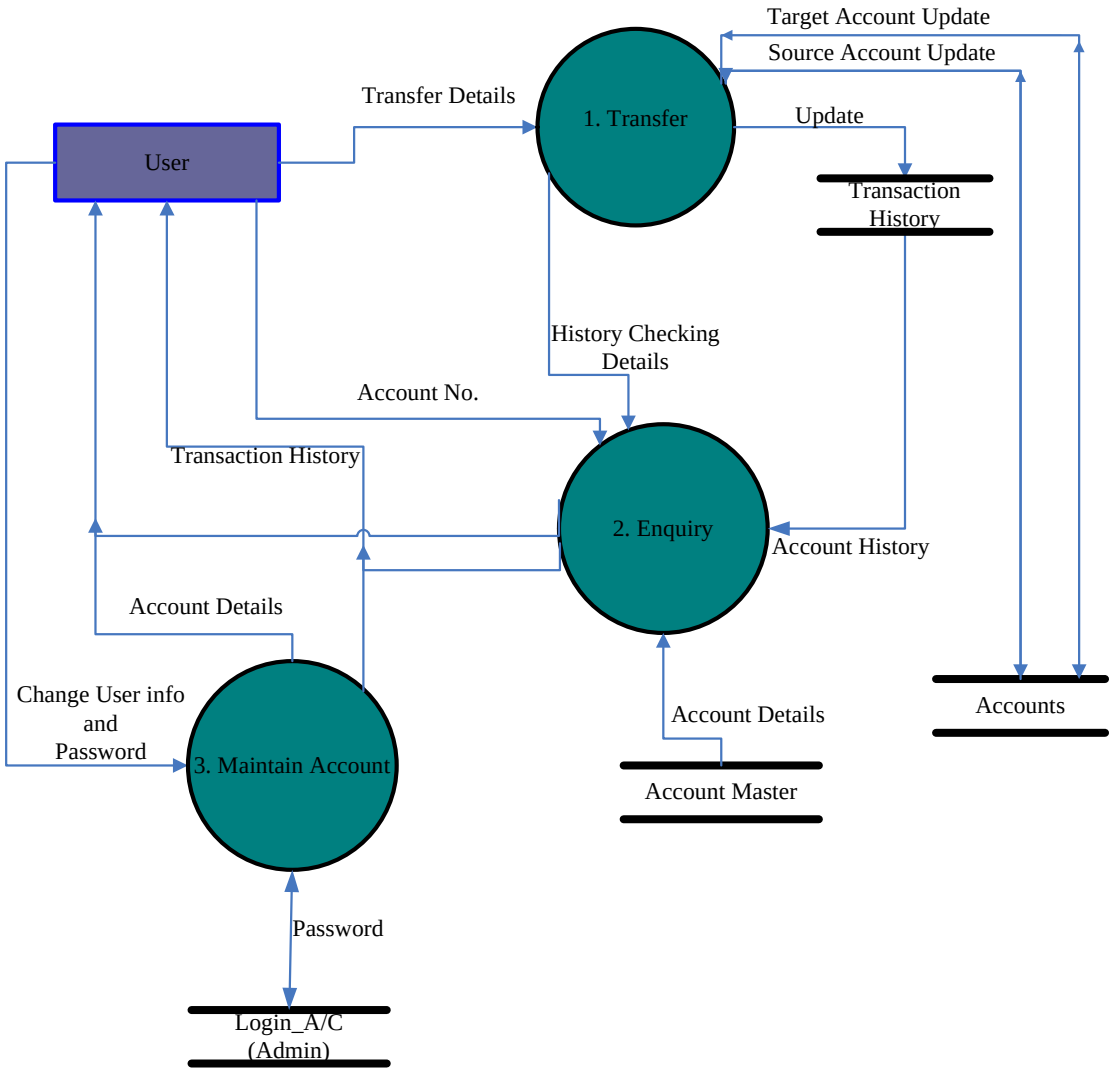

Figure 10: Top Level DFD Diagram

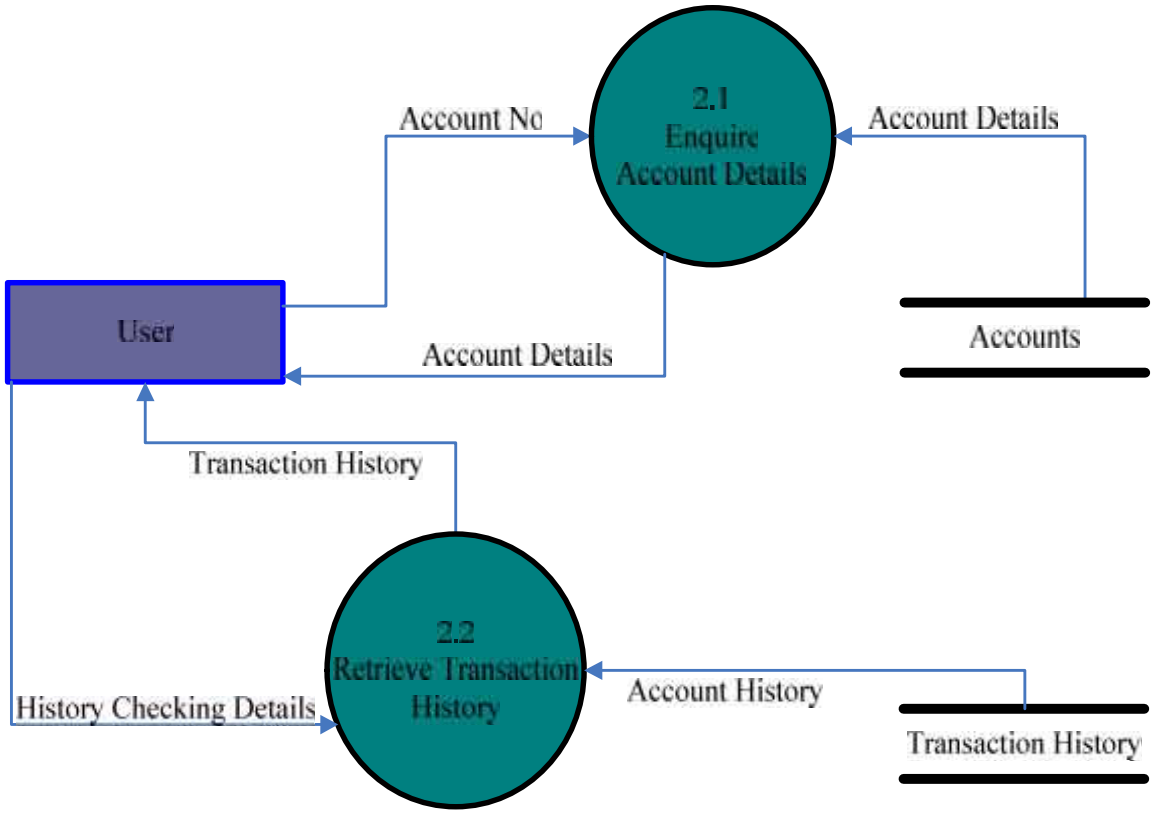

Figure 11: Logical Flow Diagram - Enquiry

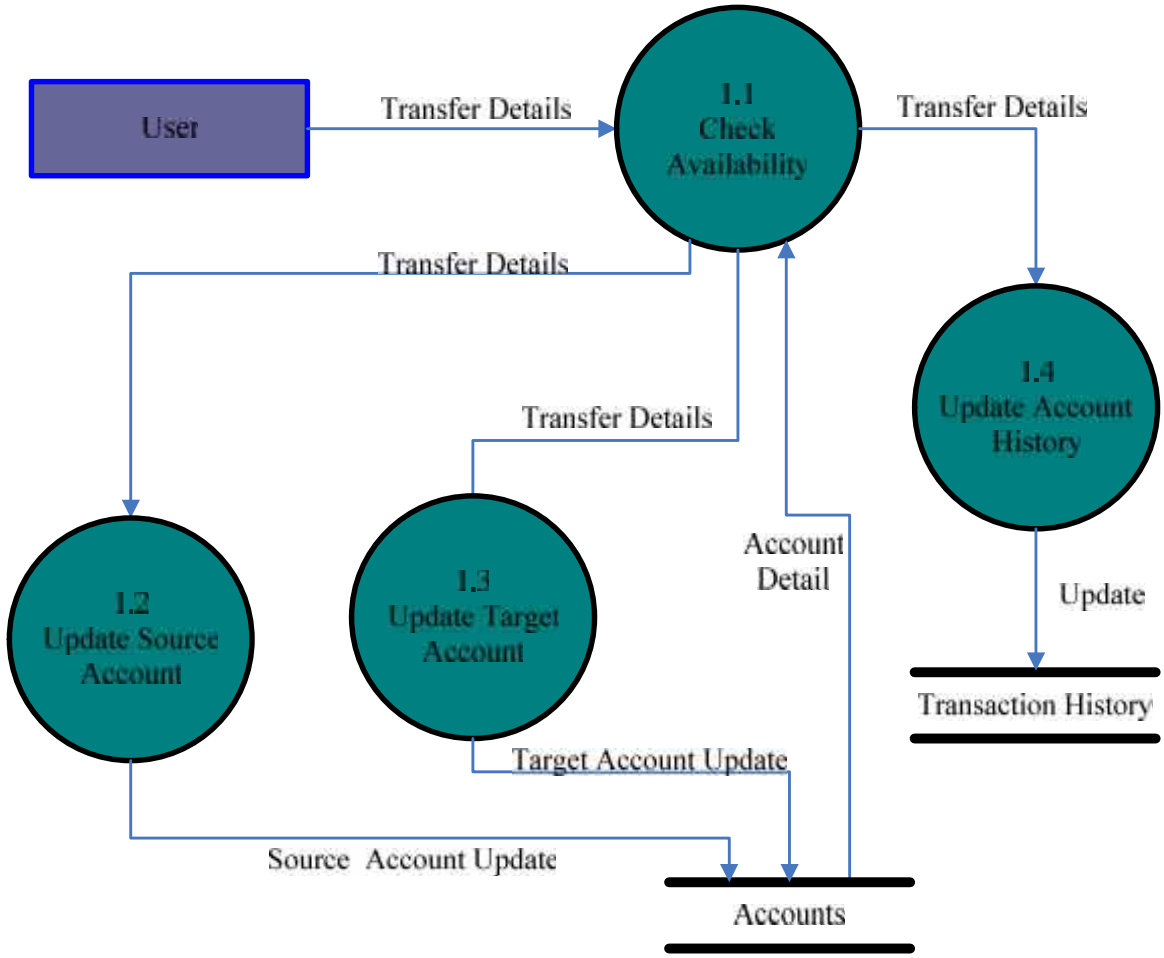

Figure 12: Logical Flow Diagram - Fund Transfer

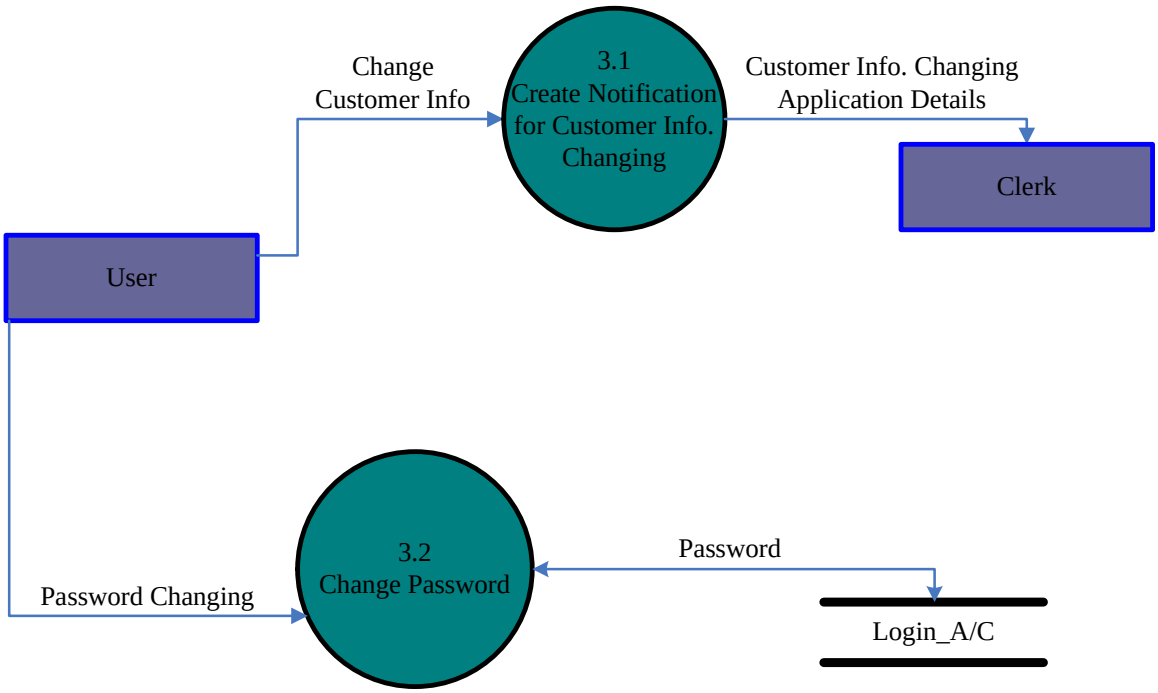

Figure 13 : Logical Flow Diagram - Maintain Account

Chapter V

CONCLUSION AND RECOMMENDATION

5.1 Conclusion

Today's world is all about information who have information and who is capable of manipulate that information to knowledge they will be success. And in another word, we can say that who have vital information they can rule the market. Business houses are getting success by selling information rather than any products.

During the doing this thesis, I found that these organization do not entertain to disclose all their information. Internet banking is all about service and security. So they do not want to disclose about the system they are using. Hackers and crackers are able to do some nasty in the system if they just know about the devices and the software any organization using. Because there is no such system which is not vulnerable, that’s why all system provides patches to make them more secure.

But after long procedure I am able to get little information about the systems these banks are using nowadays. On the basis of that little information I have complete my study, which itself is not complete study about the internet banking. Hope in future, new research will be carried on in this topic again and again because technology is that thing which will be change in every next day and new kinds of security measures will be developed to make more secure the system which banks are using nowadays.

At the last, I want to conclude with the security and the users of internet banking providers of Nepalese government banks. I found that the number of users of internet banking is very poor that’s why I recommended some marketing policy to implement by banks to increase number of internet banking users. About the security of internet banking, banks itself are not feel secure that’s why they are not providing all the services as internet banking which they are capable of also. Because of threat, Indian government also announces from this august to provide two factor authentication to all the services provider. So if the banks use Two Factor Authentication and Biometric devices as security measures then internet banking will be more secure.

5.2 Recommendation

6.2.1 Is Internet Banking Safe?

As in any other system, there are risks involved in Internet banking. However, potential risks are mitigated with banking institutions' continuous check on the security of the system and the care taken by you when using Internet banking services.

6.2.1.1 Actions Taken By Banking Institutions To Ensure Security

In offering Internet banking services, banking institutions have invested considerable resources and efforts to ensure that their Internet banking set up is safe for consumers. In addition, banking institutions are also required to comply with the minimum guidelines. Amongst the safety measures taken by banking institutions are:

- Regular tests of the system to ensure its reliability
- Provision of security arrangements
- to ensure a secure infrastructure:
  - A number of security measures such as encryption, firewalls, automatic log-off and monitoring tools
  - A system to detect and disable attacks from hackers
- A two-factor authentication method that provides two levels of checking to validate the user
- Undertake a periodic review every 6 months to assess possible risks and detect possible weaknesses in the banking institution's risk management system

5.2.1.2 Actions User Should Take To Ensure Security

Users have an important role to play in ensuring the safety of Internet banking transactions. Some of the recommended actions that you, as a bank customer, should practise are:

- Do not reveal your login ID and password or PIN
  - Memorise it and do not write it down anywhere
  - Do not send any personal information particularly your password or PIN via ordinary e-mail
  - Do not store your login ID and password or PIN on the computer
  - Change your password or PIN regularly and avoid using easy-to-guess passwords such as names or birthdays. Ideally, your password should be a combination of characters (uppercase and lowercase) and numbers
  - Do not respond to any request for your login ID and password or PIN over the phone, through fax, e-mail or pop-up message, no matter how official or important it may seem
  - Change your password or PIN immediately and notify your banking institution if you suspect any unauthorised use of your accounts or that someone else may know your password or PIN
  - Check your transaction history details and statements regularly to make sure that there are no unauthorised transactions on your accounts or additions to the list of registered payees
- Check for the right and secure website
  - Always enter the URL of the website directly into the web browser. You should avoid being re-directed to the website, or hyperlink to it from an e-mail or another website
  - Make sure that you are in the correct website before doing any online transactions or providing personal information
  - Ensure that you are in a "secure" website by checking the Universal Resource Locators (URLs) to ensure that it begins with "**https://**" instead of "http://" and look for a display of a closed padlock symbol on the status bar of your browser. However, you are cautioned that the URL and the closed padlock symbol, which represents the Secure Sockets Layer (SSL)

certificate, could also be forged. Therefore, you should exercise greater vigilance by checking the URL and the SSL certificate from the 'Page Properties' tab to confirm the authenticity of the website

- Install a web browser toolbar that alerts you of any known phishing fraud website to minimise the risk of falling into phishing scams

- Protect your personal computer from hackers, viruses and malicious programmes
  - Install a personal firewall and a reputable anti-virus programme to protect your personal computer from virus attacks, spyware or malicious programmes such as "Trojan Horse"
  - Ensure that the anti-virus and antispyware programmes are up-to-date and are running at all times
  - Keep your operating system and web browser up-to-date with the latest security patches in order to protect against weaknesses or vulnerabilities
  - Configure your browser to reject ActiveX controls to reduce the likelihood that spyware could be installed on your computer
- Be careful when downloading software
  - Always check the programme or attachment received with an updated anti-virus programme to ensure that it does not contain any virus that could attack your computer
  - Never download any file or software from sites or sources, which you are not familiar with or click on hyperlinks sent to you by strangers. Opening such a file, software or hyperlink could expose your system to a computer virus that could hijack your personal information, including your password or PIN
- Do not leave your computer unattended when logged in
  - Log-off from the Internet banking site when you leave your computer unattended, even if it is for a short while
- Always remember to log-off
  - Always log-off when you have completed your banking transactions
  - Clear the **memory cache** and **transaction history** after logging out from the website to remove your account information. This would avoid stored information from being retrieved by unwanted parties

- Other measures
  - Do not have other browser windows open while you are banking online
  - Avoid using shared or ‘planted’ or public personal computers, e.g at Internet cafes, to conduct your Internet banking transactions
  - Disable the “file and printer sharing” feature on your operating system
  - Contact your banking institution to discuss any security concern you may have on your online accounts, including remedies required

The implication of these findings and conclusions are that, banks need to play a leading role in influencing the perception, and there by the attitude and behavior of current and potential internet banking users. The outcome of this study has two practical implication and recommendation for banks.

5.2.2 Push Strategy

Awareness of internet banking services is essential in the early adoption stages. As internet banking services are still new in Nepal, effective presentations using all forms of media advertising such as leaflets, brochures, web pages, etc., will be useful to introduce the services to a wider audience and educate potential adopters, information about internet banking should be provided by bank tellers and bank assistants at branches. The information should include references to "time saving", "convenience" at anywhere any time, "low costs', and information availability. In addition, banks should design their web sites as effective delivery channels and offer information beyond banking services.

It is essential to provide a well designed and user-friendly web site to attract potential adopter's attention. The customer should not be required to expand a lot of effort or time, or undergo too great a change in behavior, to adopt internet banking services.

Information and instructions on the web should be provided in both Nepali and English in order to make the adopter comfortable. Wide publicity underscoring the benefits and ease of use by demonstrating internet banking services should be provided. This could be implemented by providing personal computers at bank branches accompanied by good documentation and bank assistance. Regular

surveying of customers' responses and opinions of the services should be conducted to ensure continuous improvement.

Reliability of access when need is one of the key encouragement factors. Although this 'reliability' partly depends on customers' networks, which were excluded from the study, internet banks can enhance accessibility by co-operating with ISPs to provide good quality internet access. Bank should also separate internal and external uses and give priority to external uses. While reliability is a key element from a customer's perspective, so is the security system. It must be enhanced continuously to guarantee integrity of online transactions as this will build customer confidence. Security provisions should be posted on banks' web sites clearly and understandably to create customer confidence and improve the trustworthiness reputation of banks. Security information should be provided in non-technical terms, and be accompanied by standard security statements. A perception of quality service will increase the bank's image for good services, accuracy and effectiveness. Failure of execution not only causes dissatisfaction and uncertainty to the customer but also makes the whole internet banking process more complex and less comprehensible.

In summary, recommendations for "supplier push" strategies are as follows:

1. **Build Customers' Recognization of Internet Banking :** Emphasize the advantages of internet banking services, i.e. time saving, low cost services, and convenience and information availability; and provide various types of information both financial and non-financial.

2. **Attract Customers to The Web Site :** provide a well-designed and user friendly web site; provide information in both Nepali and English languages; provide demonstrations in public places, e.g. bank branches, department stores, etc. Provide both electric and documentary documentations of online services; and regularly survey customers' responses to internet banking procedures and further develop the web site.

3. **Attract Customers by Ease of Access:** regularly monitor customers' access; implement at traffic management systems fro internal and external users; coordinate services with internet services providers.

4. **Build Customers' Confidence :** present the security used in both technical and non-technical terms; outline the procedure and information on how to cope with problems if they occur; and provide instructions on how to use internet banking services safely.

5. **Other Strategies :** offer incentives such as free internet access dial-up, frequent user benefits, member rewards, etc.

5.2.3 Pull Strategy

Bank should develop internet diffusion strategies by adopting "pull" strategies.

Increased diffusion will increase the number of internet banking adopters since they are likely to come from the internet population. Furthermore, support from the government and the industry regulator will positively affect internet banking services by increasing the confidence of the adopters.

Effective co-operation among banks has to be developed. The value of internet banking is increased by linking one activity with other both within banks and with outside suppliers, channels and customers. Furthermore, internet banks should collaborate with internet service providers because it will enable banks to better control quality of services as well as enhance adopters' accessibility. In addition, a high quality internet infrastructure should be provided since it is one of the primary requirements for internet usage.

Support from the government and industry regulator should be effective to increase the growth of internet banking services. The Nepalese government should be encouraged to initiate suitable steps to remove legal and regulatory barriers to ecommerce in general and internet banking in particular. In addition to lobbying the Nepalese government, banks should also proactively participate in improving internet services in order to increase online banking. For example, electronic laws should be promoted by the banks in order to reduce customers' perceptions of risks. Current cooperation has been commercial purposes, rather than for mutual benefit of the industry.

In summary, recommendations for "market pull" strategies are as follows :

1. **Increase service value by collaboration :** collaborate with internet service providers; offer free internet access; expand banking service across banks; and increase linkages to suppliers and merchants.

2. **Be proactive :** support the government to enact electronic commerce laws; work with the industrial regulator; and provide education on the uses of the internet and internet banking.

Customer-targeting strategies Internet banks should focus on people with high purchasing power as the first priority and attempt to shift them online. This requires extensive analyses of customers' needs and the provision of customized services that are of value to them.

In summary, recommendations for moderating factors are as follows :

1. **Target right customers :** persuade people in good positions and appropriate income to adopt the services.

2. **Provide value to customers :** monitor the historical bank usage of customers to know their needs; and provide customized services to customers.

5.3 Academic Contributions of the Study

This study makes significant contribution across all area of IT adoption and usage research and practice. These contributions are:

1. The development of a conceptual model that explains and predicts the factors that influence the adoption and acceptance of information technology/ system of the internet; and it's application regarding the new technology in the bank sector in Nepal, such as internet banking.

2. The empirical support for proposed hypothesis based on the integrative research framework and the literature;

3. It is potential to be generalized to nation-wide general organizational study.

The result is an indication of the good explanatory power of the model for intentions and can be used as a research model for further study on IT adoption.

BIBLIOGRAPHY

Akhtar, Mahmood. (2009). *Distributed Online Banking*. Retrieved July, 10 2009 from http://www.micsymposium.org/apache2-default/mics_2004/Akhtar.pdf

answers.com (2007). *Online Banking*. Retrieved March, 12 2007, from http://www.answers.com/Online%20Banking

bankrate.com (2007). *What is Online Banking?*. Retrieved June, 12 2009, from http://www.bankrate.com/brm/olbstep2.asp

Banstola, Amrit. (2007). *Prospects and Challenges of E-banking in Nepal*. The Journal of Nepalese Business Studies. Kathmandu; IV (1): 96-103.

Bishop, M. (2005). *Introduction to Computer Security*. US, Pearson Education, Inc.

Bajracharya, Anil (2008). *Internet Banking in Nepal*. A Master's Thesis, Biratnagar, P.U.

Booz-Allen and Hamilton. (1997). *Corporate Internet Banking: A Global Study of Potential*. http://www.boozallen.com/media/file/beyond_shared_services.pdf; Retrieved June 13 2009 The Impact of Remote Channel http://www.bah.com/viewpoints/insights/bank_brickless.htm

Bradley, L. & Steward, K. (2002). *A Delphi Study of the Drivers and Inhibitors of Internet Banking*. International Journal of Banking Marketing. http://www.emeraldinsight.com/10.1108/02652320210446715; 20 (6): 250-260.

Brogdon, C. (1999). *Banking and the Internet : Past, Present and Possibilities*. Internet WWW page, available at URL : http://wwwdb.standford.edu/pub/gio/CS99I/banking.html Version current as of July 15, 1999.

bytepile.com (2009). *RAID types - Classification*. Retrieved July, 14 2009, from http://bytepile.com/raid_class.php

Chircu, A. M, Kauffman, R. J. (2000). *Reintermediation Strategies in Business-to-Business Electronic Commerce*, International Journal of Electronic Commerce. Minneapolis, MN 55455, USA; University of Minnesota, 4(4): 7-42.

Crane, D.B., and Bodie, Z. (1996). *Form Follows Function: The Transformation of Banking.* Harvard Business Review, Boston, Mar/Apr, 74(2) : 109-117.

cronto.com *Beyond Phishing – De-Mystifying The Growing Threat Of Internet Banking Fraud*. Retrieved May, 23 2009, from http:// www.cronto.com

Daniel, E. & Storey, C. (1997). *On-line Banking: Strategic and Management Challenges*. London, Elsevier Science. Ltd.

Federal Financial Institutions Examination Council. (2001). *Authentication in an Internet Banking Environment*. Retrieved June 23, 2009 from http://www.ffiec.gov/press/pr031908.htm

Garykessler.com (2009). *An Overview of Cryptography*. Retrieved June, 23, 2009, from http://www.garykessler.net/library/crypto.html

Grimes. R. (2006). *E-commerce in Crisis: When SSL isn't Safe*". www.infoworld.com/pdf/special_report/2006/18SRmalware.pdf 5(2): 27-31.

Guru, Catalin (2002). *E-banking in Transition Economies: the Case of Romania*, Journal of Financial Services Marketing. Basingstoke.UK. Palgrave Macmillan Ltd. 6(4): 362 -379.

internet.com (2007). *Phishing.* Retrieved February, 22, 2007, from http://www.webopedia.com/TERM/p/phishing.html

Jayawardhena, C. and Foley, P. (2000). *Changes in the Banking Sector - The Case of Internet Banking in the UK*. Internet Research: Electronic Networking Applications and Policy. http://www.emeraldinsight.com/10.1108/10662240010312048

John D. Wright. (2002). *Electronic Banking: New Developments and Regulatory Risks*, IMF Seminars on Current Development. www.imf.org/external/np/leg/sem/2002/cdmfl/eng/wright.pdf

Karjaluoto, H. (2001). *Measuring attitudes towards Internet Banking : Empirircal evidence from Finland*. Proceedings of the European Marketing Academy Conference. Bergen, Norway, May 8-11, 2001.

Katz, J. and Aspden, P. (1997). *Motivations for and Barriers to Internet Usage: Results of a National Public Opinion Survey*. Internet Research: Electronic Networking Applications and Policy, http://www.emeraldinsight.com/Insight/html/Output/Published/EmeraldFullTextArticle/Pdf/1720070302.pdf : 70-188. Retrieved January 12, 2002

Kelly. C.J. (2005). *The Cost of Securing People's Privacy*. Computerworld. http://www.computerworld.com/s/article/101408/The_Cost_of_Securing_the_People_s_Privacy:31

Kotler, P. and Keller, K.L. (2006), *Marketing Management (12th Ed.)*. Upper Saddle River, N.J.,Pearson Prentice Hall.

Lemos, R. (2006). *Password Policies*, PC Magazine: Networking and Security. http://www.pcmag.com/article2/0,2817,1951040,00.asp

Lindgreen A., Antioco M. (2005), *Customer relationship management: The case of a European Bank*, Marketing Intelligence & Planning. http://www.emeraldinsight/com/10.1108/02634500510589903. 23(2):136-154.

Manandhar, Niraj (2007). *Design Process of a Mobile Banking Service*. Master Degree Thesis, Kathmandu, Shanker Dev Campus.

Mols, N.(1998). *The Behavior Consequences of PC Banking*, International Journal of Bank Marketing, http://www.emeraldinsight.com/10.1108/02652329810228190: 16(5):195-201

Nathan, L. (1999). "Community Banks are Going Online". Community and Banking, Federal Reserve Bank of Boston, www.your-community-bank.com:

newscientist.com (2006). "*Keep your fingers out of my account*", Technology. www.newscientist.com Retrieved February 14, 2007

Sathye, M. (1999). *Adoption of Internet Banking by Australian Consumers: An Empirical Investigation*, International Journal of Bank Marketing. http://www.emeraldinsight.com/10.1108/02652329910305689. 17(7):324-334.

Science Direct. (2006). *A Smart Answer to Online Fraud?* Card Technology Today. http://www.sciencedirect.com/science/journal/09652590, 18(5):10-11.

teachtarget.com (2007). *Biometrics.* Retrieved February 27, 2007, from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211666,00.html

Thapa, Devinder (2003). *Future Prospective of Online Banking in Nepal*. A Master's Thesis, Kathmandu, T.U.

Turban, E., Lee, J., King, D., and Chung, H.M. (2000). *Electronic Commerce: A Managerial Perspective*. Pretence Hall International Inc.

wda.org (2007). *SSL*. Retrieved February 19, 2007, from http://www.wda.org/Public/help/glossary.htm

Yadav, R., (2004, May). *IT revolution in Nepal*. Business Age, Kathmandu, 27

wikipedia.org (2009), *Hot Swapping*. Retrieved July, 14 2009, from http://en.wikipedia.org/wiki/Hot_swapping

http://blog.cronto.com/index.php?title=2fa_is_dead&more=1&c=1&tb=1&pb=1 Retrieved June 14, 2009

http://blog.cronto.com/index.php?title=e_crime_crowd_sourcing&more=1&c=1&tb=1&pb=1 Retrieved June 14, 2009

http://www.answers.com/topic/windows-2000. Retrieved June 14, 2009

http://www.comarch.eu/en/industries/finance/products/internet_banking Retrieved June 14, 2009

http://www.comarch.eu/r/res/fin/documents/folders/EN/Comarch_Internet_Banking_EN.pdf Retrieved June 14, 2009

http://www.intruguard.com/OnlineBankingSecurityfromDenialofServiceAttacks.html Retrieved June 14, 2009

http://www.microsoft.com/sqlserver/2005/en/us/top-30-features.aspx Retrieved June 14, 2009

http://www.nbl.com.np Retrieved June 14, 2009

http://www.pointbank.com/internet_banking.htm Retrieved June 14, 2009

http://www.rbb.com.np Retrieved June 14, 2009

http://www.webinternetbanking.com/internetbankingsystem.html Retrieved June 14, 2009

QUESTIONNAIRE

Dear respondent,

The following questionnaire is for my Master in Business Studies thesis entitled "Internet Banking in Nepal : A Case Study in Nepalese Government Bank". The information you provide is only for educational provision only. Thank you in advance for your cooperation and valuable time that you are dedicating.

Personal Information

Name of Bank : ……..

Name of Respondent :…….

The Respondent Position :……

1. When did your bank start offering Internet Banking ?

   ……

2. What are the facilities you are providing with Internet Banking ?

   ……

3. What is the current status of internet banking in Nepalese government bank ?

   ……

4. Where is the bank's website hosted ?

   ……

5. Who is the responsible for maintaining the bank's web site ?

   ……

6. Does the bank have a contact with third party to the web site host ?

   ……

7. How many customer do you have as a internet bank customer ?

   ……

8. Is it tested, before offering to customers ? If yes, then what kind of test you have done ?

   ……

9. How many customers can benefited at a time ?

   ……

10. Which is a mean time that mostly users access bank's website ?

    ……

11. How does bank connect to the internet ?

    ……

12. Is the bank's web site reviewed internally ?

    ……

13. Are the banks using sufficient risk management tools to assure secure financial transactions ?

    a. Yes b. No

    if yes, then how ?

    ……

    ……

14. Are links and interactive programs checked for accuracy and functionality ? If yes, who checks them and how frequently ?

    ……

15. Who is responsible for doing the implementation of the updates/patches ? Are they tested before putting into production ?

    ……

16. Does management keep up-to-date on addressing newly disclosed security threats to the computer operating system and application software ?

……

17. What are the devices used in your system ? Please mention its serial number also.
    a. …….
    b. ……..
    c. ……..
    d. ……..
    e. ……..
18. Who is responsible of installing, configuring and updating the firewalls ?

    ……

19. Who is responsible for monitoring firewall activities ?

    ……

20. How frequently are the firewalls being monitored ?

    ……

21. Are all unused services blocked at the firewall ? If yes, then what ports are left open at the firewall ?

    ……

    ……

22. Are controls in place restricting physical access to computer hardware, software and communication equipment ? If yes, please explain.

    ……

    ……

23. Do employees have access to customer passwords ?

    a. Yes b. No.

24. Are safeguards in place to detect and prevent duplicate transactions ?

    a. Yes b. No

    If yes, then please specify.

    ……

    ……

25. At what level is sensitive data encrypted ?

    a. 40 bit b. 128 bit c. others ……

26. Is electronic banking training provided to other officers and employees of the bank ?

    a. Yes b. No

27. Do IT personnel participate in training process ?

    a. Yes b. No.

    If yes, what types of programs ?

    ……

28. What was your reasoning for offering Internet Banking and/or any other electronic banking services ?

    a. Profit b. Convenience c. Retain customers

    d. Competition d. New customers e. Customers' request

    f. Others, if any : ……..

29. Are you satisfied with this service in you bank ? Please give reason.

    ……

    ……

30. What are the reasons that customer choose your internet banking instead of private bank's internet banking service ?

    ……
    ……

31. Is your customers are satisfied with your service ?

    .....

32. What are the new features you are going to provide to your customer ?
    .....
    .....
    .....
33. How many cost you have invested to run internet banking ?

    .....

34. Please draw your network architecture. Just to display how you have managed your network devices.