



**TRIBHUVAN UNIVERSITY
INSTITUTE OF ENGINEERING
PULCHOWK CAMPUS**

THESIS NO.: 069/MSCS/656

Security Analysis and Comparison of Nepalese Internet Banking Web Applications

**by
Keshav Raj Joshi**

**A THESIS
SUBMITTED TO THE DEPARTMENT OF ELECTRONICS AND COMPUTER
ENGINEERING IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE IN COMPUTER SYSTEM AND
KNOWLEDGE ENGINEERING**

**DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING
LALITPUR, NEPAL**

MAY, 2016

Security Analysis and Comparison of Nepalese Internet Banking Web Applications

by

Keshav Raj Joshi

069/MSCS/656

Thesis Supervisor

Dr. Arun Kumar Timalina

A thesis submitted in partial fulfillment of the requirements for the degree of Master of
Science in Computer System and Knowledge Engineering

Department of Electronics and Computer Engineering
Institute of Engineering, Pulchowk Campus
Tribhuvan University
Lalitpur, Nepal

May, 2016

COPYRIGHT ©

The author has agreed that the library, Department of Electronics and Computer Engineering, Institute of Engineering, Pulchowk Campus, may make this thesis freely available for inspection. Moreover the author has agreed that the permission for extensive copying of this thesis work for scholarly purpose may be granted by the professor(s), who supervised the thesis work recorded herein or, in their absence, by the Head of the Department, wherein this thesis was done. It is understood that the recognition will be given to the author of this thesis and to the Department of Electronics and Computer Engineering, Pulchowk Campus in any use of the material of this thesis. Copying of publication or other use of this thesis for financial gain without approval of the Department of Electronics and Computer Engineering, Institute of Engineering, Pulchowk Campus and author's written permission is prohibited.

Request for permission to copy or to make any use of the material in this thesis in whole or part should be addressed to:

Head
Department of Electronics and Computer Engineering
Institute of Engineering, Pulchowk Campus
Pulchowk, Lalitpur, Nepal

Recommendation

The undersigned certify that they have read and recommended to the Department of Electronics and Computer Engineering for acceptance, a thesis entitled “**Security Analysis and Comparison of Nepalese Internet Banking Web Applications**”, submitted by **Keshav Raj Joshi** in partial fulfillment of the requirement for the award of the degree of “**Master of Science in Computer System and Knowledge Engineering**”.

.....
Supervisor: Dr. Arun Kumar Timalina

Assistant Professor
Department of Electronics and Computer Engineering
Institute of Engineering
Pulchowk Campus

.....
External Examiner: Mr. Roshan Regmi
Head Information Technology
NMB Bank Ltd.

Departmental Acceptance

The thesis entitled “**Security Analysis and Comparison of Nepalese Internet Banking Web Applications**”, submitted by **Keshav Raj Joshi** in partial fulfillment of the requirement for the award of the degree of “**Master of Science in Computer System and Knowledge Engineering**” has been accepted as a bonafide record of work independently carried out by him in the department.

Dr. Dibakar Raj Pant

Head of the Department

Department of Electronics and Computer Engineering,

Pulchowk Campus,

Institute of Engineering,

Tribhuvan University,

Nepal.

ACKNOWLEDGMENT

It is a great pleasure for me to acknowledge the assistance and contributions of many individuals in making this thesis a success. I would like to extend thanks to many people who played an important role in accomplishing of this thesis work. First and foremost, I would like to thank my supervisor, **Dr. Arun Kumar Timalina**, for his assistance, ideas, and feedbacks during the process in doing this thesis. Without his guidance and support, this work cannot be completed.

Secondly, I would like to express my sincere gratitude to our Head of Department **Dr. Dr. Dibakar Raj Pant**, Prof. **Dr. Sashidhar Ram Joshi**, Prof **Dr. Subarna Shakya**, **Dr. Aman Shakya**, **Dr. Sanjeeb Prasad Panday** and Mr. **Manoj Ghimire** for their encouragement and precious guidance during the thesis work. I would like to thank Department of Computer and Electronics, Pulchowk Campus for providing the opportunity to have a thesis.

I also wish to thank my classmates and friends who have helped in completing this thesis work.

Lastly, I wish to express my sincere gratitude to my family for their encouragement and moral support.

ABSTRACT

Banking industry is considered one of many businesses that have taken advantages of the internet and IT development by introducing internet banking service to their customers that brings many benefits to banks and customers. However information security risks are associated with internet banking. In this research a new way to look at mathematics, multi criteria decision making (MCDM), is used. This research analyzes the security of existing deployments of internet banking services from the perspective of end user, whose main goal is completing the online transaction securely. Many internet banking security parameters are taken and given weight according to their security effectiveness with the help of research papers, and then existing deployments are compared based on these parameter weights by using MCDM algorithm. Context authentication has become increasingly important in internet banking, which involves confidential data that belong to users who trust their banks. Developing a usable and secure authentication approach and method is the most challenging area for researchers in the fields of security and human-computer interaction. Along with MCDM, a new approach with two factor user authentication system is suggested which improves current authentication system to an extent. This model doesn't allow users to login same account from different places simultaneously and any such activities are notified to genuine user.

Keywords: - Information security, Internet banking system, Multi-Criteria Decision Making, User authentication.

TABLE OF CONTENTS

COPYRIGHT ©	ii
Recommendation	iv
Departmental Acceptance	v
ACKNOWLEDGMENT	vi
ABSTRACT	vii
LIST OF TABLES	x
LIST OF FIGURES	xi
LIST OF ABBREVIATIONS	xiii
CHAPTER 1: INTRODUCTION	1
1.1 BACKGROUND.....	1
1.2 MOTIVATION OF THE THESIS.....	6
1.3 OBJECTIVES OF THE THESIS.....	6
1.4 OUTLINE OF THE THESIS	6
CHAPTER 2: LITERATURE REVIEW	8
2.1 INTERNET BANKING GENERAL REVIEW.....	8
2.2 THE REASONS OF INTERNET BANKING DEVELOPMENT	9
2.3 BENEFITS OF INTERNET BANKING	10
2.4 LIMITATIONS OF INTERNET BANKING.....	11
2.5 INTERNATIONAL TRENDS IN INTERNET BANKING.....	12
2.6 CHALLENGES IN INTERNET BANKING FOR DEVELOPING COUNTRIES	13

2.7 INFORMATION SECURITY	14
2.8 BANKING SECURITY	16
CHAPTER 3: RESEARCH METHODOLOGY	26
3.1 OVERVIEW OF MULTI-CRITERIA DECISION MAKING.....	26
3.2 IDENTIFY CRITERIA AND MEASURES	28
3.3 DATA COLLECTION.....	37
3.4 SCALING EACH MEASURE AND CALCULATING WEIGHT.....	38
3.5 USER AUTHENTICATION	38
3.6 USABILITY AND COST.....	42
CHAPTER 4: RESULT AND DISCUSSIONS	44
4.1 DATA INTERPRETATION AND RESULT.....	44
4.2 SENSITIVITY ANALYSIS.....	45
4.3 IMPLEMENTATION OF PROPOSED USER AUTHENTICATION SYSTEM.	49
4.4 CONCLUSION AND RECOMMENDATION	49
REFERENCES.....	51
APPENDIX A	54

LIST OF TABLES

Table No.	Title	Page No.
2.1	The proposed layered multi factor user authentication system.....	20
3.1	Execution rate for sparse and dense data file.....	30
3.2	Comparison between AES and 3DES	30
3.3	Cipher strength rating guide	31
3.4	Protocol support rating guide	32
3.5	Type of measures.....	37
3.6	Collected data for three different banks.....	37
3.7	Weight of different parameters	38
4.1	Weighted score of different bank.....	44

LIST OF FIGURES

Figure No.	Title	Page No.
2.1	Banking channel architecture.....	19
2.2	Model for internet banking system with fingerprint recognition.....	21
3.1	Existing internet banking authentication system.....	40
3.2	Existing authentication system if another user tries with same username and password from other location/device at same time.....	40
3.3	Proposed internet banking authentication model.....	41
4.1	Numerical Incremental sensitivity analysis comparing bank A & B.....	46
4.2	Numerical incremental sensitivity analysis comparing bank B & C.....	47
4.3	Numerical incremental sensitivity analysis comparing bank A & C.....	47
4.4	Numerical incremental sensitivity analysis for banks D, E, F & G	48
A.1	User registration page.....	54
A.2	User credentials entered.....	54
A.3	Request to enter one time password.....	55
A.4	One time password sent on email.....	55
A.5	User logged in successfully.....	55
A.6	Denied login access on trying to login from another location on same time.....	56

A.7	An email sent to genuine user notifying about invalid login attempt.....	56
A.8	Login page on entering wrong username and/or password.....	57
A.9	Message on entering wrong one time password.....	57

LIST OF ABBREVIATIONS

CISA	Certified Information Systems Auditor
COBIT	Control Objectives for Information and Related Technology
ICT	Information and Communications Technology
ISACA	Information Systems Audit and Control Association
IP	Internet Protocol
IT	Information Technology
MCDM	Multi-Criteria Decision Making
OTP	One Time Password
PC	Personal Computer
PKI	Public Key Infrastructure
SA	Sensitivity Analysis

CHAPTER 1: INTRODUCTION

1.1 BACKGROUND

Banking industry is considered one of many businesses that have taken advantages of the internet and IT development by introducing internet banking service to their customers that brings many benefits to banks and customers. Internet banking processes have given banks customers the full power to control their bank accounts from any place with the availability of the internet at anytime. The secret of the internet banking that attracts many customers is "the round-the-clock availability and ease of transactions and avoidance of queues and restrictive branch operating hours". The number of users using online banking continues to growth along with the number of internet users around the world.

Despite the fact that both the internet and internet banking services have brought many benefits to banks and their customers, there is a dark side of these technologies and can lead to severe consequences. A recent research about the dark side of the internet shows that internet users can be affected by many danger risks such as viruses, phishing emails, confidential data theft, online fraud and others. The reasons behind the growth of these risks are the increase in internet users, the rapid technological development such as smart phones and social networks, and the difficulty of discovering some types of risks.

Banks should take significant steps to protect their information from any type of breaches. For example, implementing updated security controls, using encrypted data mechanism, and educating customers about risks and how they can protect themselves and using sophisticated authentication mechanisms. The importance of information security to banks comes from the sensitive date held by banks about customers such as account numbers, usernames and passwords that enable customers to access their banks' accounts online. There are some security requirements that banks must achieve to protect their information from security risks which are, authentication, access control, confidentiality, integrity, availability and non-repudiation. Therefore information security

is essential to a financial institution's ability to deliver internet banking services, protect the confidentiality and integrity of customer information, and ensure that accountability exists for changes to the information and the processing and communications systems.

Information Systems Security Audit is an independent review and examination of system records, activities and related documents to determine the adequacy of system control ensure compliance with established security policy and approved operational procedures, detect breaches in security so as to verify whether data integrity is maintained, assets are safeguarded, organizational goals are achieved effectively and resources are used efficiently. Security audit is a systematic, measurable technical assessment of how security policies are built into the information systems.

The three fundamental features of an information system that gets tested in course of security audit are assessment of confidentiality, availability and integrity of the information systems assets. The principle screening variables are various conceivable physical and logical security threats.

The purpose of any audit will be essentially to examine three basic compliances in terms of Confidentiality, Integrity and Availability (CIA):-

- Confidentiality concerns the protection of sensitive information from unauthorized disclosure. Keeping in view the level of sensitivity of the data the stringency of controls over its access should be determined.
- Integrity refers to the accuracy and completeness of the information as well as to its validity in accordance with business values and expectations. It is an important audit objective as it provides assurance to the management as well as the users that the information can be relied and trusted upon. It also includes reliability, which refers to degree of consistency of the system to function.
- Availability relates to information and information systems being available and operational when they are needed. It also concerns safeguarding of necessary resources and associated capabilities. This implies that the organization has measures

in place to ensure business continuity and timely recovery can be made in case of disasters.

The use of computers, computer based information systems and internet based systems have pervaded deep and wide in every modern day organization. An organization must exercise control over these computer and internet based information systems because the cost of errors and irregularities that may arise in these systems can be high and can even challenge the very existence of the organization. An organizations ability to survive can be severely undermined through corruption or destruction of its database, decision making errors caused by poor-quality information systems, losses incurred through computer abuses, losses incurred through failure of user authentications, loss of computer assets and their control on how the computers are used within the organization. Therefore managements across the world have deployed specialized auditors to audit their information systems to find out gaps between declared policies/frameworks and actual use and shortcomings in the information system design and usage.

Traditional methods of security accreditation are becoming increasingly ineffective in maintaining security, irrelevant and damaging to the effectiveness and efficiency of IT systems and the organizations they serve. It is important to move towards a genuine risk-management approach to IT security [1]. The Internet banking service reduces costs and increases profits for banks, while it provides users with convenience for the transactions which are not executed in the face-to-face format by overcoming the limitation of time and space [2]. Auditing information systems security is difficult and becomes crucial to ensure the daily operational activities of organizations as well as to promote competition and to create new business opportunities [3]. As globalization and new information technology become more popular, information systems have begun supporting platforms that support enterprise and economy, as long as enterprises introduce process-aware information system to support business operation, there exists risk in business process [4]. Nowadays it is almost impossible to find a branch of human activity where there is no information technology. Because of IT technologies rapid growth the companies often encounter with the need of increasing the information security. However, information

security is a comprehensive system that is very difficult to manage. As a consequence, there is a risk to the information system safety in the most organizations.

With that in mind, information security audit becomes a good solution to this problem. The audit process is highly expensive in terms of time and cost as well as in the degree of involvement of human resources. Information security auditing plays key role in providing any organization's good security level [5].

Banks have traditionally been in the forefront of harnessing technology to improve their products, services and efficiency. Banks have, over a long time, been using electronic and telecommunication networks for delivering a wide range of value added products and services. The delivery channels include direct dial-up connections, private networks; public networks etc and the devices include telephone, Personal Computers(PCs) including the Automated Teller Machines, etc. With the popularity of PCs, easy access to internet and World Wide Web (WWW), internet is increasingly used by banks as a channel for receiving instructions and delivering their products and services to their customers. This form of banking is generally referred to as internet banking, although the range of products and services offered by different banks vary widely both in their content and sophistication.

The levels of banking services offered through internet can be categorized in to three types:

- i. The Basic Level Service is banks' website which disseminate information on different products and services offered to customers and members of public in general. It may receive and reply to customers' queries through e-mail,
- ii. In the next level are simple transactional websites which allow customers to submit their instructions, applications for different services, queries on their account balances, etc, but do not permit any fund-based transactions on their accounts,
- iii. The third level of internet banking services are offered by fully transactional websites which allow the customers to operate on their accounts for transfer of funds, payment of different bills, subscribing to other products of the bank and to

transact purchase and sale of securities, etc. The above forms of internet banking services are offered by traditional banks, as an additional method of serving the customer or by new banks, who deliver banking services primarily through internet or other electronic delivery channels as the value added services. Some of these banks are known as ‘virtual’ banks or ‘internet only’ banks and may not have any physical presence in a country despite offering different banking services.

Security of internet banking transactions is one of the most important areas of concerns to the regulators. Security issues include questions of adopting internationally accepted state-of-the art minimum technology standards for access control, encryption / decryption, firewalls, verification of digital signature, Public Key Infrastructure (PKI), security feature of user accounts etc. The regulator is equally concerned about the security policy for the banking industry, security awareness and education.

Multiple-criteria decision-making (MCDM) optimization technique is used in this research work. Multiple-criteria decision-making or multiple-criteria decision analysis (MCDA) is a sub-discipline of operations research that explicitly considers multiple criteria in decision-making environments. In our daily lives or in professional settings, there are typically multiple (conflicting) criteria that need to be evaluated in making decisions so in such situation multi-criteria decision making techniques are used.

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users’ information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. The permissions and folders returned define both the environment the user sees and the way user can interact with it, including hours of access and other rights. The process of an administrator granting rights and the process of checking user account permissions for access to resources are both referred to as authorization. The privileges and preferences granted for the authorized account depend on the user’s permissions, which are either stored locally or on the authentication server. The settings defined for all these environment variables are set by an administrator.

With the increasing number of internet-enabled devices, reliable machine authentication is crucial to allow secure communication in home automation and other networked environments. In the internet of things scenario, which is increasingly becoming a reality, almost any imaginable entity or object may be made addressable and able to exchange data over a network. It is important to realize that each access point is a potential intrusion point. Each networked device needs strong machine authentication and also, despite their normally limited activity, these devices must be configured for limited permissions access as well, to limit what can be done even if they are breached

1.2 MOTIVATION OF THE THESIS

Every day the number of people who uses the internet banking system is increasing and the banking transactions through internet banking are also increasing. Along with these transactions a number of cyber frauds and security weaknesses are associated which causes the customer's economic and privacy loss. Goal and focus of the research work is to identify the most secured internet banking system among multiple choices deployed by different banks and to make strong user authentication system in internet banking web applications.

1.3 OBJECTIVES OF THE THESIS

The objectives of this thesis are:

- To compare the internet banking web application security of different banks using multi-criteria decision making optimization technique.
- To enhance current user authentication system used on internet banking system.

1.4 OUTLINE OF THE THESIS

Chapter one provides the introduction where brief background and motivation of this thesis are illustrated followed by the objective and motivation.

Chapter two reviews the literature, which includes information security standards and literature survey of different IEEE journals and papers.

Chapter three describes the methodological processes by showing detailed optimization algorithm, data collection and analysis and proposed user authentication system.

Chapter four presents the results derived from the method explained, its analysis and sensitivity analysis of the result. Along with this, chapter four describes about the implementation of suggested user authentication system.

CHAPTER 2: LITERATURE REVIEW

2.1 INTERNET BANKING GENERAL REVIEW

The actual emergence of internet banking has been linked with the internet and the growth of technology evolution. Banks have been attracted by the internet and technology in offering financial services via the web. The history of internet banking dates back to 1981, when four banks in New York (Citibank, Chase Manhattan, Chemical and Manufacturers Hanover) initiated home banking services with the use of the videotext system. Later on, between 1983 and 1985, the first UK's internet banking was launched by Nottingham Building Society and the Bank of Scotland. Since the early 90s and after the arrival of the web, doors have been opened for financial institutions to offer their services online. The first online service using the web was introduced by Stanford Federal Credit Union in 1994 and was offered to all of its members. The rapid growth in the number of Internet users can lead to more users accessing their banks account via the internet [6].

Bank information is compromised by skilled criminal hackers by manipulating a financial institution's online information system, spreading malicious bank Trojan viruses, corrupt data, and impedes the quality of an information system's performance. So at present customers can do banking online which is easy and time saving and at the same time internet banking systems are vulnerable to threats. So one of the major concerns of people with respect to internet banking is the safety related to data of bank account, transactional information and also the access path of their accounts. Even the Nepal Rastra Bank (NRB) that is the main body has been issuing various directions and recommendations from time to time to strengthen cyber security of banks operating in Nepal. Further, online banking becomes less secure if users are careless or computer illiterate. An increasingly popular criminal practice is to gain access to a user's finances is phishing and other threats include malware, viruses, theft of user identity and password through other means etc. So if clients are going to use online banking to conduct financial transactions, they should make themselves aware of the risks and take precautions to minimize them [7].

IT audit originated in the United States in the 1960s. In the early 1960s, IBM published "electronic data processing audit" and "The audit rules and organization methods with electronic data processing ", which rule new internal audit rules and organizational methods within electronic data processing environment. In 1968, the United States Institute of Certified Public Accountants published "Accounting Audit and Computer", which had made technical requirements for IT audit. In 1969, the International Information Systems Audit and Control Association (ISACA) set up. This is the only international organization in the IT audit field so far. In 1977, the United States Institute of Internal Auditors issued the famous paper "Auditing possibility and rules research in system." In 1985, the Industrial Policy Bureau of Japan issued "IT auditing standards," and added the "IT auditors test" in the whole of the Japanese software proficiency test for the aim to cultivated talents engaged in IT audit. From the 1990s, with the continuous development of information technology, IT audit has been developing rapidly.

ISACA, which headquartered in Chicago, has set up 160 branches in more than 100 countries and regions, institute and promulgated the IT auditing standards and practice guidelines, and so on. These rules can provide norms and guidelines for IT auditors. The association organizes the annual CISA examination. The staff (that is, CISA) that passes the qualifying examination can make independent IT audit according with IT auditing standards and practice guidelines. In the United States, Japan and other developed countries, IT audit has been universal [8].

2.2 THE REASONS OF INTERNET BANKING DEVELOPMENT

The properties of the internet make it an ideal medium for delivery of banking products and services. Both financial entities and customers of financial products and services are benefiting from the spread of online banking services. Some banks also allow services such as stock market transactions, utility payment and the submission of standardized accounting payment files for bank transfers to third parties. The number of internet banking services to customers continues to grow and the internet offers enormous opportunities for banks, and other financial services to fundamentally reshape their

organizations. Banks can generate revenue through increased account, access fees and benefit from promotional opportunity to cross-sell products such as credit cards and loans as we saw, internet banking offers many benefits to banks as well as to customers. One of the main reasons for the growth of internet banking is that, if handled correctly, it can significantly lower the cost of delivering products and services. Costs of transactions in internet banking can be as low as a tenth of the cost of banking through conventional means. So, we can find two fundamental reasons underlying internet banking development and diffusion. First, banks get notable cost savings by offering internet banking services. It has been proved that internet banking channel is the cheapest delivery channel for banking products once established. Second, banks have reduced their branch networks and downsized the number of service staff, which has paved the way to self-service channels as quite many customers felt that branch banking took too much time and effort. Therefore, time and cost savings and freedom from place and staff have been found the main reasons underlying internet banking acceptance [9].

2.3 BENEFITS OF INTERNET BANKING

Banks just like other businesses are tuning to information technology to improve business efficiency, service quality and attract new customers and that the most important factor is encouraging consumers to use online banking are lower fees followed by reducing paper work and human error. Subsequently electronic channels can lead to lower transaction costs which are very. Disputes can be minimized between the employees as there is a clear flow of processes. Conducting business outside the normal branch working hours has also been a factor that has been considered convenient for bankers. Inexpensive access to the banks 24 hours a day and seven days a week. Increased availability and accessibility of more self service distribution channels help bank administration in reducing the expensive branch network and associated staff overheads. A reduction in the percentage of customers visiting the banks with an increase in alternative channels of distribution will also minimize the queues in branches. Internet banking ultimately leads to improved customer satisfaction. It is observed that electronic banking increases competition within the banking system and also from non-bank

financial institutions. Electronic banking also increases the power of the customer to make price comparisons across suppliers quickly and easily and as a consequence this pushes prices and margins downward. It is also observed that banks are responding to internet banking differently and that those which see internet banking as a complement and substitute to the traditional channels achieved better communication and interactivity with the customers. Other benefits that have accrued because of the adoption of internet banking in developed countries include the ability to attract new customers and widening the customer database, improving bank marketing and communication, and having the ability to retain high profit customers. Lack of user-friendly technology, customer demand, high initial set-up costs, redundancy of existing high-cost legacy systems, economic instability, regulatory controls and lack of suitable skills have been highlighted as some of the most important issues delaying the adoption or diffusion of electronic banking.

The critical success factors of internet banking

In setting up internet banking services commercial banks must make sure that the systems are well integrated and more convenient to the customer. Consumers do not want to navigate from website to website to access services, web services have to be convenient, easier to use, and less expensive than the alternative traditional banking to win the loyalty of customers. The interactive nature of internet banking brings more understanding of the customer. According the data gathered about customer-bank interaction can be analyzed using mining techniques and this marketing decision support capability will ultimately determine the success of the bank's electronic banking services.

2.4 LIMITATIONS OF INTERNET BANKING

In spite of the gross benefit received from internet banking, other factors have been hindering it from functioning as it should. Some of these factors include problems of security. The security and privacy aspects are major issue in case of internet banking transaction. Various sites are not properly locked, to ensure whether customer's money is safe in the cyber world or not especially in these times of cyber fraud. Also high cost of

setting up is also an issue in the implementation of internet banking. The infrastructural cost of providing internet banking facility is very high. The banks not only have to automate front-end services but also back office services, which involve high cost in terms of equipments and other computerized and communication facilities. There is also lack of awareness of the internet banking services to most customers. Another great hindrance is lack of awareness because; effective and wide media efforts in publishing internet banking need to be emphasized. Lack of computerization is also a great hindering factor. Lack of computerization and low density of telephone lines is also a bottleneck for online banking. Following types of internet banking attacks may occur to hack user's account:

- Fraudulent supplier requests from emails
- Spoofing
- Vishing (via phone)
- Investment or share sale fraud
- Lottery fraud
- Keystroke capturing/logging
- Pharming (using fake websites)

2.5 INTERNATIONAL TRENDS IN INTERNET BANKING

Though data on internet banking are scarce, and differences in definitions make cross-country comparisons difficult, a preliminary analysis by researchers from International Monetary Fund (IMF) shows that internet banking is particularly widespread in Austria, Korea, the Scandinavian countries, Singapore, Spain, and Switzerland, where more than 75 percent of all banks offer such. The Scandinavian countries have the largest number of internet users, with up to one-third of bank customers in Finland and Sweden taking advantage of internet banking. In the US, internet banking is still concentrated in the largest banks. While most US consumers have accounts with banks that offer internet services, only about 6 percent of them use these services. As of today, most banks have combined the new electronic delivery channels with traditional brick and mortar

branches, but a few that have emerged offer their products and services only through electronic distribution channels. These “virtual” or “internet only” banks do not have a branch network but might have a physical presence, for example, an administrative office or non branch facilities like ATMs. The US has about 30 virtual banks; Asia has two, launched in 2000 and 2001; and the European Union has several, either as separately licensed entities or as subsidiaries or branches of brick and mortar banks. In developing economies, however, the spread of internet banking is much limited. There are some emerging economies, which have higher internet usage than their incomes would suggest such as Korea. An important factor that affects usage is the cost of connecting to the internet, which varies widely.

2.6 CHALLENGES IN INTERNET BANKING FOR DEVELOPING COUNTRIES

Based on “best practices” in developed countries, United Nations Conference on Trade and Development (UNCTAD) report has identified four challenges that developing countries, in general, are expected to overcome to achieve the advantages that internet banking initiatives can bring about [9]:

1. The ability to adopt global technology to local requirements: An adequate level of infrastructure and human capacity building are required before developing countries can adopt the global technology for their local requirements.
2. The ability to strengthen public support for e-finance: Historically, most e-finance initiatives in developing countries have been the result of cooperative efforts between the private and public sectors.
3. The ability to create a necessary level of regulatory and institutional frameworks: The lack of regulatory frameworks, trust, security and privacy standards, high trade barriers, customer and investor protections impede progress in implementing internet banking initiatives on a larger scale in many developing countries.
4. The ability to mainstream small and medium scale enterprises towards internet banking: The availability of and access to quality data and banking information is required for and medium scale enterprises in developing countries to move

towards internet banking. Similarly, on-line credit information will enhance and medium scale enterprises' ability to secure financing.

2.7 INFORMATION SECURITY

Information security, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take.

Sometimes referred to as computer security, Information Technology security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smart phones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.

Security policies, guidelines, standards and procedures provide a mandate for maintaining internet banking security. A policy is defined as what will and will not be permitted, such as "users are required to have passwords and keep them secure". Guidelines are suggested methods of how to adhere to the policy, such as "users should change passwords on a regular basis". Standards are specific technical rules for a particular platform, such as Microsoft IIS or database servers. A standard might state "passwords must be set to expire every 90 days and must force the user to use a combination of alpha-numeric characters". Finally, procedures provide users and systems administrators with methods for maintaining security, such as "how to install a Microsoft IIS Server Securely". It is important to understand the distinction between these to ensure appropriate compliance. A configuration audit is one where the auditors verify that

servers and devices are configured according to an established standard and maintained with an appropriate procedure [1].

Standardizing Security Audit – Initiatives So Far

Institutions and professional bodies all over the world have issued various guidelines and best practices regarding Information System Security from time to time.

British Standards (BS 7799):- Provides guidelines to organizations to identify manage and minimize the range of threats to which information is regularly subjected. These include internal threats, external threats, accidents, malicious actions and industrial sabotage.

ISO/IEC 27002:- The goal of ISO/IEC 27002 is to provide information to parties responsible for implementing information security within an organization. It can be seen as a best practice for developing and maintaining security standards and management practices within an organization to improve reliability on information security in inter-organizational relationship.

Center for Internet Security (CIS) has a mission to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls. CIS benchmarks support high level standards that deal with the "Why, Who, When, and Where" aspects of IT security by detailing "How" to secure an ever widening array of workstations, servers, network devices, and software applications in terms of technology specific controls.

Generally Accepted System Security Principles (GASSP) (which is sponsored by the International Information Security Foundation (I2SF) promotes good practice and provide the authoritative point of reference and legal reference for information security principles, practices and opinions.

Control Objectives for Information and Related Technology (COBIT):- Executives need confidence that they can rely on information systems and the information produced

by those systems and get a positive return from IT investments. COBIT enables business executives to better understand how to direct and manage the enterprise's use of IT and the standard of good practice to be expected from IT providers. COBIT provides the tools to direct and oversee all IT-related activities.

Information Technology Infrastructure Library (ITIL):- IT service management is concerned with planning, sourcing, designing, implementing, operating, supporting and improving IT services that are appropriate to business needs. ITIL provides a comprehensive, consistent and coherent best practice framework for IT service management and related processes, promoting a high-quality approach for achieving business effectiveness and efficiency in IT service management.

Commonly Accepted Security Practices & Recommendations (CASPR) provides advice about how to use technologies, products, and methodologies to secure the IT environment, through papers written and vetted by a community of experts.

2.8 BANKING SECURITY

When a bank's system is connected to the internet or intranet, an attack could originate anytime, anywhere. Some essential level of security must be established before business on the internet can be reliably conducted. An attack might be in the form of unauthorized access, destruction, corruption or alteration of data or any type of malicious procedure to cause network failure, reboot or hang. Modern security techniques have made cracking very tedious but not impossible. Furthermore, if the system is not configured properly or the updated patches are not installed then hackers may crack the system using security hole. A wide array of information regarding security hole and their fixes is freely available on the web.

Banking Security Architecture

In Internet banking as with traditional banking methods, security is a primary concern. The latest methods in Internet banking system security are used to increase and monitor the integrity and security of the systems.

The security of the average internet banking application is addressed at three levels. The first concern is the security of client information as it is sent from the customer's PC, mobile phones, corporate clients etc. to the web server. The second area concerns the security of the environment in which the Internet banking server and client 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 systems.

Data security between the client browser and web server usually is handled through a security protocol called Secure Sockets Layer (SSL). SSL provides data encryption, server authentication, and message integrity for an 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.

Online banking application supports data 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 client 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.

The client information database is housed on a database server, which implements security algorithm in addition to the firewall technology. The client database is usually stored on a RAID-5 drive array, which provides uninterrupted data access, even in the event of a hard drive failure.

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.

Implementation of the SSL security protocol on the web server and client browser ensures authenticated data has been received from the client. 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 [10].

The Open Payment Framework is built entirely on a Service Oriented Architecture (SOA) delivering common, reusable services consisting of a comprehensive data model, choreographed payment business processes and configurable services including parsing, validation, cost based routing, warehousing security, auditing and many more[10].

Example of banking channel architecture is shown on figure 2.1[10]

Banking channel is a communication method between the bank and its customers in order to provide/get service and/or provide/get information. Example for banking channels could be of course branch, automatic machines, internet (PC, mobile). All channels share the same purpose which is communicating with the customer and enabling the customer to reach the bank either for information or to receive specific service, but each channel can have different set of information and/or service anyone is dealing with. In most cases there are overlaps meaning different channels provide the same information and/or

service but just do it in different manner, and in some cases specific service or information could only be provided by one specific channel.

The fact that banks has different channels born from the following reasons:

1. The bank has the interest to enable its customers and prospects to interact with him anytime anywhere so he could make more business and provide better service
2. The customers have the need to be able to use the banks services in an easy way whenever they want wherever they are
3. The technology is advancing and provides new creative, cost effective and convenient approaches to both provide/consume banking related services
4. The baking business has become very competitive which requires the banks to provide better service and find new models for attracting its customers

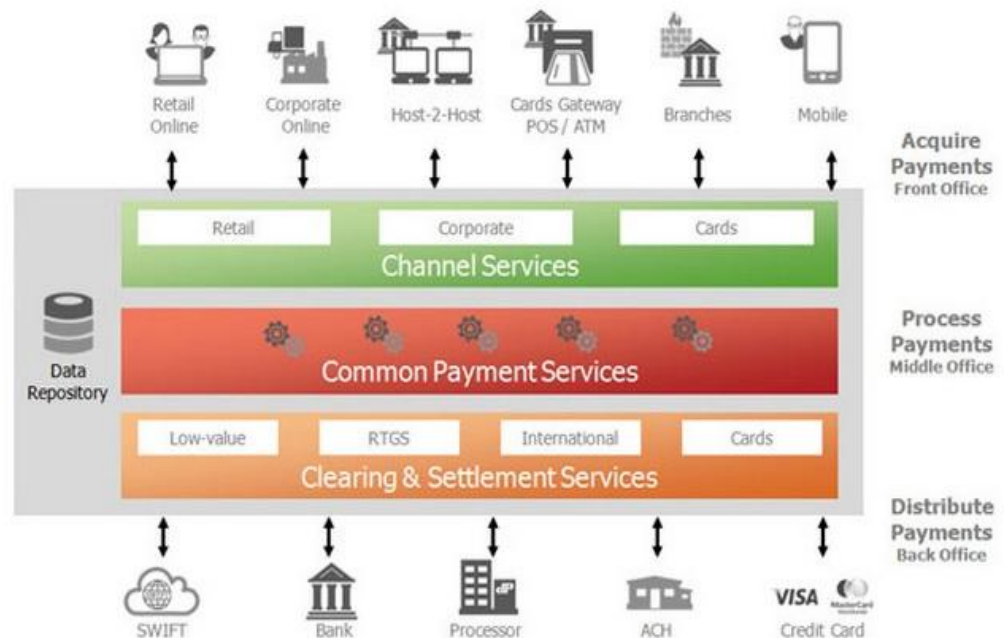


Fig 2.1: Banking channel architecture

Because of the expansion of internet banking services in the past decade, limited researches have been done in this field. From these researches the following studies can be mentioned:

A research has been carried out by some researchers which identified factors that affect bank customers that tend to use bank ATM systems [11]. Therefore based on the extracted components from research libraries, and factor analysis on collected questionnaires from Mellat bank customers (both users and non-users of ATM systems), six factors that have effect on the tendency of customers to use ATM bank systems were identified. These factors include: location desirability, customer awareness, system integration, variety of services, ease of use/access and reliability. The results showed location desirability for users of ATM systems and reliability for non-users are the most important factors.

Table 2.1: The proposed layered multi-factor user authentication system

Multi-factor authentication levels:	
Level 1	<p>knowledge based factors:</p> <p>Level 1 uses registered knowledge based factors such as credit card information, bank account information, i-PIN, OTP, etc</p>
Level 2	<p>possession-based factors (software based):</p> <p>Level 2 uses an accredited certificate issued by a CA after a CA identifies the user with a reliable certificate issued by the government such as an NID card, driver's license, passport, etc</p>
Level 3	<p>possession-based factors (device based):</p> <p>Level 3 uses an accredited certificate with another security measure such as security card, mobile phone (some form of storage media), security token, etc.</p>
Layered multi-factor authentication levels (using control information):	
Level 4	<p>a combination of knowledge based factors and possession-based factors</p> <p>Level 4 uses an accredited certificate with other hardware devices such as an OTP, security token, 2- channel authentication, etc.</p> <p>a combination of knowledge based factors and biometric-based factors</p>
Level 5	<p>Level 5 uses an accredited certificate with biometric information such as a fingerprint, etc.</p>

A research has been done to identify a multi-layer of multi factors authentication model for online banking services as shown on table 2.1 [12]. In this work researchers analyze user authentication methods being used in various online environments, such as internet banking, online transactions and financial services, to identify the characteristics and issues of such authentication methods in order to present a user authentication level system model suitable for different online services.

Researchers integrated multi factor authentication with multi layer authentication techniques in order to produce a standard layered multi factor authentication model suitable for different internet banking services based on risk assessment criteria. The produced model consist of 5 level in which each level contain a one or combination of authentication factors such as knowledge based, possession-based or biometric-based factors. The model then enhanced by adding control information factors, specifically for levels (4, 5), in order to support layering needs.

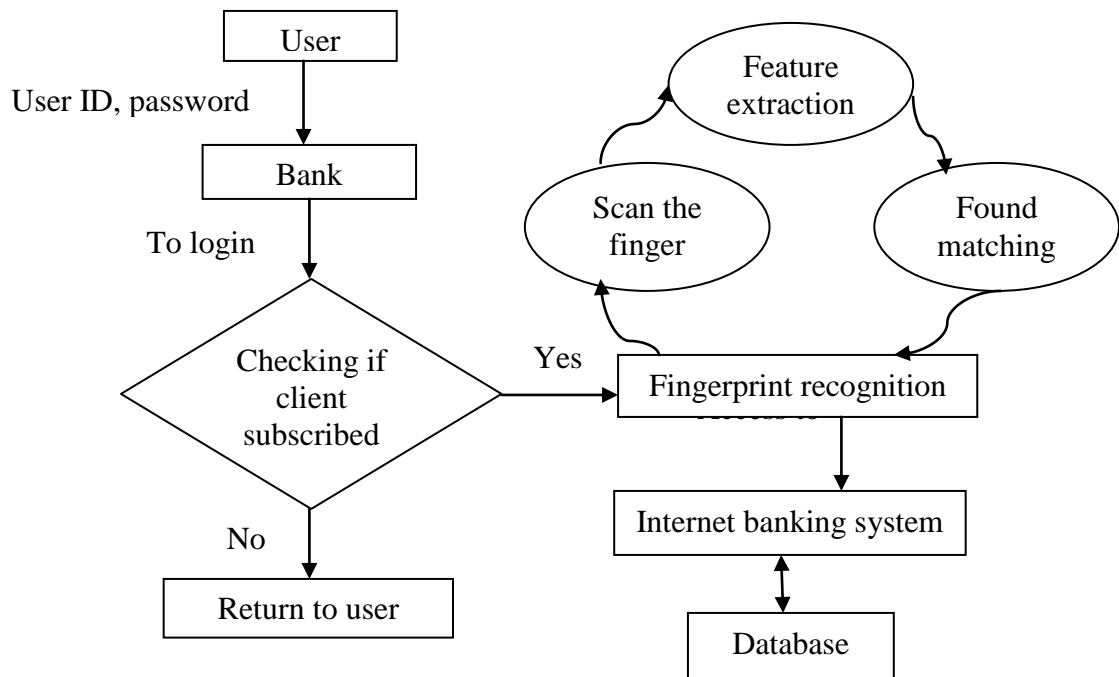


Fig. 2.2: Model for internet banking system with fingerprint recognition

An article “Novel algorithm for secure internet banking with finger print recognition” proposes a model that uses biometric parameter finger print recognition [13]. Since web banking or internet banking is used to describe banking transactions through internet application, But there are many security problems like fraudulent websites, fake emails from banks, capturing user IDs and passwords, hacking personal bank accounts and steal money etc. To overcome these problems, this research paper gives a solution through novel algorithm with finger print recognition.

A research paper “Information security and auditing for distributed network” describes management framework also for the non uniform distributed network [1]. An approach for information security in a Client/Server based distributed network is described in this paper. With this work researchers address several factors concerning security and auditing of information in distributed network environments.

Researchers, experts have been giving full attention to subjects about online banking security, the research include framework for the governance of information security in banking system and the security issues internet banking are facing today and solutions for online banking security threats [7]. Experts have summed up security issues in two categories: system security issues and information security issues and the corresponding solutions are cryptography, identity authentication and the data transmission protection technology. Researchers also described current authentication threats and proposed solutions and new authentication protocol for online banking and introduced new approaches for online banking security. Laura Falk et. al found that 76% of the sites in their survey suffered from at least one design flaw that are not widely understood, even by experts who are responsible for web security and methodology for testing websites is presented and discussed. Researchers also defined attack and protection trees and discussed how they can be implemented in the security analysis of an online banking system to maintain user’s trust and confidence in the security of their online bank accounts. Many researchers have done studies of several banks in their countries to compare their systems.

In the research article "Comparative study of online banking security system of various banks of India", different bank's internet banking security parameters are compared. To provide customers with secure, reliable, robust online environment to do online banking the banks should adopt "best of breed" technologies to authenticate customers identities when they logon, to ensure that their data is transmitted securely and reliably. This paper tried to explore several of technology and security standards the authoring body is recommending to banks for safe internet banking and comparison of different banks based on the recommendations given by authoring body for secure online banking. Also, different bank's internet banking system by considering different parameters based on whether they are implemented or not is compared. But it is not recommend that which one is the best or secured among these different deployments. Since there are many security measures among which comparison is done, it is harder to decide which one is best. To make it easier a multi-criteria decision making (MCDM) optimization technique is implemented in this work.

An article Improving E-Banking Security with Biometrics: Modeling user attitudes and acceptance is published by researchers and use of biometric factor is suggested for user authentication [14]. Despite the widespread success of online banking, there remains a reluctance to use it primarily because of uncertainty and security concerns. Researchers evaluate the potential of biometric authentication for online banking as a way of improving adoption and use of online banking. Using structural equation modeling techniques, study revealed that user perceptions of biometrics security positively influenced their attitude and intention to use biometric banking. It also found that self efficacy in biometric use, positively influenced user's perception of the security of biometrics.

A study is done on title "Cryptanalysis of Remote User Authentication Scheme with Key Agreement" [15]. They suggested that password authentication with smart card is one of the most convenient and effective two-factor authentication mechanisms for remote systems to assure one communicating party of the legitimacy of the corresponding party by acquisition of corroborative evidence. This technique has been widely deployed for various kinds of authentication applications, such as remote host login, online banking, e-

commerce and e-health. A dynamic-identity-based user authentication scheme with session key agreement is presented by researchers. In this research, it is shown that once the smart card of an arbitrary user is lost, messages of all registered users are at risk. Using information from an arbitrary smart card, an adversary can impersonate any user of the system.

User authentication protocol entitled “Web Based Security with LOPass User Authentication Protocol in Mobile Application” is proposed [16]. It is proposed that the user authentication protocol named LOPass which creates long term password and one time password for authenticating the user. It has three phases as registration, login and recovery phase. In LOPass, random password is generated for each login. Registration is used for the registration of the user. Recovery phase is used, if the user’s mobile phone gets lost. The user needs to remember only his long term password which is secret.

In the recent day's web applications usage is increasing by banking, financial institutes and health or hospital management systems such as online or net banking and mobile banking, e-commerce applications, news feeds, inpatient and outpatient information etc. All these online applications require support for security properties like authentication, authorization, data confidentiality, and sensitive information leakage. The most widely accepted common method of authentication for an online application is to use a combination of alphanumeric with special characters usernames and passwords [17].

Now days, the internet has become most convenient and widely used media for people exchanging information and doing business over the internet such as accessing web based emails, online auctions or banking sites. But nowadays, accessing the internet is faced with many challenges. One of the most important challenges is to ensure security with vital role to provide security in websites. The text passwords are convenient and simplest form for a user authentication on websites and this level is more prone to security attacks. User mostly uses these weak passwords and it is often used across several websites. The reuse of the same password in untrusted websites causes password threats. Hackers invoke password stealing methods to grab password such as phishing, malware and key loggers. By grabbing password such way, hackers may login any user’s account from any

place. Hence based on these literature papers and experience gained during collection of data for using MCDM a little change in user authentication architecture is proposed. It is required that, if any user is logged in from certain location or IP and the same user account is attempting to login from other IP or location, it should be blocked and the user must be informed about this because the same user can not login single account from different location at a time.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 OVERVIEW OF MULTI-CRITERIA DECISION MAKING

Multiple-criteria decision-making (MCDM) or multiple-criteria decision analysis (MCDA) is a sub-discipline of operations research that explicitly considers multiple criteria in decision-making environments. Either in our daily lives or in professional settings, there are typically multiple (conflicting) criteria that need to be evaluated in making decisions. Some measure of quality is typically another criterion that is in conflict with the other.

MCDM is concerned with structuring and solving decision and planning problems involving multiple criteria. The purpose is to support decision-makers facing such problems. Typically, there does not an exact unique optimal solution for such problems and it is necessary to use decision-makers preferences to differentiate between solutions. In an MCDM problem, a number of alternatives are evaluated with respect to a number of criteria in order to select the best alternative(s).

In some real-world decision making processes, due to reasons like time pressure, lack of knowledge or data, or limited expertise related with problem domain, the decision maker sometimes might only provide the information with linguistic preferences. In some cases, it does occur that the weights of all criteria are uncertain and provided by the decision maker with linguistic preference information. Further, when ranking all the alternatives according to each criterion, the decision maker would also provide information with linguistic preferences. To deal with those situations, an effective decision making method must be found.

According to MCDM different worst to best criteria are identified first by the decision-maker. Comparisons are then conducted between each of these criteria. A maxmin problem is then formulated and solved to determine the weights of different criteria. The weights of the alternatives with respect to different criteria are obtained using the same

process. The final scores of the alternatives are derived by aggregating the weights from different sets of criteria and alternatives, based on which the best alternative is selected.

MCDM problems are generally divided into two classes with respect to the solution space of the problem: continuous and discrete. To handle continuous problems, multi objective decision-making (MODM) methods are used. Discrete problems, on the other hand, are solved using multi-attribute decision-making (MADM) methods.

The majority of real world decision making problems involve multiple decision makers, and the problem arises when aggregating the preferences of a group of decision makers to constitute a joint decision model. Multi-criteria analysis offers the way to aggregate the data on individual criteria in order to reach a consensus. In MCDM process, the selection is facilitated by evaluating each choice on the set of criteria, then, the decision alternatives and criteria are collected in a table (decision matrix). The utilization of MCDM methods is able to foster group learning ability and it is particularly valuable in handling structured decision making problem.

There are three main steps involved in selection of best alternatives: (1) determine the relevant criteria and alternatives, (2) evaluate the relative impacts of alternatives on those criteria, and (3) determine a ranking of each alternative [18].

A “discrete MCDM” problem (for the sake of simplicity and in line with common practice, MCDM) is generally shown as a matrix, as follows:

$$A = \begin{matrix} & \begin{matrix} c_1 & \dots & c_n \end{matrix} \\ \begin{matrix} a_1 \\ \vdots \\ a_m \end{matrix} & \begin{bmatrix} p_{11} & \dots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{m1} & \dots & p_{mn} \end{bmatrix} \end{matrix} \quad \text{..... (i)}$$

Where $\{a_1, \dots, a_m\}$ is a set of feasible alternatives and $\{c_1, \dots, c_n\}$ is a set of decision-making criteria, and p_{ij} is the score of alternative i with respect to criterion j . The goal is to select the best (e.g. most desirable, most important) alternative, in other words an alternative with the best overall value.

3.2 IDENTIFY CRITERIA AND MEASURES

The first thing to do is to identify the criteria of an internet banking that were important to users from information security perspective. Alternatives represent the different choices of action available to the decision maker. Usually, the set of alternatives is assumed to be finite, ranging from several to hundreds. They are supposed to be screened, prioritized and eventually ranked. Each MCDM problem is associated with multiple attributes. Attributes are also referred to as "goals" or "decision criteria". Attributes represent the different dimensions from which the alternatives can be viewed. Since different attributes represent different dimensions of the alternatives, they may conflict with each other.

The following nine internet banking parameters are taken from the perspective of information security for different internet banking applications of different banks.

- Cryptographic algorithm
- Number of encryption bits
- SSL version
- Onscreen keyboard
- SMS challenge
- Authentication level
- Second channel notification
- Double password control for transaction
- Validity of password

Cryptographic Algorithm

Cryptographic algorithms are sequences of processes, or rules, used to encipher and decipher messages in a cryptographic system. In simple terms, they're processes that protect data by making sure that unwanted people can't access it. These algorithms have a wide variety of uses, including ensuring secure and authenticated financial transactions.

Most cryptography algorithms involve the use of encryption, which allows two parties to communicate while preventing unauthorized third parties from understanding those communications. Encryption transforms human readable plaintext into something unreadable, also known as cipher text. The encrypted data is then decrypted to restore it, making it understandable to the intended party. Both encryption and decryption operate based on algorithms.

There are many different types of cryptographic algorithms, though most of them fit into one of two classifications - symmetric and asymmetric. Some systems, however, use a hybrid of both classifications. Symmetric algorithms, also known as symmetric-key or shared-key algorithms, work by the use of a key known only to the two authorized parties. While these can be implemented in the form of block ciphers or stream ciphers, the same key is used for both encrypting and decrypting the message. The Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are the most popular examples of symmetric cryptography algorithms.

Asymmetric cryptography algorithms rely on a pair of keys - a public key and a private key. The public key can be revealed, but, to protect the data, the private key must be concealed. Additionally, encryption and decryption of the data must be done by the associated private and public keys. For example, data encrypted by the private key must be decrypted by the public key, and vice versa. RSA is one of the most common examples of this algorithm.

During the collection of data of different bank it is found that AES and 3DES algorithms are implemented. On the basis of the research paper "New Comparative Study Between DES, 3DES and AES within Nine Factors" and "Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based on Various File Features", weight "0" is given to the 3DES encryption algorithm and weight "0.4" is given to the encryption technique AES considering the factors key length, cryptanalysis resistance against attack, time required to check all possible keys and mainly their data encryption rate. Corresponding values of these factors are on table 3.1 and table 3.2

Table 3.1: Execution rate for sparse and dense data file [19]

Algorithm name	Dense AIFF file	Sparse AIFF file
	Encryption rate(MB/s)	Encryption rate(MB/s)
AES	108.62	108.64
DES	38.14	38.14
3-DES	13.42	13.53

Table 3.2: Comparison between AES and 3DES [20]

Factor	AES	3DES
Key length	128, 192, or 256bits	(k1, k2 and k3) 168 bits
Cipher type	Symmetric block cipher	Symmetric block cipher
Block size	128, 192, or 256 bits	64 bit
Developed	2000	1978
Cryptanalysis resistance	Strong against differential, truncated differential, linear, interpolation and square attacks	Vulnerable to differential, brute force attacker could be analyze plain test using differential cryptanalysis.
Security	Considered secure	One only weak which is exit in DES
Possible keys	2^{128} , 2^{192} , or 2^{256}	2^{112} or 2^{168}
Possible ASCII printable character keys	95^{16} , 95^{24} , or 95^{32}	95^{14} or 95^{21}
Time required to check all possible keys at 50 billion keys per second	For a 128-bit key: $5 \cdot 10^{21}$ years	For 112-bit key: 800 days

Number of Encryption Bits

In cryptography, key size or key length is the size measured in bits of the key used in a cryptographic algorithm (such as a cipher). An algorithm's key length is distinct from its

original cryptographic security, which is a logarithmic measure of the fastest known computational attack on the algorithm, also measured in bits. Keys are used to control the operation of a cipher so that only the correct key can convert encrypted text (cipher text) to plaintext. Bigger is the number of encryption bits greater will be the security of the cipher text since smaller encryption keys are easier to break and more vulnerable to different type of attacks like brute force attack, differential attack etc.

According to the SSL server rating guide [21][21], the different number of encryption bits is scored as shown in table 3.3.

Table 3.3: Cipher strength rating guide [21]

Cipher strength	Score
0 bits (no encryption)	0%
<128 bits	20%
<256 bits	80%
>=256 bits	100%

SSL Version

The first public version of SSL, version 2, suffered from a number of security flaws, which have been fixed in SSLv3. As browsers nowadays still support SSLv2, and as it is still in use in some systems. The same cryptographic keys are used for message authentication and for encryption; this means that in export mode the security of the message authentication codes (MAC) is unnecessarily weakened. SSLv2 has a weak MAC construction and relies solely on the MD5 hash function. SSLv2 does not have any protection for the handshake; hence a person-in-the-middle attack cannot be detected. Finally, a truncation attack is possible, as SSLv2 simply uses the TCP connection close to indicate the end of data, so that the attacker can simply forge the TCP FINs and the recipient cannot tell that it is not a legitimate end of data.

The IETF TLS working group adopted the SSLv3 protocol. Some minor modifications were made to increase the security: the way cryptographic keys are expanded from the

initially exchanged secret was improved, the Hash-based message authentication code (HMAC)-like MAC construction was replaced by the real HMAC and, implementations were required to include support for the Diffie-Hellman key agreement, the Digital Signature Standard, and 3DES encryption [22].

According to the SSL server rating guide [21], the different SSL versions are scored according to their vulnerabilities as shown on table 3.4.

Table 3.4: Protocol support rating guide [21]

Protocol	Score
SSL 2.0	0%
SSL 3.0	80%
TLS 1.0	90%
TLS 1.1	95%
TLS 1.2	100%

Onscreen Keyboard

One of the most common ways the hacker hack your password is by using a Trojan. Many of them inbuilt key loggers. Whenever you type anything on your keyboard, it goes to them. To enhance the security while logging into secure websites is by using virtual keyboard.

Online Virtual Keyboard is the best Security implementation to make sensitive data safe from “spyware” and “Trojan program”. To use online virtual keyboard is the best practice in websites where is to protect sensitive data from hackers, crackers and malicious programs. Most of banks who offer online banking facility, offers virtual keyboard to type in your password to login.

Based on whether virtual keyboard is used or not weight is given in this parameter. The system that uses virtual keyboard is given weight "1" and that does not uses is given "0".

SMS Challenge

A username and password are no longer enough to authenticate your users. Each day brings new stories of stolen identities and brands of all sizes falling victim to hackers. This method has been applied in some banking systems to notify users about transactions requiring their authorization. It provides a second authentication channel for transactions that fit certain characteristics by sending to the user a set of characters which have to be entered on the system in order to authorize and process the transaction through the online banking system.

Based on whether SMS challenge is used or not weight is given in this parameter. The system that uses SMS challenge is given weight "1" and that does not uses is given "0".

Authentication Level

The security of information may be one of the principal concerns to the Internet users. Only organizations such as banks with dedicated Internet connections face the risk of someone from the internet gaining unauthorized access to their computer or network. However, the internet banking system users still face the security risks with unauthorized access into their banking accounts.

Recently most banks offer online banking to their customers. Internet banking services needs strong security standards rather than other internet activities because of the sensitivity of information by nature. To increase security, most banks use two-factor authentication, which involves two basic factors:

- i. Something the user knows (e.g., password, PIN, pass phrase)
- ii. Something the user has (e.g., smart card, other hardware token)

The term authentication describes the process of verifying the identity of a person or entity. It is the process of determining whether someone or something is, in fact, who or what it is declared to be. Authentication is part of most online applications. There are various authentication methodologies which differ in term of complexity. Techniques

used and deployment requirements affects the level of security provided. User name and password is the most common form of authentication used. Unluckily it is also one of the most insecure methods.

Authentication methods can involve up to three factors:

- i. Knowledge: something the user knows (e.g. a PIN or a Password),
- ii. Possession: something the user has (e.g. a Smart Card or a USB Token),
- iii. Attribute: something the user is (e.g. biometric characteristics like a fingerprint or the pattern of the eye)

According to these three factors, authentication schemes can be divided in single factor and multi factor authentication:

- i. Single factor authentication relies on one factor only. Basic user name/password authentication for example is based on something you know and
- ii. Multi factor authentication is based on two or more factors. This can be accomplished through software (e.g. a software certificate), hardware (e.g. Smart Card or USB token) or any out-of-band approaches of one time passwords (e.g. via SMS or E-Mail).

Multi-layered authentication in the online banking context refers to the requirement of multiple login names, passwords, or other authenticating device or knowledge to gain access to increasingly sensitive information or higher-risk transactions. This approach may be used by posing additional security questions or asking for additional passwords as higher risk transactions are requested [11]. The entire bank has implemented another authentication layer for transaction on account.

Most bank use two-factor authentication, which involves two basic factors: Something the user knows (e.g., password, PIN, pass phrase) and something the user has (e.g., smart card, other hardware token). Based on whether multiple factors are used or single factor is used weight is given in this parameter. The system having multiple factor is given weight "1" and that having single is given "0".

Second Channel Notification

Second channel notification is a facility used by banks to send message or email (also called alerts) to customers to notify the transactions on their account. Banks are required to notify customers immediately through alternative automated channels (e.g. SMS messages email etc.) after customers conduct high-risk transactions. Based on whether second channel notification are used or not weight is given in this parameter. The system having second channel notification is given weight "1" and that having no second channel notification is given "0".

Double Password Control for Transaction

Username and password are mostly used user authentication factor. Generally in banking system there are two types of password used. The first one is password associated with username which is used to login user account and view user account information but banking transaction are not allowed. Another password is used to perform banking transactions and payments. This password is of two types, The One Time Password (OTP) is required to do transactions. Every transaction must be done through OTP option and is different every time. OTPs avoid a number of shortcomings that are associated with static password-based authentication. This password is delivered to user via SMS or email or any special hardware device given to customer by bank. If not used, this type of password expires after certain time. One-time password requires access to something a person has (such as a small key ring fob device with the OTP calculator built into it, or a smartcard or specific cell phone) as well as something a person knows (such as a PIN).

Another is transaction password, which is used for utility payments and other banking transactions. Same password is used for every transaction. It may have certain time validity or not.

Based on whether double password is implemented or not weight is given in this parameter. The system that uses completely double password control is given weight "1". Some internet banking applications are designed as utility payments (such as purchasing of recharge cards, electricity bill payment, phone bill payment etc.) are possible without

transaction passwords but account to account transfer and interbank transactions require transaction password, such type of implementation is assumed as partial implementation of double password control and such system is given weight “0.5”. If double password control is not implemented then the assigned weight will be “0”.

Validity of Password

A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training.

Some policies require users to change passwords periodically, often every 90 or 180 days. Systems that implement such policies sometimes prevent users from picking a password too close to a previous selection. This policy can often backfire. Some users find it hard to devise "good" passwords that are also easy to remember, so if people are required to choose many passwords because they have to change them often, they end up using much weaker passwords; the policy also encourages users to write passwords down. Also, if the policy prevents a user from repeating a recent password, this requires that there is a database in existence of everyone's recent passwords instead of having the old ones erased from memory.

Based on validity of password used weight is given in this parameter. If there is no limit on password validity, that is, if forceful password change is not implemented then weight “0” is given. If password validity is nine months weight is 0.25, for six month weight is 0.5, for three months weight 0.75 is given.

Classification of the measures based on their type (continuous or categorical) is shown on table 3.5.

Table 3.5: Type of measures

Measure	Type: Continuous/ Categorical
Cryptographic algorithm	Continuous
Number of encryption bits	Continuous
SSL version	Continuous
Onscreen keyboard	Categorical
SMS challenge	Categorical
Authentication level	Continuous
Second channel notification	Categorical
Double password control for transaction	Continuous
Validity of password	Continuous

3.3 DATA COLLECTION

For each measure data is collected for seven internet banking systems which are listed in table 3.6 shown below categorized as Bank A, Bank B, Bank C, Bank D, Bank E, Bank F and Bank G.

Table 3.6: Collected data for three different banks

Bank	Cryptographic algorithms	Number of encryption bits(Key size)	SSL version	Onscreen keyboard	SMS challenge	Authentication factor	2 nd channel notification	Double password control for transaction	Validity of password
A	AES	256	TLS1.0	yes	no	single	no	partially yes	no limit
B	3DES	168	TLS1.0	no	no	single	no	yes	3 months
C	AES	256	TLS1.2	yes	no	single	yes	yes	6 months
D	AES	256	TLS1.0	no	yes	double	no	yes	no limit
E	AES	128	TLS1.2	yes	yes	double	no	yes	no limit
F	AES	128	TLS1.2	yes	yes	double	no	yes	3 months
G	AES	256	TLS1.0	yes	no	single	no	partially yes	6 months

3.4 SCALING EACH MEASURE AND CALCULATING WEIGHT

Based on the above discussion each parameter of each bank is given weight as shown on the table 3.7.

Table 3.7: Weight of different parameters

Bank	Cryptographic algorithms	Number of encryption bits	SSL version	Onscreen keyboard	SMS challenge	Authentication factor	Second channel notification	Double password control for transaction	Validity of password
A	0.4	1	0.9	1	0	0.5	0	0.5	0
B	0	0.8	0.9	0	0	0.5	0	1	0.75
C	0.4	1	1	1	0	0.5	1	1	0.5
D	0.4	1	0.9	0	1	1	0	1	0
E	0.4	0.8	1	1	1	1	0	1	0
F	0.4	0.8	1	1	1	1	0	1	0.75
G	0.4	1	0.9	1	0	0.5	0	0.5	0.5

3.5 USER AUTHENTICATION

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. The process of an administrator granting rights and the process of checking user account permissions for access to resources are both referred to as authorization. The privileges and preferences granted for the authorized account depend on the user's permissions, which are either stored locally or on the authentication server. The settings defined for all these environment variables are set by an administrator.

Authentication is the first step in access control, and there are three common factors used for authentication: something you know, something you have, and something you are. Authentication is required to keep unauthorized persons from gaining access to resources and to ensure that authorized persons can access the resources they need.

Most of the internet banking systems still use single factor authentication therefore to make this system more secure and to add another factor is important task. Since multifactor authentication is expensive, the initial outlays for tokens, password generators, biometrics and even authentication servers are high cost, while ongoing support costs often outstrip the already high help-desk costs for retrieving and resetting passwords.

User names and passwords in single factor authentication are convenient. But users forget them, people have far too many and get them confused, user names and passwords encourage poor security practices, like writing them down or keeping an easily hacked word file titled “passwords.” Yet, they are simple and easy to use if single factor authentication mechanism is strong and strong password is used. If we have a strong password that we’ll remember, we can use it across applications, with a number of service providers and on different channels. We shouldn’t, but let’s face it: most of us do. And that’s why authentication should be on top of the list of our security concerns, not at the bottom.

In current user authentication system, normally a user is authenticated by its username and password as shown in fig. 3.1. If user enters username and password on bank’s website, it checks for registered clients and if matches found user will be authenticated and access to internet banking system is given. But if the same username and password is used by another person from other location or from other device at same time, internet banking account can be accessible as shown in fig. 3.2 that is first user session terminates and a new session establishes for a person who logged in later. For doing banking transaction another transaction password is required. Logically same person cannot login same account from different location simultaneously hence the deployed user authentication system cannot be perfect.

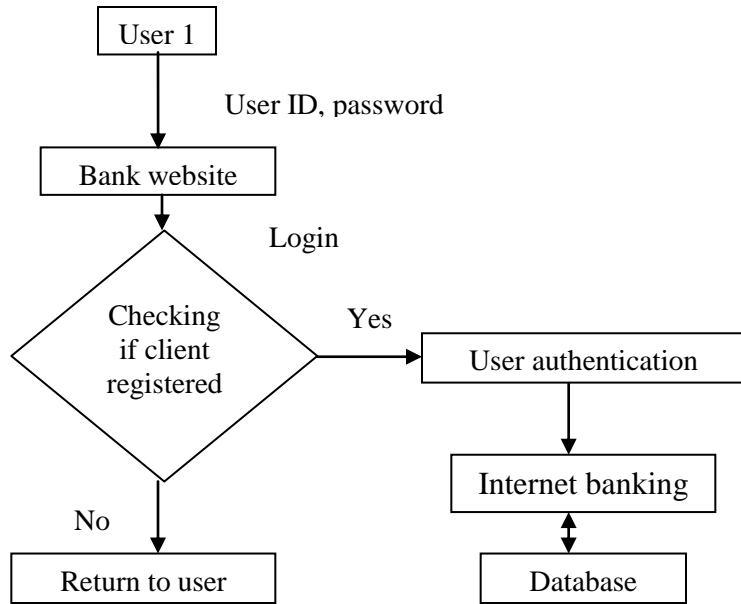


Fig. 3.1: Existing internet banking authentication system

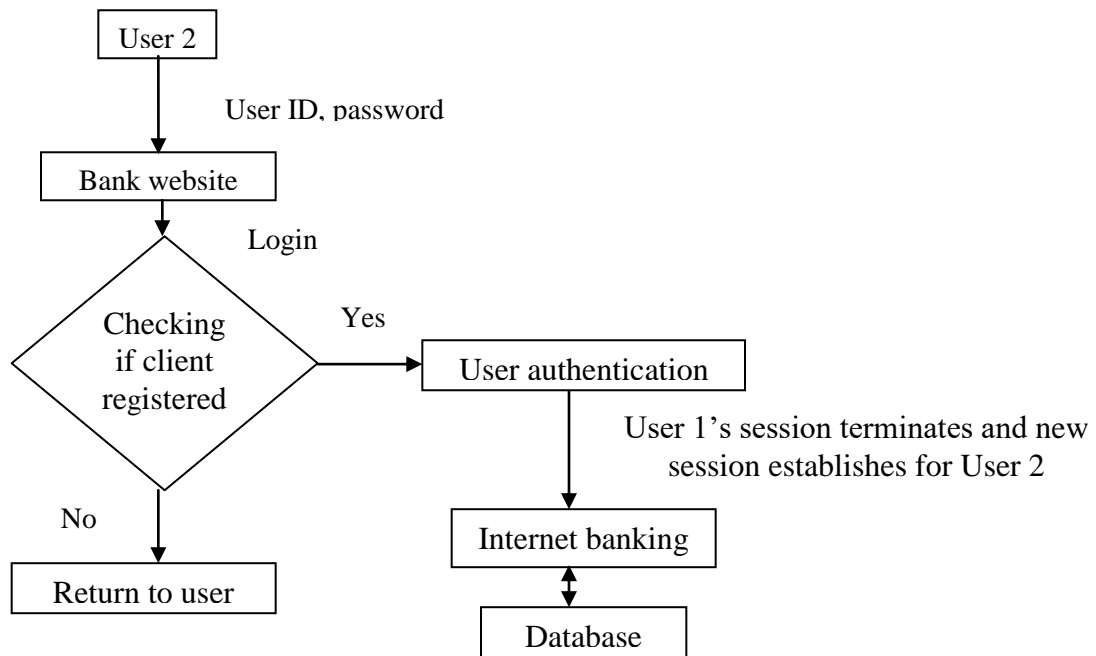


Fig. 3.2: Existing authentication system if another user tries with same username and password from other location/device at same time

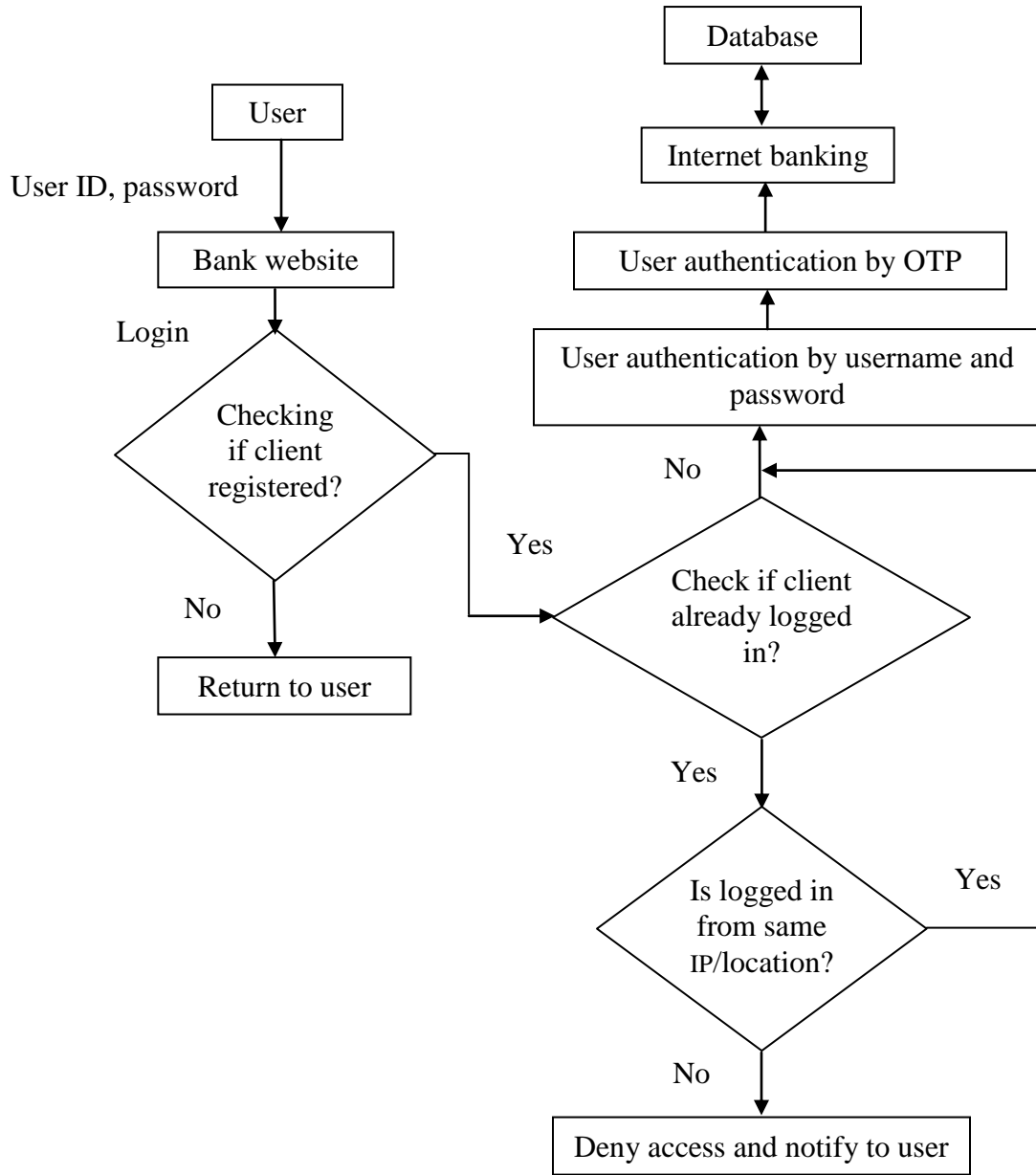


Fig. 3.3: Proposed internet banking authentication model

Since nearly all of the banks use username and password for user authentication, so hackers may stole those credentials using different frauding techniques such a phishing attacks, use of key loggers/malwares, call spoofing/vishing etc. and get access to user's account. Hence to prevent such actions to an extent a new approach for user authentication is proposed which adds a layer of security to an existing system which is described in fig. 3.3, and this model also adds an authentication factor one time password

(OTP). In proposed model when user enters username and password, it checks for registered user. If user is registered it checks whether it is already logged in or not? If not, user is authenticated by username and password and then authenticated by one time password sent to user via email and then access to internet banking system will be given. If user is already logged in, then it checks for its IP/location. If same IP/location is found, access to internet banking is given, but in case of different IP/location, access is denied and genuine user will be notified for such activities on user's account.

3.6 USABILITY AND COST

Usability is testing the software from a user's point of view. Essentially it means testing software to prove and ensure that it is "user-friendly", as distinct from testing the functionality of the software. In practical terms it includes ergonomic considerations, screen design, standardization, user centric etc.

The bank should consider following major usability characteristics from user's point of view during development of internet banking system:

- Ease of learning
- Ease of use
- Ease of remembering
- Subjective satisfaction
- Efficiency of use

Following are the benefits to the banks on testing usability of the system:

- Reducing customer support
- Customer retention & increased customer satisfaction
- Shorten development life cycle
- Removal of unnecessary features

The subscription of internet banking on different bank ranges from free service to five hundred rupees per year. From bank's point of view designing cost of internet banking web application costs from around five lakh to fifteen lakh if they outsourced the service to other companies, cost depends on the features implemented on system. These outsourcing companies charge them on two ways. One is, they charge certain percentage of initial cost annually for maintenance of system. Other is they charge certain percentage of user subscription fee and hence total charge depends on number of total users of internet banking of bank.

CHAPTER 4: RESULT AND DISCUSSIONS

4.1 DATA INTERPRETATION AND RESULT

The data is collected for each parameter and shown in table 3.7. To compare the above banks, their total score and weighted score is calculated and shown on the table 4.1.

Table 4.1: Weighted score of different bank

Bank	Cryptographic algorithms	Number of encryption bits	SSL version	Onscreen keyboard	SMS challenge	Authentication factor	Second channel notification	Double password control for transaction	Validity of password	Total score	Average score
A	0.4	1	0.9	1	0	0.5	0	0.5	0	4.3	0.477
B	0	0.8	0.9	0	0	0.5	0	1	0.75	3.95	0.438
C	0.4	1	1	1	0	0.5	1	1	0.5	6.4	0.711
D	0.4	1	0.9	0	1	1	0	1	0	5.3	0.588
E	0.4	0.8	1	1	1	1	0	1	0	6.2	0.688
F	0.4	0.8	1	1	1	1	0	1	0.75	6.95	0.77
G	0.4	1	0.9	1	0	0.5	0	0.5	0.5	4.8	0.533

Weighted average given in the table captures how important the various measures are. On the basis of this weighted average approach, we can select the best choice among multiple choices. The bank having higher weighted score is more secure than the bank having lesser weighted score. In the table 4.1 bank F has highest weighted score and bank B has lowest weighted average. So the bank F is considered as most secure and bank B is considered as least secure. This ranking may change on changing their parameter values. Even on changing single parameter value of bank its ranking may alter.

4.2 SENSITIVITY ANALYSIS

The solution to a decision problem, the global ranking of alternatives, may not provide enough information to the decision maker to make a final decision. There are several reasons why a Sensitivity Analysis (SA) should be conducted on the results. For instance, the judgments for some criteria may be subjective or there may be uncertainty in the data that leads to the preference value. In addition, the preference judgments may come from a group decision where there are different opinions. A sensitivity analysis provides more insight about the problem and in this way the decision maker should be able to make a more informed decision [23]. The sensitivity analysis may also be used to determine how robust a decision is.

Methods to perform sensitivity analysis problems may be grouped into three main categories: numerical incremental analysis, probabilistic simulations and mathematical models.

Numerical Incremental Analysis

Numerical incremental analysis involves changing the weight values and calculating the new solution. The method, also known as One-at-a-time (OAT), works by incrementally changing one parameter at a time, calculating the new solution and graphically presenting how the global ranking of alternatives changes. This is the most commonly used method.

The fig. 4.1 shows the numerical incremental sensitivity analysis of bank A and B by increasing first, cryptographic algorithm(CA), parameter of bank B and by decreasing second, number of encryption bits(EB) of bank A.

The graph shows that initially bank A has higher average weight than bank B and hence the bank A is considered as more secure. After incrementing the parameter value of bank B and decrementing the parameter value of bank A, their average weight has been changed and it became reversed i.e. the weighted average of bank B is greater than weighted average of bank A and hence bank B is considered as more secure. When cryptographic algorithm parameter value of bank B is one and encryption bit parameter

value of bank A is zero, their ranking is reverted. If initially both parameters have same value, that is 0, and increases simultaneously then there will be no change on their ranking. Hence it can be concluded that weighted average and ranking depends equally on every parameter. On changing even a single parameter may change whole ranking of alternative banks. When number of parameters or criteria increases their effect on average weight decreases and if number of parameters is few, their effect on average weight is more and altering their effect causes greater effect on average weight.

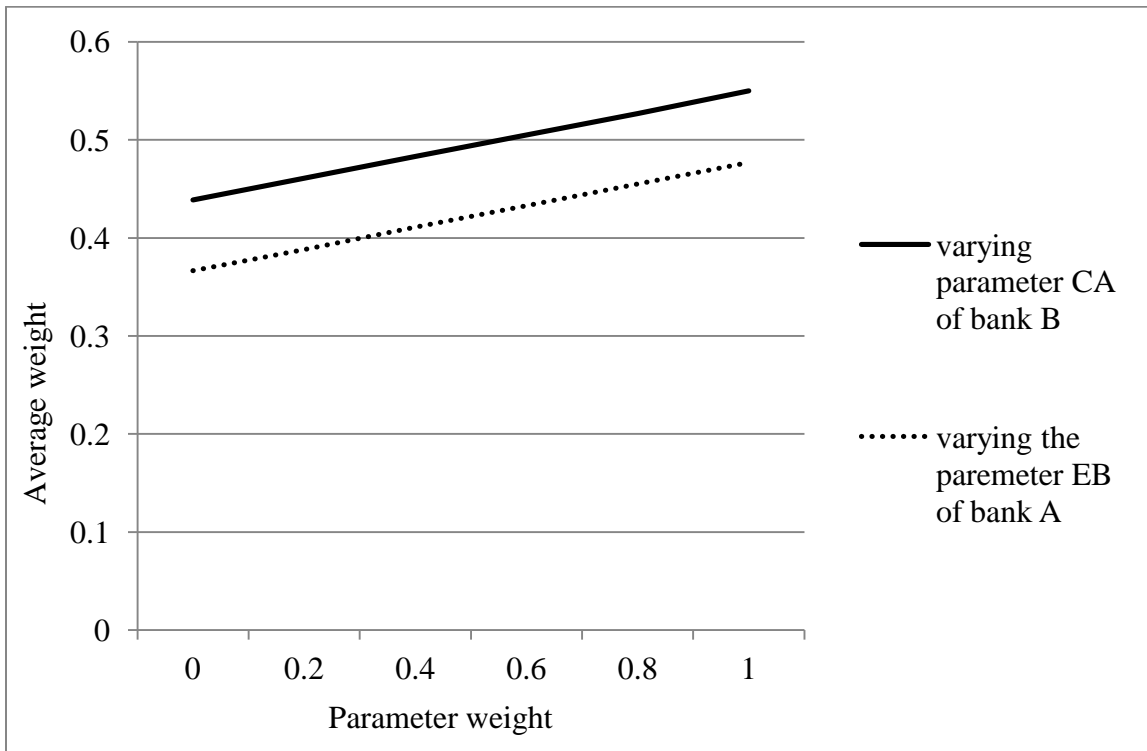


Fig. 4.1: Numerical incremental sensitivity analysis comparing bank A & B

The fig. 4.2 shows the numerical incremental sensitivity analysis of bank B and C by increasing first, cryptographic algorithm(CA), parameter of bank B and by decreasing second, number of encryption bits(EB), of bank C. Graph shows that their average weight changes on changing parameter weight but their ranking is same. Even when the parameter value of bank B is one and parameter value of bank C is zero, their ranking is same. If multiple parameters of bank B and C are changed then their ranking may alter.

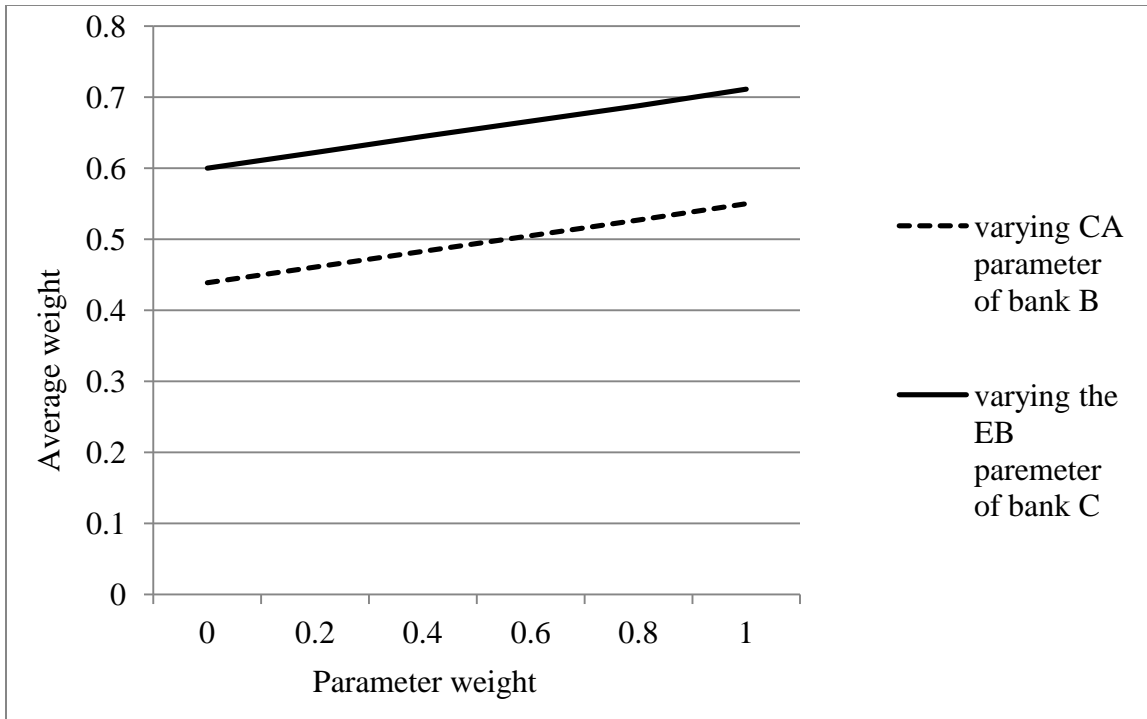


Fig. 4.2: Numerical incremental sensitivity analysis comparing bank B & C

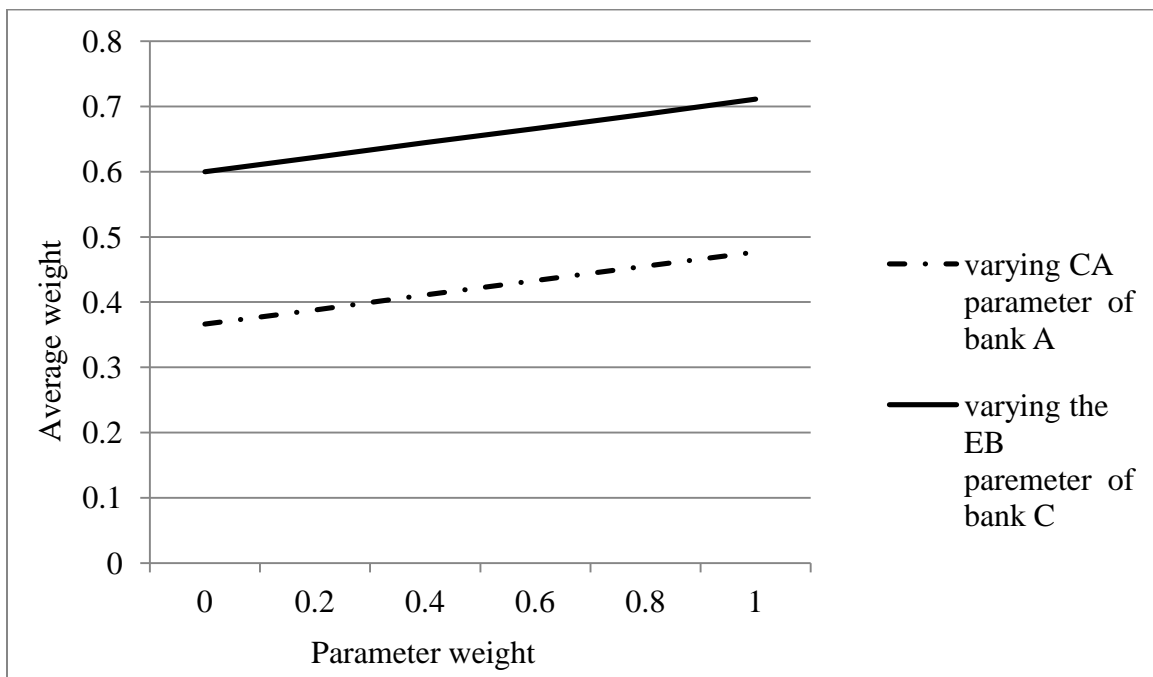


Fig. 4.3: Numerical incremental sensitivity analysis comparing bank A & C

The fig. 4.3 shows the numerical incremental sensitivity analysis of bank A and C by changing second (number of encryption bits) parameter of bank A and third parameter of

bank C. Graph shows that their average weight changes on changing parameter weight but their ranking is same.

The fig. 4.4 shows the numerical incremental sensitivity analysis of bank D, bank E bank F and bank G by changing first (CA) parameter of bank D third, SSL version (SV), parameter of bank E and first, cryptographic algorithm (CA) of bank F and first parameter of bank G. Graph shows that their average weight changes on changing parameter weight and ranking of F is not changed on changing parameter value but ranking of D and E will change when parameter value of bank E is zero and parameter value of D is zero.

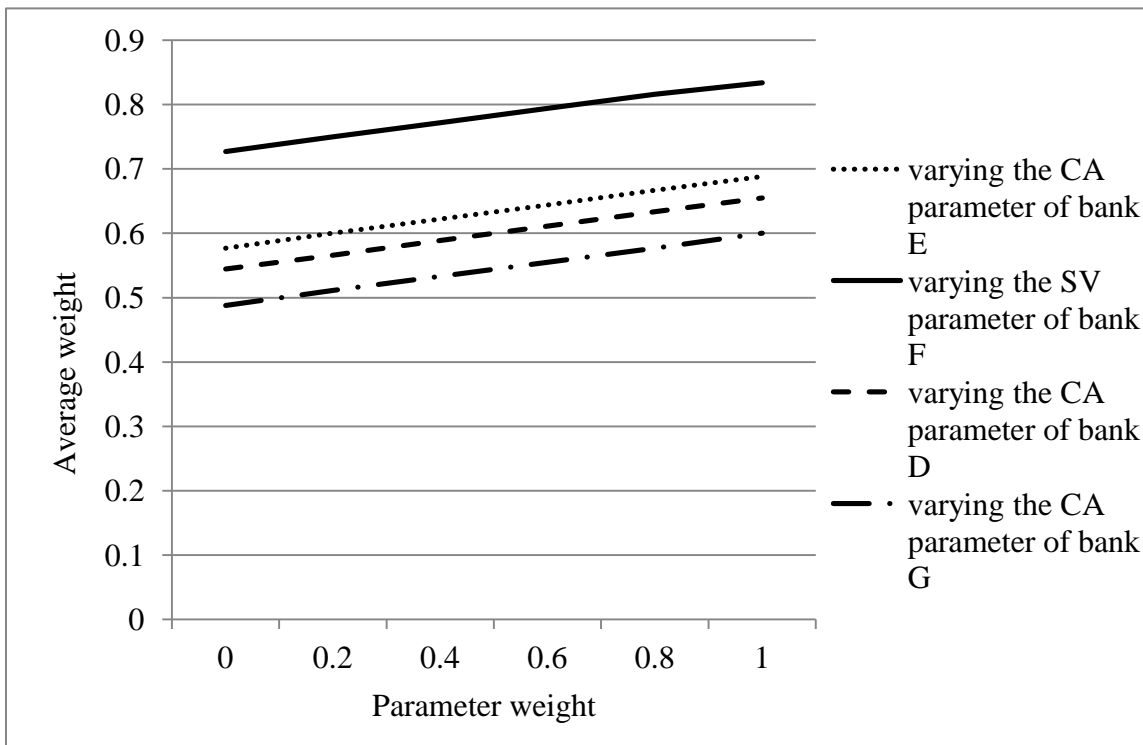


Fig. 4.4: Numerical incremental sensitivity analysis for banks D, E, F & G

Sensitivity of Parameter

Every parameter taken in multi-criteria decision making affects the ranking of plans. The parameter that affects most to the ranking of the alternatives is called most sensitive parameter. In this analysis the categorical measures, onscreen keyboard, SMS challenge,

second channel notification, are most sensitive parameters because their value may be either 0 or 1 and it makes huge difference on average weight on changing these values. Parameters in the MCDM are mutually exclusive.

4.3 IMPLEMENTATION OF PROPOSED USER AUTHENTICATION SYSTEM

The implementation screenshots of above discussed proposed user authentication system are shown on the appendix. Screenshots shows user registration page which requires name of the user, email address of the user, and password. After entering correct username and password by registered user, an email with one time password will be sent to user and has to enter it on login page for successfully login his account. Screenshots also shows that user is successfully logged in when his/her account is not logged from any other IP/location and user can perform any internet banking activities with one time password (OTP) authentication. If another user try with same username and password simultaneously from another location/IP then genuine user will be notified via email with details of location and IP.

4.4 CONCLUSION AND RECOMMENDATION

Internet banking is one of the most useful services provided by banks to their customers. It brings many benefits to banks, such as reducing costs, increasing competition and increasing profits. In terms of customers, it is possible for them to carry out financial transactions from anywhere and at any time. However, performing financial transactions using the internet banking through the internet is associated with many risks and dangers. From this point of view, it derives the importance of information security for internet banking systems provided by banks.

Comparison of internet banking web application security of different banks using multi-criteria decision making optimization technique has been done and most secure bank among selected banks was find out. During internet banking web application security analysis, weakness was found on user authentication process. Hence, another objective of

thesis was to enhance current user authentication system used on internet banking system. An improved user authentication system with two factor authentication has also been suggested and implemented as discussed on methodology and result section.

To make internet banking more secure and trustworthy user login only through registered device, where device registration will be using second channel verification, can be implemented as a future work of this thesis.

REFERENCES

- [1]. Mamta Jain, Jesal Vasavada, Gunjan Jain and Punam Patel, "Information Security and Auditing for Distributed Network", International Symposium on Instrumentation and Measurement, Sensor Network and Automation (IMSNA), 978-1-4673-2467-0/12 2012 IEEE
- [2]. Han-Na You, Jae-Sik Lee, Jung-Jae Kim, Moon-Seog Jun, "A Study on The Two-Channel Authentication Method Which Provides Two-way Authentication in the Internet Banking Environment", Computer Sciences and Convergence Information Technology (ICCIT), 5th International Conference, 978-1-4244-8567-3/2010 IEEE
- [3]. Teresa Susana Mendes Pereira and Henrique Santos, "A Security Framework for Audit and Manage Information System Security", International Conference on Web Intelligence and Intelligent Agent Technology, 2010 IEEE/WIC/ACM
- [4]. HUANG Zuo-ming, CONG Qiu-shi, HU Ji-bing, "Information System Risk Auditing Model Based on Process Mining", International Conference on Management Science and Engineering (19th) September 20-22, 2012, 978-1-4673-3014-5/12 IEEE
- [5]. Lyazzat B. Atymtayeva, Gerda K. Bortsova, Atsushi Inoue, Kanat T. Kozhakhmet, "Methodology and Ontology of Expert System for Information Security Audit", SCIS-ISIS, Kobe, Japan, November 20-24, 2012, 978-1-4673-2743-5/12 IEEE
- [6]. Cronin, Mary J., John Wiley and Sons "Banking and Finance on the Internet", ISBN 0-471-29219-2 page 41 from Banking and Finance on the Internet. Retrieved 2008-07-10. (1997)
- [7]. Rajpreet Kaur Jassal, Dr. Ravinder Kumar Sehgal "Comparitive Study of Online Banking Security System of various Banks" IJEBFA 13-358, 2013
- [8]. Luping Zhi, Xihao Zhou, "The Audit Method Research on Enterprise and Institution Information Technology Projects Invested by Government", 13th COTA International Conference of Transportation Professionals (CICTP 2013)
- [9]. Farshad havasi, Fattaneh Alizadeh Meshkany, Reza Hashemi, "E-Banking: Status, Implementation, Challenges, Opportunities", IOSR Journal Of Humanities

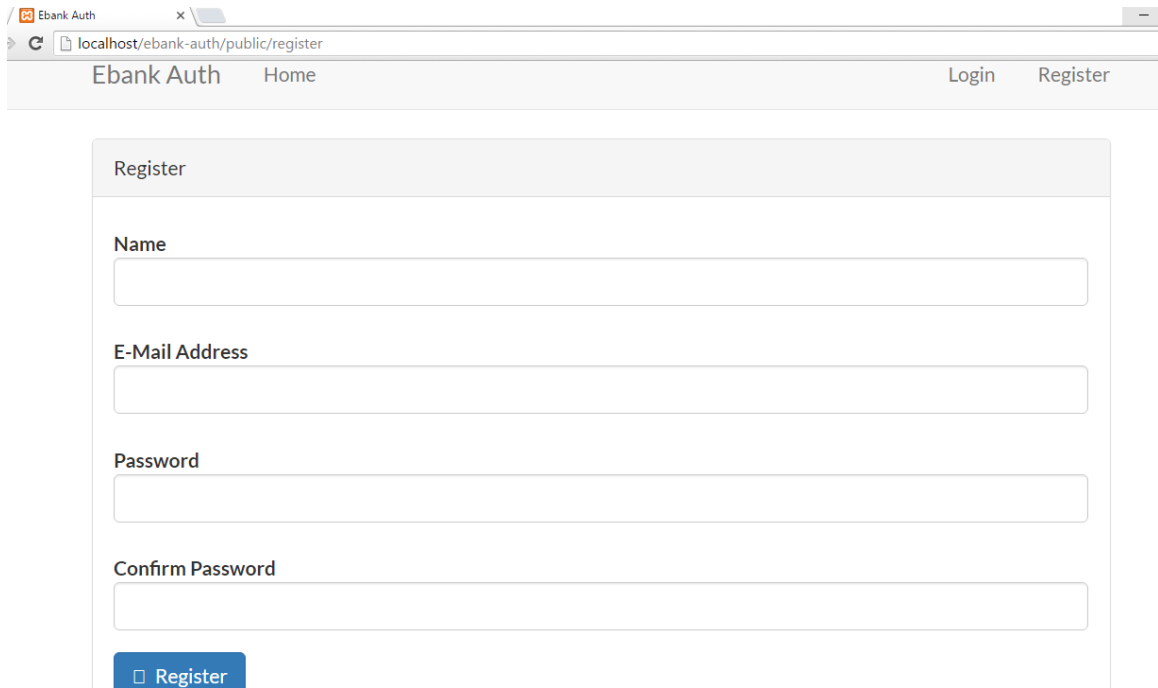
And Social Science (IOSR-JHSS), Volume 12, Issue 6, PP 40-48 e-ISSN: 2279-0837, p-ISSN: 2279-0845

- [10]. Adam Ali.Zare Hudaib, "Banking and Modern Payments System Security Analysis", International Journal of Computer Science and Security (IJCSS), Volume (8): Issue (2): 2014
- [11]. D. Venus and M. Saleh moman, "Identifying the Factors That Affect Bank Customer Trend to Use ATM Systems", International Journal of Knowledge of Management, 67, and 2004, and 157-177
- [12]. Mahmoud Musa Mohammed, Dr. Muna Elsadig, "A Multi-layer of Multi Factors Authentication Model for Online Banking Services", International Conference on Computing, Electrical and Electronic Engineering (ICCEEE), 978-1-4673-6232-0/13 2013 IEEE
- [13]. R. Priya, V. Tamilselvi and G.P. Rameshkumar, "A Novel algorithm for Secure Internet Banking with finger print recognition", International Conference on Embedded Systems (ICES 2014), 978-1-4799-5026-3/14 2014 IEEE
- [14]. R.Tassabehji , M.A. Kamala, "Improving E-Banking Security with Biometrics: Modelling user attitudes and acceptance", New Technologies, Mobility and Security (NTMS), 3rd International Conference, pp 1-6, 978-1-4244-6273-5/09 2009 IEEE
- [15]. Madhusudan, Valiveti, "Cryptanalysis of Remote User Authentication Scheme with key agreement", International Conference on Computer, Communication, and Control Technology (I4CT 2015), April 21 - 23, pp 476-480 978-1-4799-7952-3/15 2015 IEEE
- [16]. Bhole, Chaudhari, "Web based Security with LOPass User Authentication Protocol in Mobile Application", International Conference on Computational Intelligence and Computing Research, 978-1-4799-1597-2/13 2013 IEEE
- [17]. S. Basavala, N. Kumar, A. Agarrwal, "Authentication: An Overview, its types and Integration with Web and Mobile Applications ", 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, pp 398-401, 978-1-4673-2925-5/12 2012 IEEE

- [18]. Elvira Soufyani Rosanty, Halina Mohamed Dahlan, Ab. Razak Che Hussin, "Multi-Criteria Decision Making for Group Decision Support System", 978-1-4673-1090-1/12 2012 IEEE.
- [19]. Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona, "Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based on Various File Features", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, July 2014
- [20]. Alanazi, Zaidan, Jalab, "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal of Computing, volume 2, issue 3, ISSN 2151-9617, March 2010
- [21]. "SSL Server Rating Guide", 2009-2015 Qualys SSL Labs
- [22]. Javad Soroor, "Implementation of a Secure Internet/Mobile Banking System in Iran", Journal of Internet Banking and Commerce, vol. 10, no.3, December 2005
- [23]. Renzo Bertuzzi Leonelli, "Enhancing a Decision Support Tool with Sensitivity Analysis", University of Manchester School of Computer Science, 2012

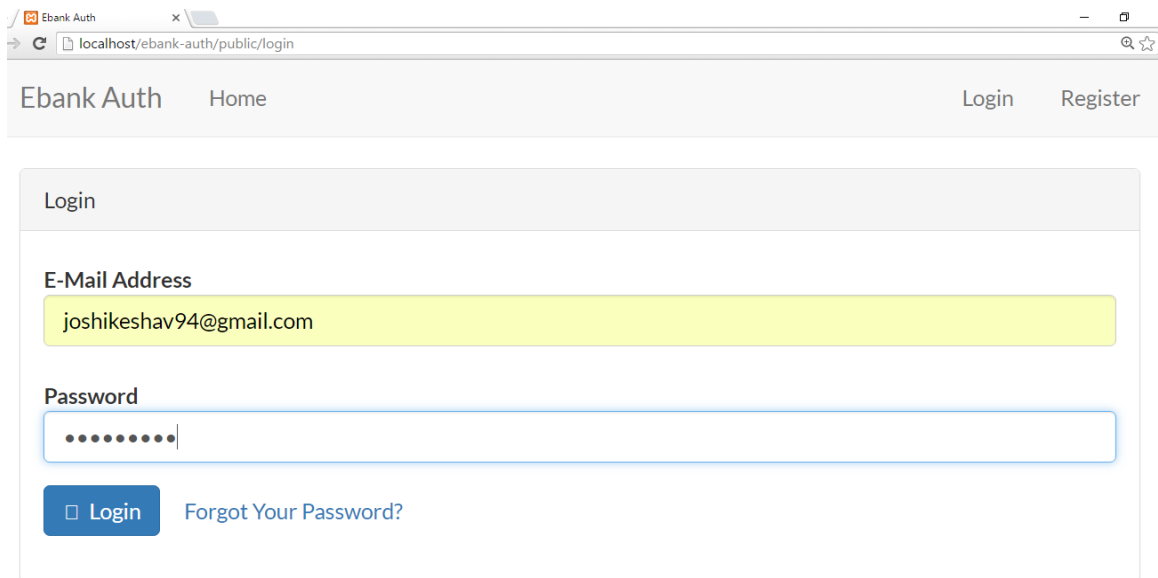
APPENDIX A

Output screenshots of proposed user authentication system



The screenshot shows a web browser window with the address bar displaying 'localhost/ebank-auth/public/register'. The page title is 'Ebank Auth' and the navigation menu includes 'Home', 'Login', and 'Register'. The main content area is titled 'Register' and contains four input fields: 'Name', 'E-Mail Address', 'Password', and 'Confirm Password'. A blue 'Register' button is located at the bottom of the form.

Fig. A.1: User registration page



The screenshot shows a web browser window with the address bar displaying 'localhost/ebank-auth/public/login'. The page title is 'Ebank Auth' and the navigation menu includes 'Home', 'Login', and 'Register'. The main content area is titled 'Login' and contains two input fields: 'E-Mail Address' and 'Password'. The 'E-Mail Address' field contains the text 'joshikeshav94@gmail.com' and is highlighted in yellow. The 'Password' field contains a series of dots. A blue 'Login' button and a link for 'Forgot Your Password?' are located at the bottom of the form.

Fig. A.2: User credentials entered

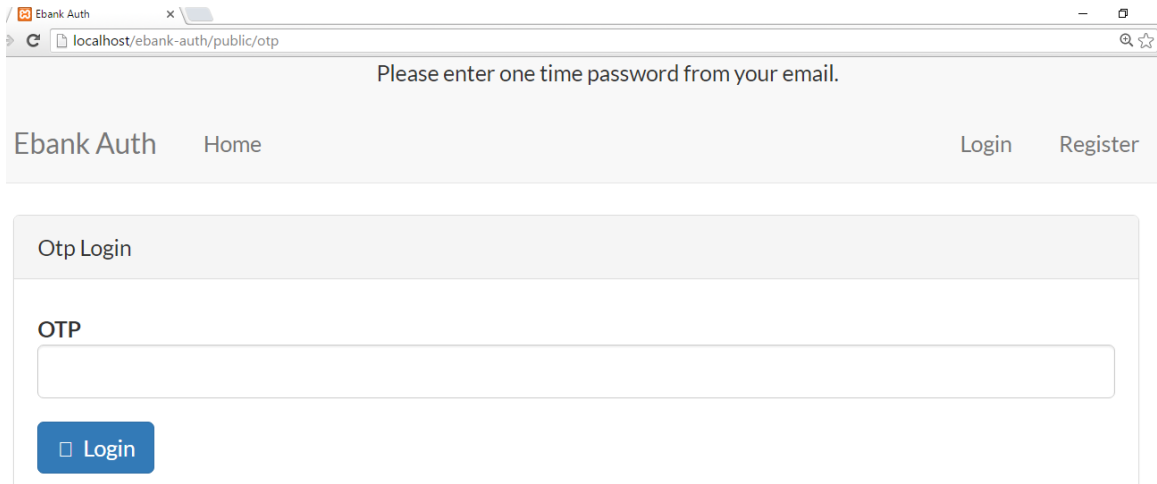


Fig. A.3: Request to enter one time password

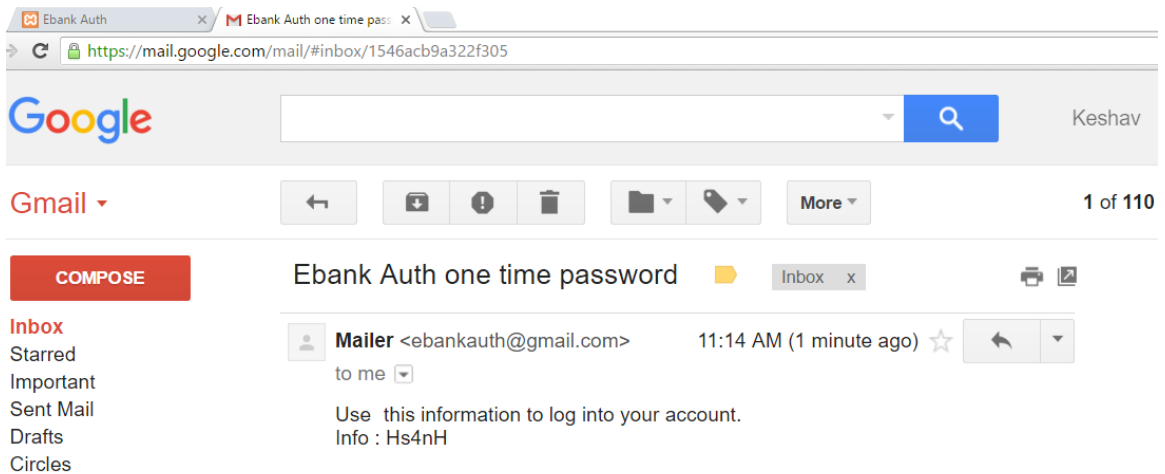


Fig. A.4: One time password sent on email

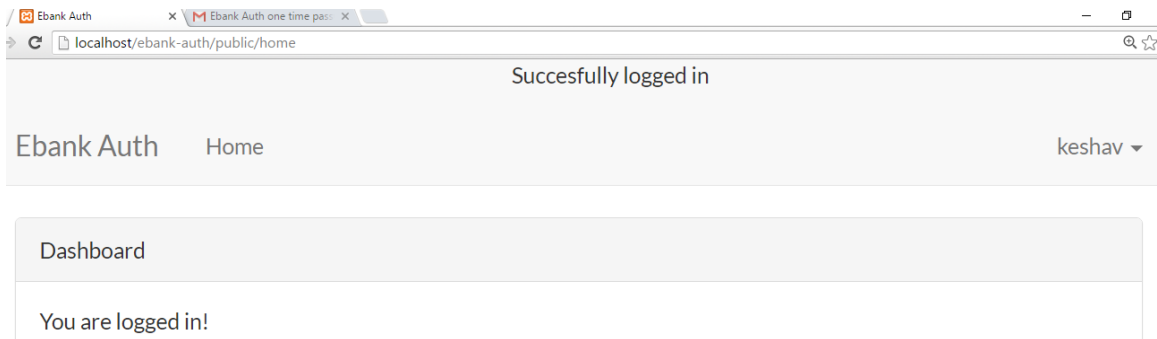


Fig. A.5: User logged in successfully

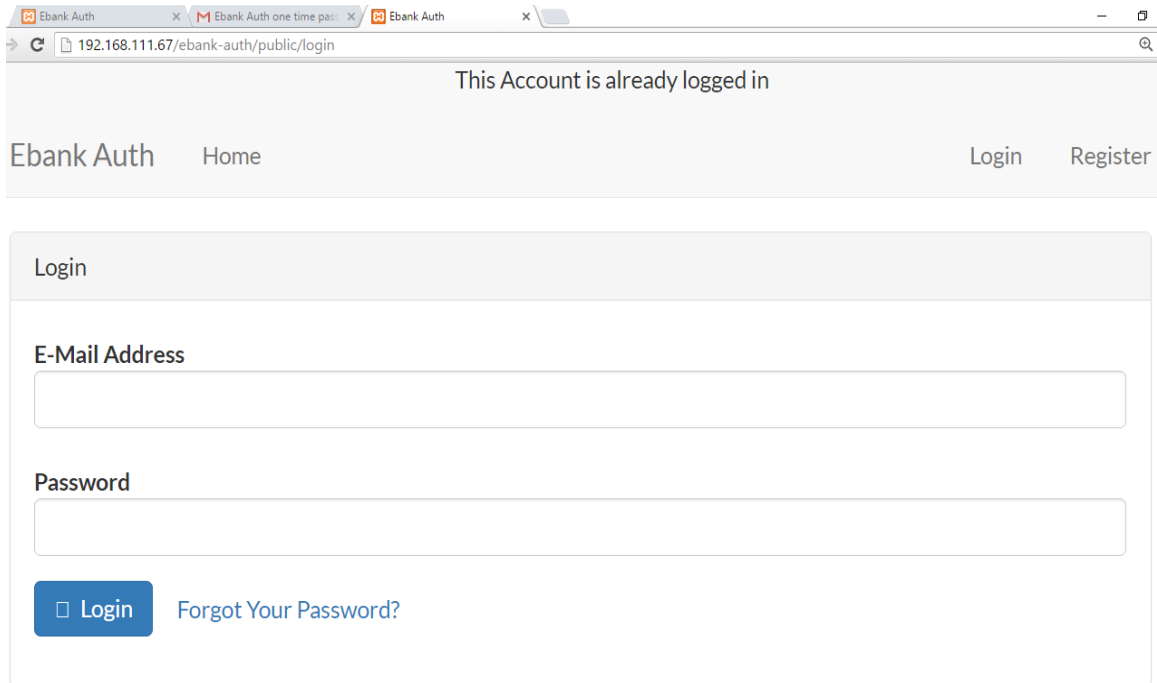


Fig. A.6: Denied login access on trying to login from another location on same time

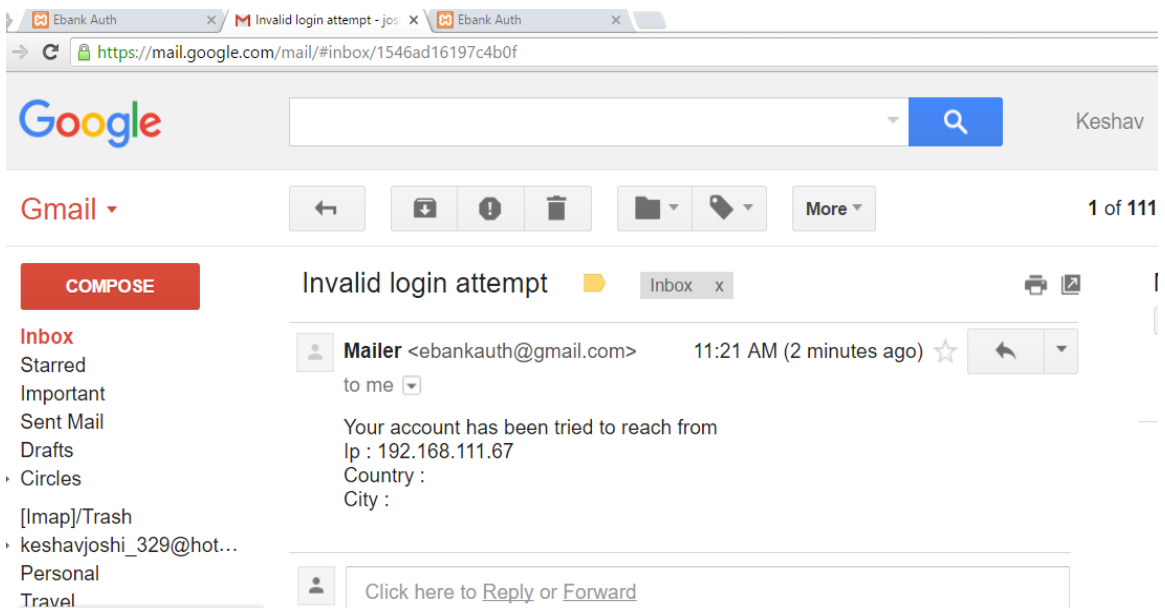


Fig. A.7: An email sent to genuine user notifying about invalid login attempt

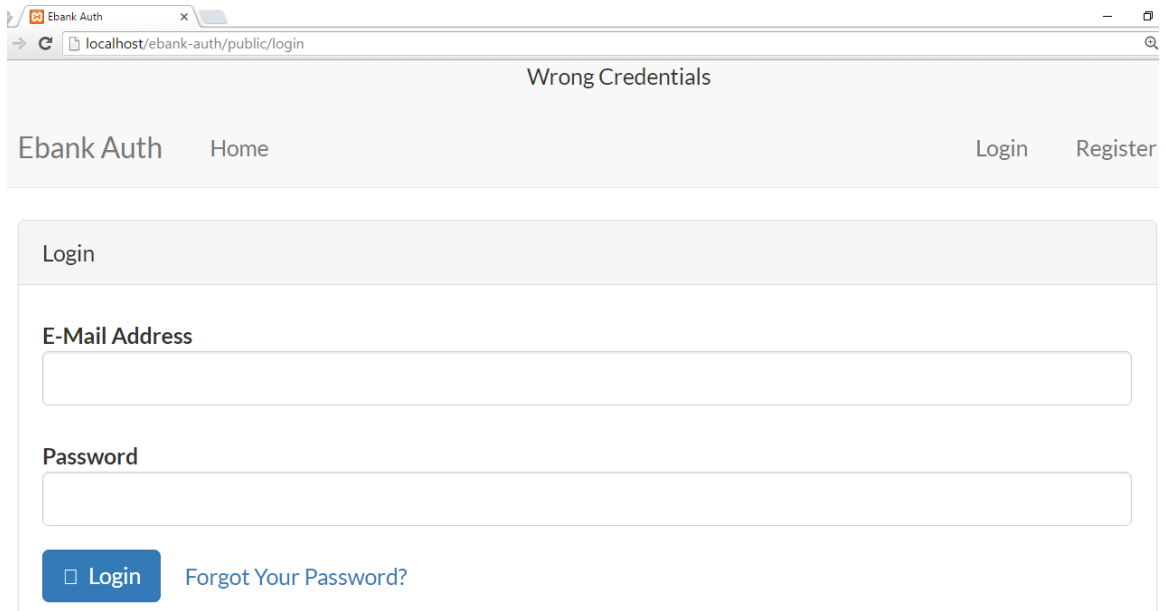


Fig. A.8: Login page on entering wrong username and/or password

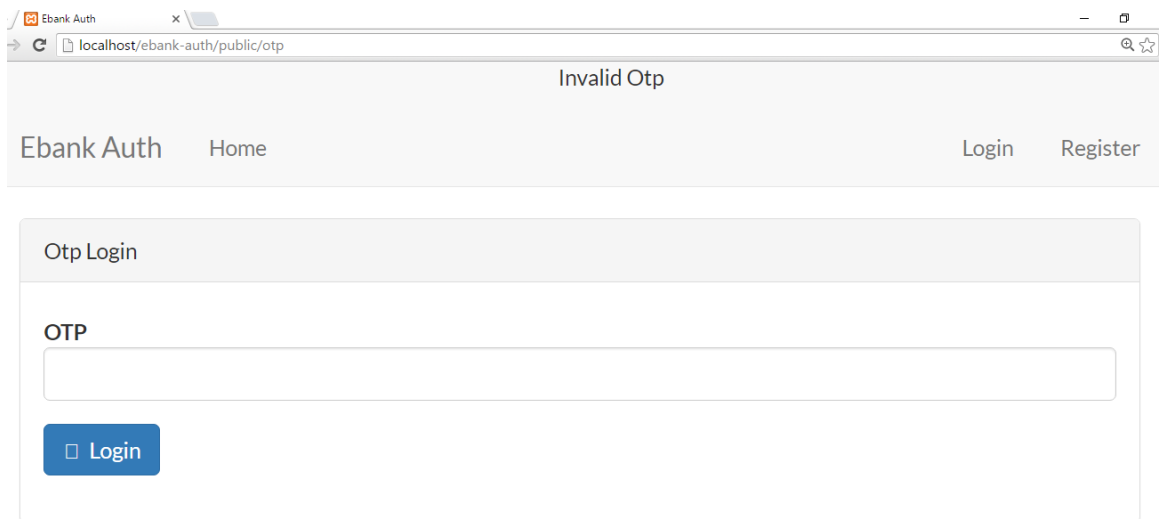


Fig. A.9: Message on entering wrong one time password