2019-03

A novel framework for secure e-commerce transactions: a case of Tanzania

Mlelwa, Kenneth Longo

NM-AIST

https://doi.org/10.58694/20.500.12479/305

A NOVEL FRAMEWORK FOR SECURE E-COMMERCE TRANSACTIONS: A CASE OF TANZANIA

Kenneth Longo Mlelwa

A Dissertation Submitted in Partial Fulfilment of the Requirements for the Degree of Doctor of Philosophy in Information and Communication Science and Engineering of the Nelson Mandela African Institution of Science and Technology

Arusha, Tanzania

March, 2019

ABSTRACT

The Internet technology development is building a huge opportunity to expand existing businesses and forming what is called a Global Economy, New Economy, or Electronic Commerce (eCommerce). General, eCommerce portrays business transactions that involve ordering, delivery and payment, customer services and intra business missions that make use of the internet as well as the digital networked computing environment that links individuals and organizations in business, government, industry and the home. On the other hand, many organizations are frightened by the new technologies, hesitant of how to take advantage of them, and doubting how these new technologies will sustain existing investments in infrastructures and skills. Adding up, eCommerce comes with a batch of challenges especially those related to trust and security issues. Security in eCommerce is the protection of eCommerce assets from unauthorized access, use, alteration, or destruction. Dimensions of eCommerce security are; *Integrity, Non-repudiation, Authenticity, Confidentiality, Privacy, Availability*. This eCommerce offers the banking industry huge opportunity, but also forms a set of new risks and vulnerability including security threats.

Without trust, a large amount of prudent business operators and clients may choose to abstain from use of the Internet and revert back to traditional methods of doing business. To defy this trend, the issues of network security at the eCommerce and customer sites must be constantly reviewed and appropriate countermeasures devised. These security measures must be implemented so that they do not inhibit or dissuade the intended eCommerce operation.

This dissertation analyzes the threat classification and control measures and on this basis, proposes a novel conceptual eCommerce transactions framework that integrates several security parameters, policy, stakeholders in business for proper and secure information exchange. A security plug-in software was developed and validated to measure the effectiveness of the proposed framework. Results show that; prior to commencing an eCommerce transaction, the merchant and customer parties must be registered by the Third-Party trustee (TPT); which will provide tokens for transaction to all Customers and Merchants parties involved. Thus when each customer and merchant gets their transactions tokens, then both parties start to communicate and this proposed framework will offer protection against security attacks. Hence, with this framework, a secure eCommerce information exchange can be achieved.

DECLARATION

I, Kenneth Longo Mlelwa do hereby declare to the Senate of Nelson Mandela African Institution of Science and Technology that this dissertation is my own original work and that it has neither been submitted nor being concurrently submitted for a degree award in any other institution.

.....

Kenneth Longo Mlelwa

Name and signature of Candidate

06th March 2019

.....

Date

The above declaration is confirmed

.....

Eng. Dr. Zaipuna O. Yonah

Name and signature of Supervisor

07/03/2019

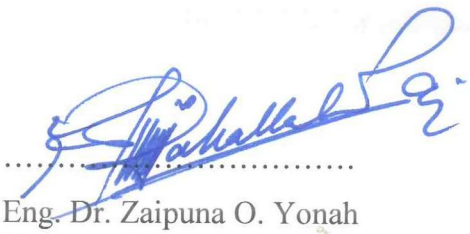
.....

Date

COPYRIGHT

CERTIFICATION

The undersigned certify that, they have read and hereby recommend for acceptance by the Nelson Mandela African Institution of Science and Technology a dissertation titled "A Novel framework for Secure eCommerce Transactions:" in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Information and Communication Science and Engineering of the Nelson Mandela African Institution of Science and Technology.



.....

Eng. Dr. Zaipuna O. Yonah
Name and signature of Principal Supervisor

07/03/2019
.....
Date

ACKNOWLEDGEMENT

First and above all, I praise God, the Almighty for providing me this opportunity and granting me the capability to pursue my PhD Studies successfully. This thesis appears in its current form due to the assistance and guidance of several people. I would therefore like to offer my sincere thanks to all of them.

I want to express my deep thanks to my esteemed supervisor Eng. Dr. Zaipuna O. Yonah for the trust, the insightful discussion, offering valuable advice, for his upport during the whole period of the study, and especially for your patience and guidance during the writing process.

I would also like to extend my appreciation to Miss. Bahati Swalehe; for her support and coordinating the students within the School of Computation and Communication Sciences and Engineering (CoCSE).

I would like to thank the Nelson Mandela African Institution of Science and Technology (NM-AIST) community and the Government of the United Republic of Tanzania for offering me a scholarship and supportive environment for the accomplishment of this study.

This work would have not been possible without the support from my employer, The Mwalimu Nyerere Memorial Academy (MNMA) especially the Department of ICT for granting me a study leave to attend the program.

Special thanks go to my parents, for their support and guidance during upbringing, without them, I would not have been who I am today.

I want to express my gratitude and deepest appreciation to my lovely boys, Mukisa-Christian and Charles-Bill, for their great patience and understandings especially when I (Dad) was busy with studies.

And finally, “I know that you did not want to be named”, a person that comforting and travel with me throughout my PhD studies, my lovely wife, Dear Ephrance, without your supports and encouragements, I could not have finished this work, it was you who looked after and take care of our family, and I understand it was difficult for you, therefore, I can just say thanks for everything, and may the Almighty God give you all the best in return.

DEDICATION

----*To my late Grandparents' Mr. Anthony Kasambala & Mrs. Regina Kasambala* ----

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS AND SYMBOLS

ABAC	Attribute-Based Access Control
B2B	Business-to-Business
B2C	Business-to-Consumer
BPSS	Business Process Specification Schema
C2B	Consumer-to-Business
C2C	Consumer-to-Consumer
CA	Certificate Authority
DMZ	Demilitarized zone
DoS	Denial-of-Service
DSL	Digital Subscriber Line
eBusiness /e-business	Electronic Business
ebXML	Electronic Business XML
eCommerce /e-Commerce	Electronic Commerce
eGovernment /e-government	Electronic Government
FIPS	Federal Information Processing Standard's
HTML	Hyper-Text Markup Language
HTTP	Hyper-Text Transfer Protocol
HTTPS	HTTP- Secure
ICT	Information and Communication Technology
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO/IEC	ISO & International Electro-technical Commission
IT	Information Technology
MAC	Mandatory Access Control
NIST SP	NIST Special Publication

NIST	National Institute of Standards and Technology
OS	Operating System
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
RBAC	Role-based Access Control
SAML	Security Assertion Markup Language
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SPSS	Social Sciences Software
SSL	Secure Socket Layer
SSO	Single Sign-On
TPT	Third Party Trustee
USA	United States of America
VBScript	Microsoft Visual Basic Scripting Edition
W3C	World Wide Web Consortium
WS	Web Services
WWW	World Wide Web
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language
XML-RPC	XML- Remote Procedure Call
XSS	Cross-Site Scripting
USP	Universal Secure Protocol

CHAPTER ONE

INTRODUCTION

1.1 Background of the Problem

As the World Wide Web (www) has grown so has the number of eCommerce merchants. The Internet has become a significant channel for business achievement, and as such, it is becoming the channel for business communications and transactions. This has led to growth in eCommerce. As there are some very well-known and high-profile eCommerce success stories so are many, many failures.

Worldwide development of Electronic commerce (eCommerce) might be hindered by old laws enacted at the time when it was still at infant level hence a need for uniformity in governing rules. It can be argued that the current security issues are likely to be affected by these rapid eCommerce changes, inviting alternative regulatory approaches that would not impede eCommerce adoption while advancing and ensuring protection of consumer interests.

Practically, security is a key issue for effective operation of an eCommerce application (Ghosh, 1998). Security threats include access control violations, integrity violations, sabotage, fraud, privacy violations, as well as denial of service (DoS) and infrastructure attacks. Collectively, all of these threats, have come to be known as cyber-war or cyber-terrorism (Ghosh, 1998). Essentially cyber-war is about corrupting the web and all of its components so that the targeted system collapses. There is currently lot of money allocated by various governments, for example, in the US and Western Europe, to conduct research on protecting the web and preventing cyber-wars and cyber-terrorism (Ghosh, 1998).

1.2 Statement of the Problem

In this era, accepting the adoption of ICT, including e-commerce by developing countries is becoming important to aggressively promote its adoption. As a result, ICT facilitates trade between developed countries with developing countries to be conducted more efficiently. With over 20% increase of eCommerce in developing countries, internet fraud has led to around US$ 2.8 billion revenue loss (Corporation, 2006). However, online merchants are using a huge amount of resources on security, yet fraud is still a mountain to climb for eCommerce (Kuchinskas, 2015). The challenge in anticipating frauds have made the study of security measures for secure eCommerce to be inevitable.

Various frameworks (methods and strategies) for different purposes have been deployed to implement security measures in eCommerce. To date still there is no general framework to suit all internet frauds for each situation. Some areas in eCommerce like networking, data transfer and data storage, scholars have applied scanning and testing methods, and modeling analysis to detect potential risks. For example, discretionary access control model, Mandatory Access Control (MAC) model, Role-based Access Control (RBAC) model and Access Control Tasks/Workflow are used to analyze access control functions (Joshi *et al*., 2000). With these methods a designer can deploy different features to describe a security perspective from different angles so as to understand, clarify and solve a security problem.

However, existing security frameworks though promising but more work is still needed to improve the models for describing abstract business logic. These frameworks should not focus on the technicality of the technologies, but rather on business logic and rules. E-commerce can be lucrative in several aspects, like in advertising and sharing profits from other vendors, and more eCommerce models are emerging. As a result of this promising business, researchers of security in eCommerce are looking to improve existing security frameworks to align with the latest technological or business development for developing countries (Jamieson and Cerpa, 2001).

At this stage, there is a need of having a framework to guarantee secure transactions in eCommerce. Therefore, it is the aim of this study to propose a framework that would facilitate eCommerce merchants to effectively conduct secure eCommerce transactions.

1.3 Research Objectives

1.3.1 General objective

The overarching objective of this study was to propose and develop a framework that would facilitate eCommerce merchants to effectively conduct secure eCommerce transactions.

1.3.2 Specific objectives

(i) To critically examine eCommerce trend in developing countries a Case of Tanzania.

(ii) To assess the main constraints that restrict the efficiency of security measures in e-commerce frameworks.

(iii) To analyze the requirements for secure transactions frameworks.

(iv) To develop a Security framework for assuring secure eCommerce transactions.

1.4 Research Questions

The study was guided by the following key research questions:

(i) What is the ecommerce trend in developing countries?

(ii) What are the current security issues and challenges facing eCommerce frameworks?

(iii) What are the main security risks/threats that are posed to eCommerce security frameworks?

(iv) What are the information requirements for secure eCommerce transactions?

1.5 Scope of Study

This study was conducted in Tanzania on Arusha, Dar es Salaam and Dodoma regionals. The choice for these regionals based on the following reasons: Tanzania is one of the developing countries located in Eastern Africa; technologically, the chosen country is still at infant stage in electronic services, implementation and service delivery. Besides, there has been few conducted studies in the area, particularly in IT security, e-government, and eCommerce. Additionally; there exists a number of security issues and challenges in relation to secure eCommerce transactions worthy of viable solutions.

1.6 Significance of the Study

The reported study was designed to:

(i) Contribute in encouraging effective use of IT infrastructures for eCommerce activities.

(ii) Provide knowledge to other academicians, researchers, and other people in the society as a point of reference or citation for their work.

(iii) Provide additional information to policy makers on how to restructure policies to guide use of electronic commerce services.

1.8 Dissertation Structure

In this dissertation, a novel framework for secure ecommerce transactions is proposed, developed and presented. The dissertation follows a paper-based format therefore chapter

two to five are fully supported by published literature. The rest of this dissertation is outlined as follows:

Chapter Two discusses and presents the current trend of eCommerce in developing countries with Tanzania as a case study. The chapter presents the challenges from both customer and merchant's perspective. The main obstacles identified from this chapter are the customer trust during and after doing an online purchasing.

Chapter Three discusses and presents an analysis and a review of challenges that restrict the efficiencies of security frameworks in eCommerce. Here, the chapter reviews various security mechanisms applied for online business and the challenges facing them.

Chapter Four Analyze the various requirements necessary for the development of a secure framework for eCommerce transactions. The chapter identifies, various factors that are needed during the development of the proposed framework. These include technical and non-technical factors.

Chapter Five proposes and presents the best fit framework for secure eCommerce transactions, in this chapter, various requirements are selected to be included for secure framework so as to achieve better secure transactions in eCommerce.

Chapter Six presents a summary of findings about the proposed secure framework for eCommerce transactions and concludes the dissertation, with recommendations.

CHAPTER TWO

E-Commerce Trend in Developing Countries: A case study of Tanzania[1]

Abstract

As the World Wide Web (www) has grown so is the number of eCommerce merchants. As there are some very well-known and high-profile eCommerce success stories so are many, many failures. The Internet has become an important channel for business success, and as such it is becoming the channel for communications and transactions. This has led to growth in eCommerce; and as this has grown so has the concerns about security. Often said security and trust are main reasons for consumers to hesitate to purchase from the internet. Unlike traditional commerce, absence of physical clues and physical interaction in the online environment makes it more difficult to establish trust with the consumers. Hence, it is more important for online venders to learn how to manage customers' trust in eCommerce; although creating customer's trust online is a challenge for most eCommerce companies. This chapter presents the results of the initial work of the study on A Novel framework for Assuring Secure eCommerce Transactions in developing countries; with Tanzania as a case study.

2.1 Introduction

In 2014, Tanzania had 7 590 794 internet users out of anticipated population of 44 928 923 (URT census, 2014) with an internet penetration rate of 15.3% (IWS, 2015). With the introduction of the first fiber optic international submarine cables in 2009 and 2010; availability of cheaper international bandwidth connectivity is set to revolutionize the internet activities of which up to that point completely relied on expensive satellite connections. As a result, the number of ISP in Tanzania has risen to 24 from 13 by 2002 (IWS, 2015).

Largely, the usage of Internet services is a focal point for sustainability of both economic and socio developments as it has enabled implementation of such service as e-government, e-learning, e-health, e-commerce, to mention a few (Miniwatts, 2015). Of all these electronic services, eCommerce is an important part of e-business commonly known as electronic commerce.

[1] This chapter is based on the paper: K. Mlelwa, B. Chachage and Y. Zaipuna. Article: E-Commerce Trend in Developing Countries: A Case Study of Tanzania. International Journal of Computer Applications 125(1):27-33, September 2015. Published by Foundation of Computer Science (FCS), NY, USA. BibTeX

For better understanding Electronic Commerce (commonly known as E-commerce or eCommerce), one should differentiate between e-commerce from electronic business (e-business); Ecommerce means electronic buying and selling on the Internet. E-business is any electronic transaction (e.g., information exchange), which subsumes e-commerce. E-business includes all activities that a firm performs in selling and buying services and products using computers and communications technologies. As such, e-business includes a host of related activities, such as on-line shopping, sales force automation, supply shopping, automation, chain management, electronic payment systems, web advertising and order management (Mlelwa and Tarimo, 2011).

Again, e-commerce is a subset of e-business. However, sometimes the two are used interchangeably. Consequently, E-business, a major contributor to the popularity of global information technologies, is a system that includes not only those businesses that center on buying and selling of goods and services to generate revenue, but also those transactions that support revenue generation.

Holistically, eCommerce means using technological advances to promote everything involving the exchange of business information among computers and humans or traders and customers (Wendy, 2000).

The concept of "transactional" e-commerce is further divided into four categories (Evans, 2002); namely business to business (B2B) (Shelly, 2002); business to consumer (B2C); consumer to business (C2B); and consumer to consumer (C2C) (Garbade, 2011; Digit, 2011).

2.2 Literature Review

Globally eCommerce is a growing sector which has so far yielded positive results. Since early 1990's there was no activity online as the Internet was a new concept. In 1999, 300 million users were online and about 75 million of them purchased goods and services via online worth $110 billion. This increased rapidly and by 2013 the amount generated from online transactions had increased to $1.25 trillion (WHO, 2013). In 2010, the United Kingdom had the largest e-commerce market in the world when measured in terms of the amount spent per capita (Robinson, 2010). The Czech Republic is the European country where ecommerce has the highest contribution to the enterprises´ total revenue. Almost a quarter (24%) of the country's total turnover is generated by eCommerce channel (Eurostat, 2010).

Other emerging economies, like China's e-commerce continues to grow every year. With

about 384 million internet users, China's online sales rose to $36.6 billion in 2009 and this is due to the huge growth supported by the improved trust level by shoppers. The Chinese merchants have been able to help online shoppers feel more comfortable (Robert, 2010). China's cross-border e-commerce is also growing at a good pace. E-commerce transactions between China and other countries increased by 32% to 2.3 trillion Yuan ($375.8 billion) in 2012 and accounted for 9.6% of China's total international trade (Frank, 2013). In 2013, Alibaba had an e-commerce market share of 80% in China (Steven, 2014).

The increase in Internet penetration, the spread of mobile technology and improvement in payment and delivery infrastructure are parameters that can boost eCommerce in Africa. The increase of middle class who are seeking more convenient shopping and better quality; attract both local and international Internet merchants to operate (yStart.com, 2013).

In Africa, 720 million people have access to phones and 167 million have Internet access. With internet penetration rapidly spreading across the East African region, it represents a huge potential which has hitherto been untapped. For example, in Kenya, there are about 30 million mobile phone subscribers and Internet penetration is also currently at 49.7%, with mobile data subscriptions making up most of it. Despite most people accessing Internet via mobile phones, fixed fiber subscriptions have also grown by 86.8% from FY 2011/2012 to FY 2012/2013. Despite positive trends in both mobile and Internet penetration, growth across countries varies and, in some cases, drastically. Mobile penetration in Tanzania, for example, is at 60% and internet penetration at 12%; much lower than Kenya. However, mobile and internet use is much higher in urban areas than compared to rural areas (Manyika *et al*., 2013). These trends show that eCommerce is poised to dominate East African specifically Tanzania, retail markets over the next five years (CCK, 2012), While market watchers may not be quite as optimistic in their forecasts, no one disputes that e-commerce on the continent is starting to take root (Ogundeji, 2014).

2.3 Methodology

2.3.1 Design of the study

The study was aimed at examining eCommerce trends in developing countries: a case of Tanzania. For this reason, the study adopted exploratory case study methodology. In social sciences and life sciences, a case study is a research method involving an up-close, in-depth, and detailed examination of a subject of study (the case), as well as its related contextual conditions. Although no single definition of the case study exists, case-study research has

long had a prominent place in many disciplines and professions (Mills *et al*., 2010; Robert, 2014).

2.3.2 Population

The targeted population for this study was defined as the totality of all stakeholders involved in eCommerce activities (mostly consumers) and aware of the opportunities that eCommerce has in developing countries. The population of interest is usually defined by the purpose of the research and the research question itself (Marczyk *et al*., 2005).

2.3.3 Sampling technique

Non-probability purposeful sampling was used to obtain a sample of informants that helps to obtain rich information based on their experiences. The study area was divided into various parts. Then, proportionate splitting of respondents was done for each part. Lastly, random sampling of participants was done from a defined population of interest (Saunders *et al*., 2007).

2.3.4 Data collection method and procedure

The semi-structured interview technique (Kvale, 1996) was carried out with various customers. The semi structured interview technique based on a pre-prepared topic was used to guide data collection. In this study, a questionnaire was used as a research tool. It was prepared and submitted to 213 respondents. Before collecting the data, a questionnaire was fully examined and pre-tested by the researchers. Then, it was cross-checked for apparent mistakes and unclear signals, and numbered for easy computerization and identification of each respondent.

2.3.5 Data analysis

All filled responses were checked to ensure accuracy and consistency in capturing information from the field. Using statistical Package for Social Sciences Software (SPSS) version 24 of 2015, the captured data was analyzed to produce frequency graphs and histograms. From frequency graphs and histograms interpretations have been done according to the research questions and objectives. Findings from in-depth interviews and focus group discussions regarding customers' experience on e-commerce activities, challenges, and perception were complemented by questionnaire using a quantitative approach. Both qualitative and quantitative data was used so as to help the researcher to realize and appreciate the experience associated with eCommerce trend in developing countries.

2.4 Results and Discussion

2.4.1 E-Commerce user Demographics

The researcher analyzed 213 responses collected through survey. Most respondents were of the age below 41 years (only 6% were above 41 years) and mainly male (62%) (Fig. 1 and 2). One of the limitations faced while using the data collection tool was the representation of females being drastically low. Also, it was found that only 8% of respondents had education at level of secondary education and below (Fig. 3), and 68% (Fig. 4) responded as having a positive attitude towards purchasing goods and services over internet. Only 15% were of negative attitude and the rest said they have no opinion on that.

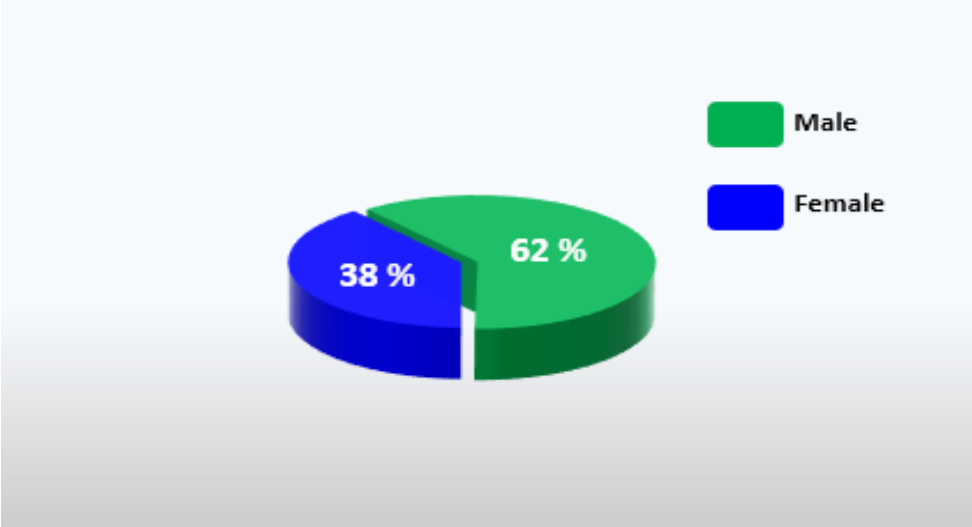


Figure 1: Gender distribution among respondents

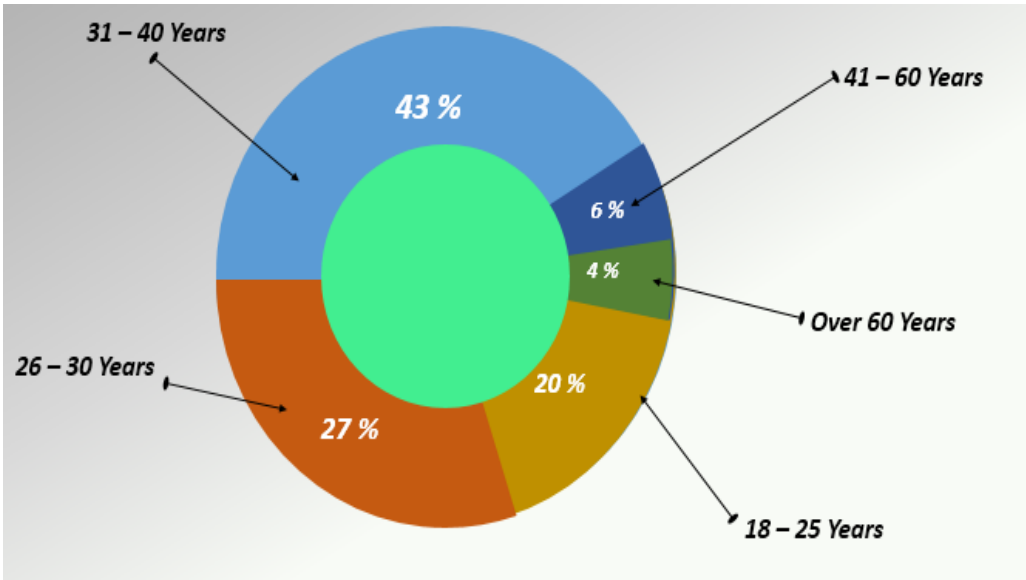


Figure 2: Age distribution among respondents.

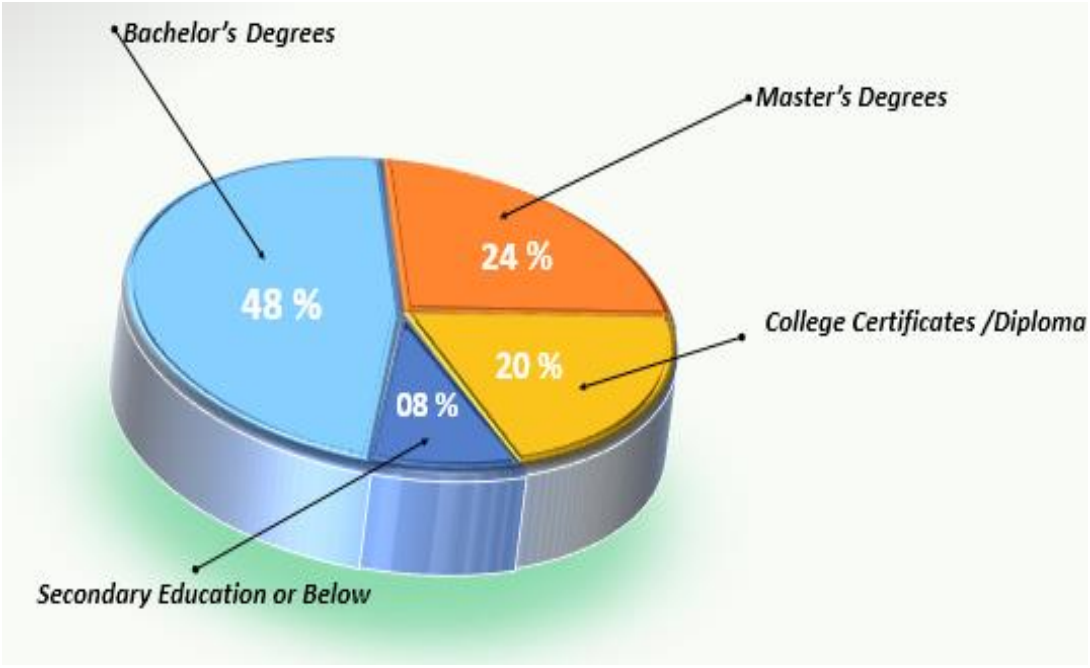


Figure 3: Represents the Education distribution.

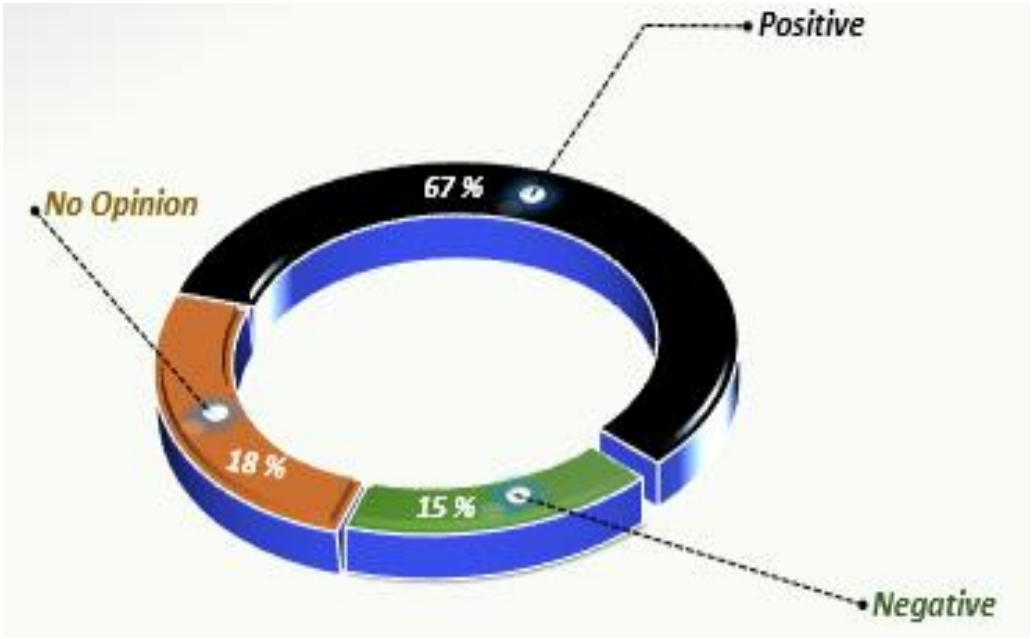


Figure 4: An attitude towards purchasing goods/services over internet.

2.4.2 Usage and Barriers for online shopping

In terms of usage of internet for shopping 100 respondents, which is 47%, said they had never used the internet for shopping, and this could be coursed by either their worries about their safety of payment and Low trust level on online store; as illustrated in Fig. 5.

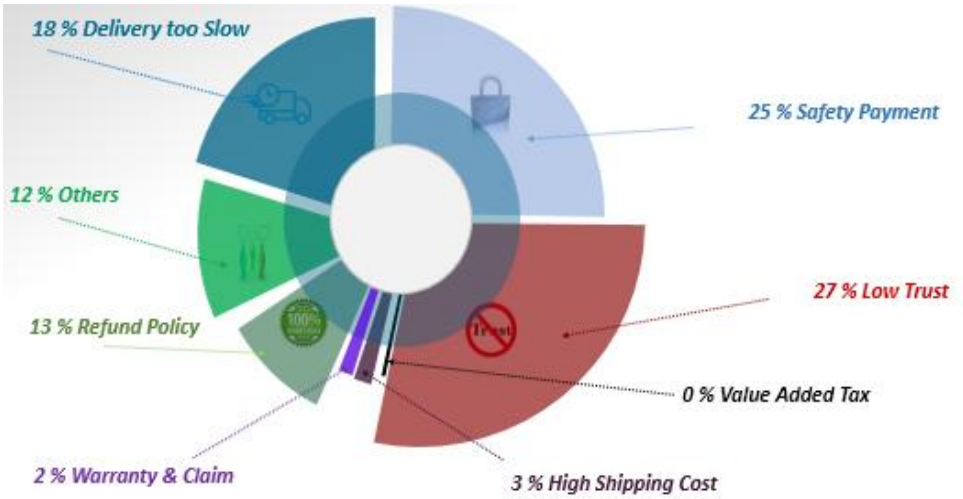


Figure 5: Barriers for online shopping.

2.4.3 E-Commerce trend

It has been noted that; for the past three years the number of online shoppers has increased yearly (Fig. 6), which means more awareness to eCommerce. The introduction of smart phones has catalyzed online shopping activities, especially for electronics goods such as Mobile phones and laptops (32%), Clothes (21%), Music/Software (13%) and Books (17%) (Fig. 7); however still there is a significant number of other commodities (27%) such as buying electricity online and payment for air tickets are among the major activities by online shoppers.

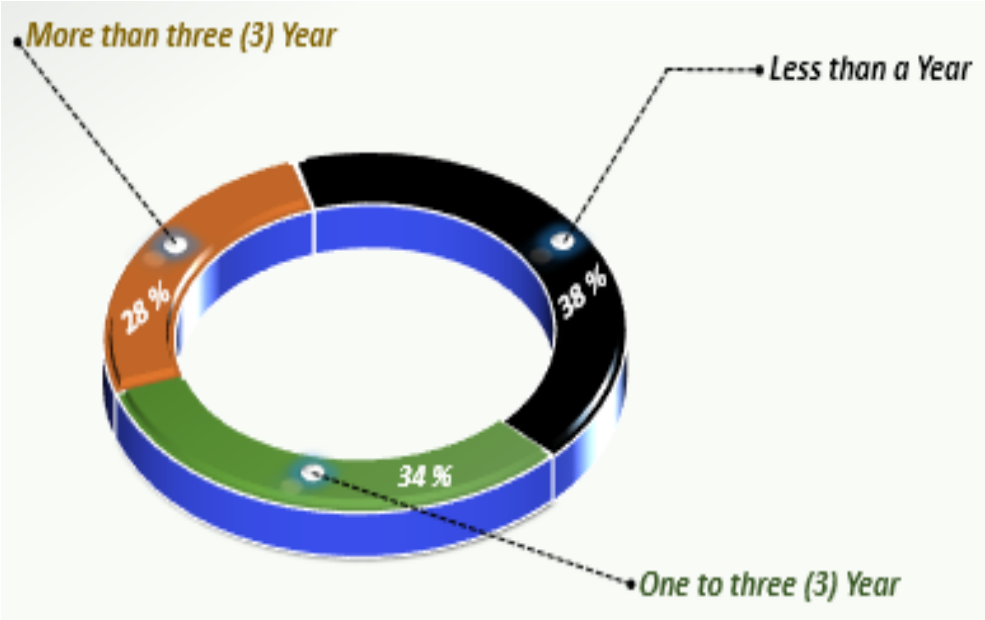


Figure 6: Depict as how long have they been shopping online.

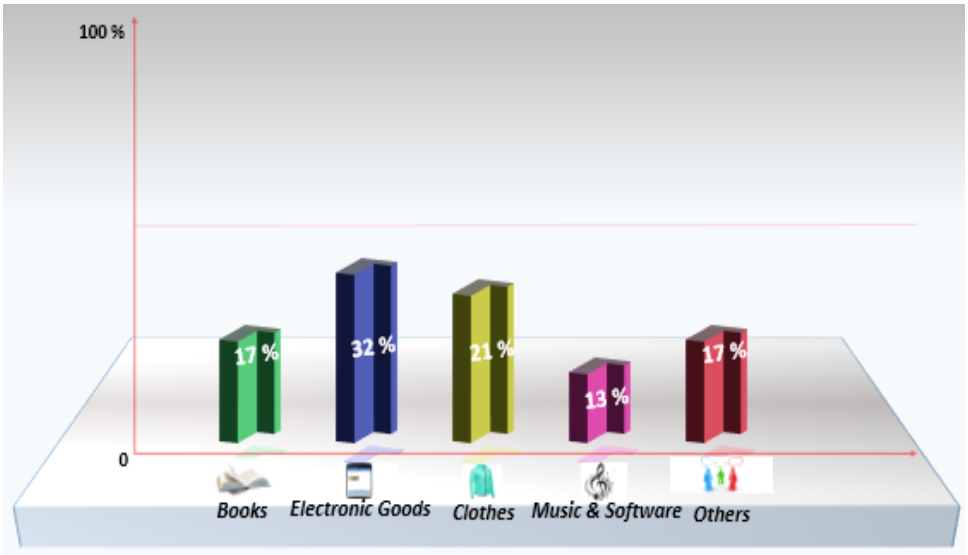


Figure 7: Most popular online shopped products.

The main reasons that force customers to shop online according to this study includes Convenience and Time saving (33%), Price (21%) and Brand conscious (16%) (Fig. 8). It has been found that 28% (Fig. 9) of those who normally shop online have to go to retail stores before making their final purchase. Again, except 8%, the rest responded that they do visit more than one online store before they make their mind on actual purchase; Fig. 10 depicts this.

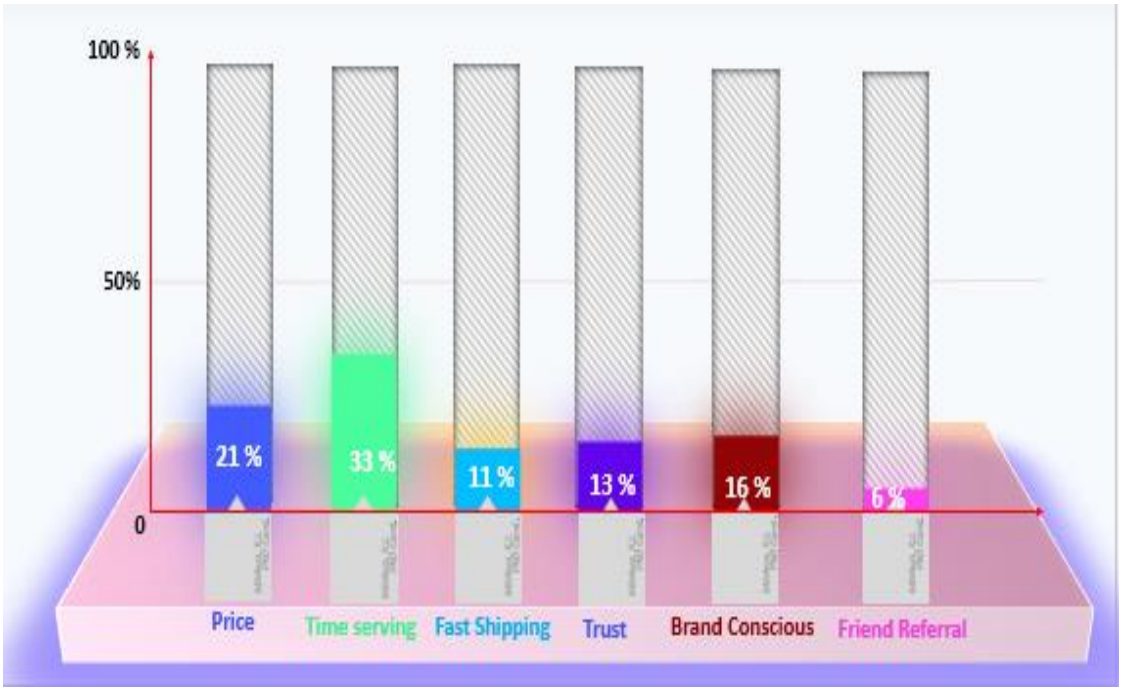


Figure 8: Main reasons for online shopping

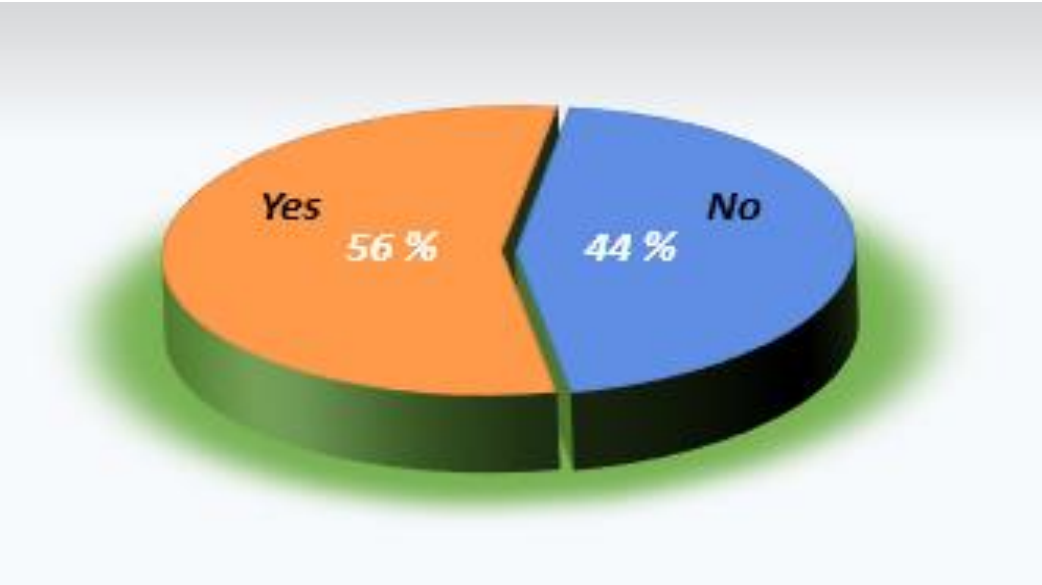


Figure 9: Online customers who are visiting traditional stores before purchasing online.

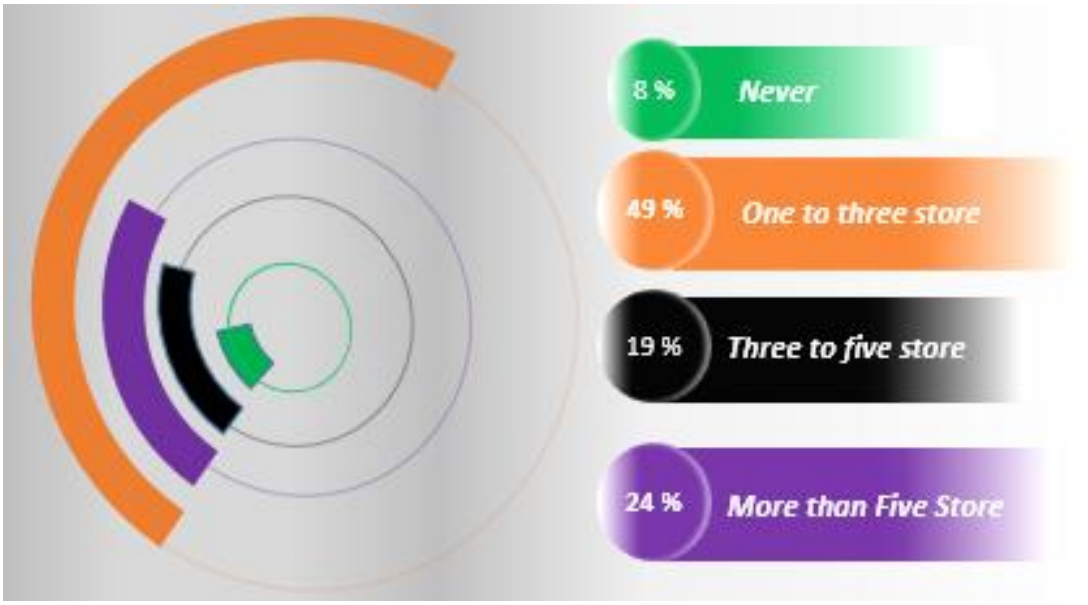


Figure 10: online customers who are visiting other online stores before purchasing online.

Results from various respondents show that; online advertisements play a vital role on recruiting online purchasers. From this study it was found that about 48% of respondents have been attracted first by advertisements before they purchased online and 40% of respondents were referred either by their friends or family of a certain product before they decided to purchase. Fig. 11 depicts this.

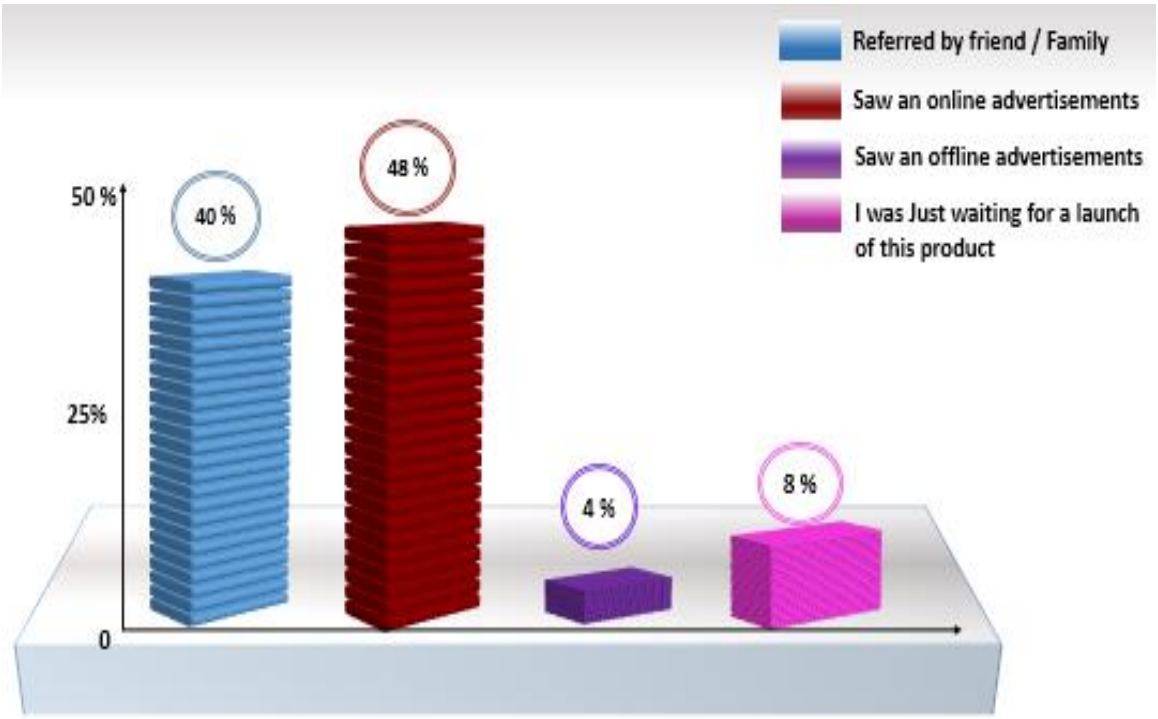


Figure 11: Results owing where customers got their Ideas before buying products online.

2.4.4 Security and Privacy

One of the critical success factors of e-commerce is security and privacy. Without the assurance of it, eCommerce may not work normally. And it is a complexity issue, because e-commerce security relates to the confidence between sellers and buyers. There is wide agreement between academic researchers that security is not only a technical challenge; rather it involves managerial, organizational and human dimensions to be more effective (Bjorck, 2004; Elofe, 2003). Therefore, understanding (and acting upon) customer's perception of security is vital to successful e-commerce interactions, because even when a company uses the best technical solutions that provide full security, without the underlying perception and awareness from customers that their particular website is secure, then these technical solutions may mean nothing.

As can be seen in Fig. 12, the vast majority of the respondents, 52% and 30% perceived secure and reliable payment systems to be very important.

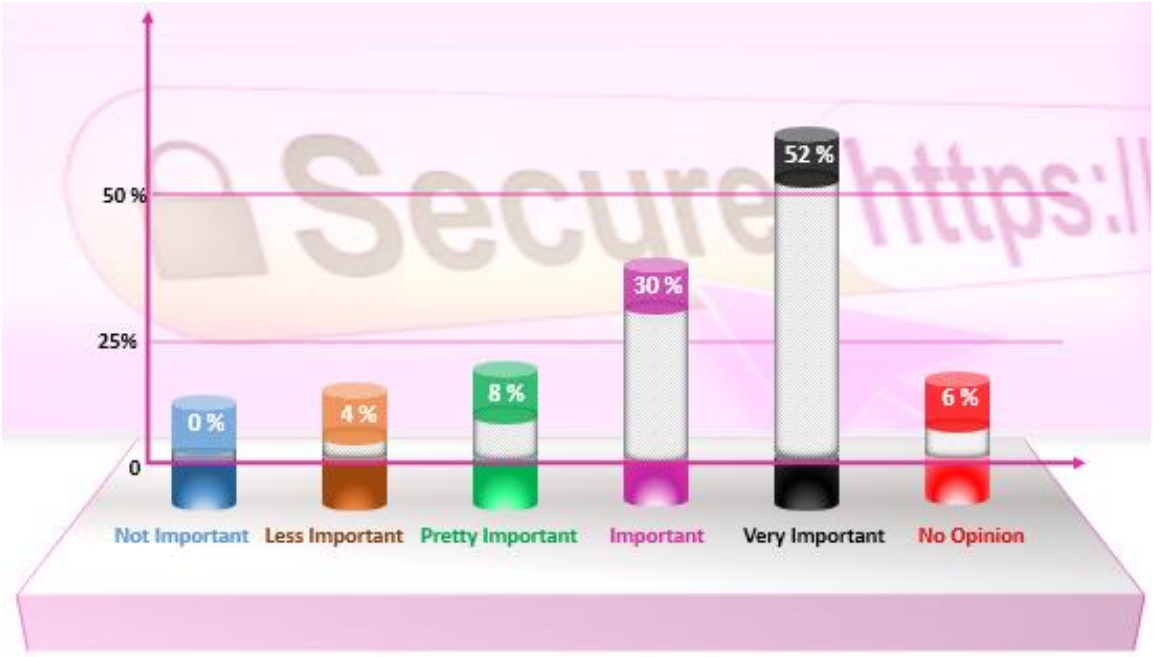


Figure 12: Results confirming the importance of Secure and Reliable payment systems.

On the category of information about how security works, the researcher found that 57% and 28% of respondents perceived this sub factor to be very important and important, respectively (Fig. 13).

Figure 13: Results on Customers' information about security issues.

Results from various respondents showed that; majority of respondents thought that it is very important to know how their personal information is handled, such that their personal details won't end up in the hands of wrong guys.

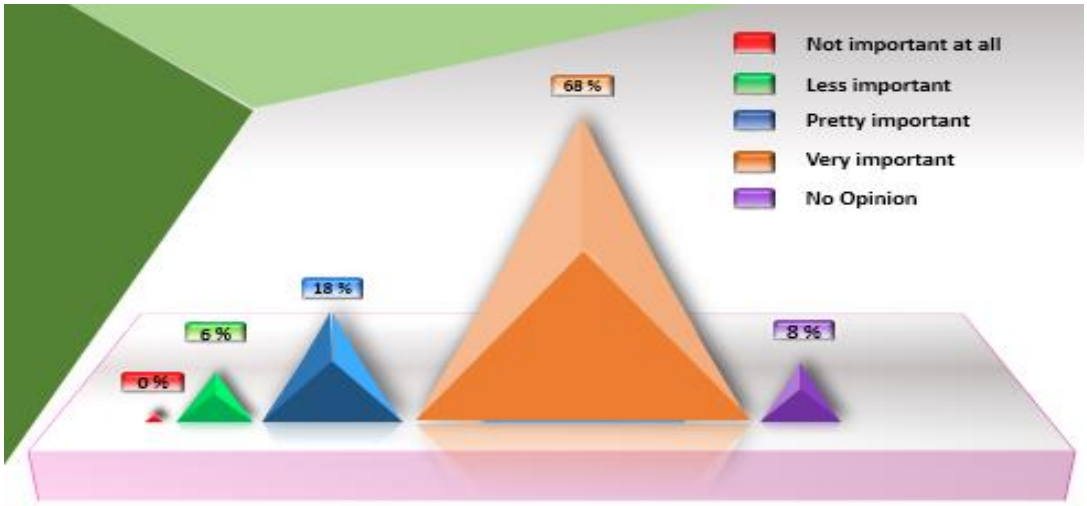


Figure 14: Results on handling on personal information filled when ordering online.

2.4.5 Guarantee and Customer Services

This part is concerned with a measure of customer's Guarantee and Services. Previous studies (Semeijn *et al*., 2005) have found that loyal customers are crucial to eCommerce survival because the competition is just a mouse click away. Unfortunately, there are always situations where service failure occurs during service delivery. The service recovery policy is considered a key factor to influence customer satisfaction. It has been noted that; the majority of respondents answered Very important and important on a category of standard terms in connection to the order form (see Fig. 15).

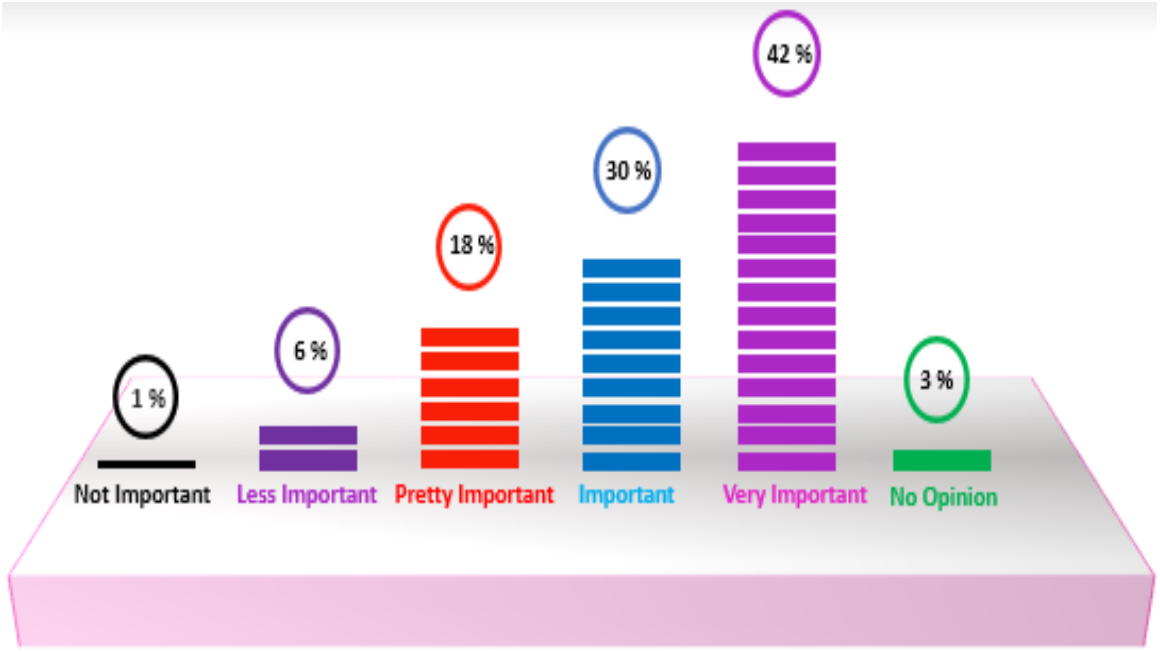


Figure 15: Rating of the standard terms in connection to an order form.

2.4.6 Website and Brand

The internet offers both growth and loyalty opportunities for brands. To this end, over recent years, companies have accelerated the development of their websites to include richer and more interactive content. Fig. 16 and 17 demonstrate the satisfaction of visitors with overall website and brand experience. These figures show that Brand, Reputation and recommendation of the Brand are rated almost equally by users. Higher rating of these two factors imply that customers are more inclined to revisit and recommend a site and in turn develop more positive attitudes toward the brand as well as higher purchase intent.

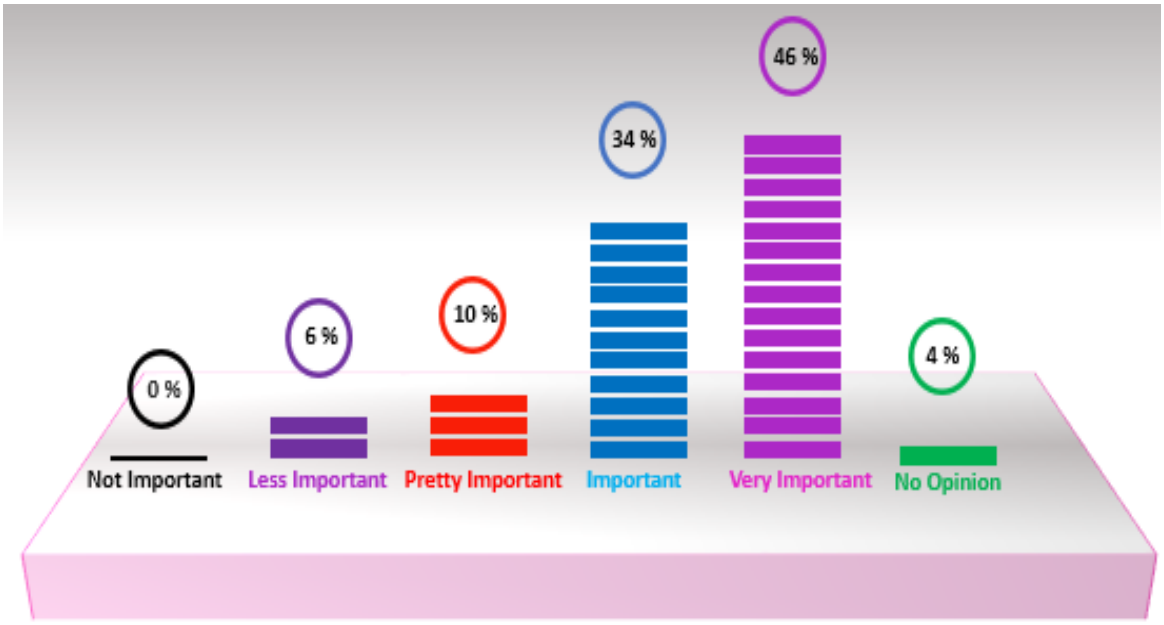


Figure 16: Rating of the product brand.

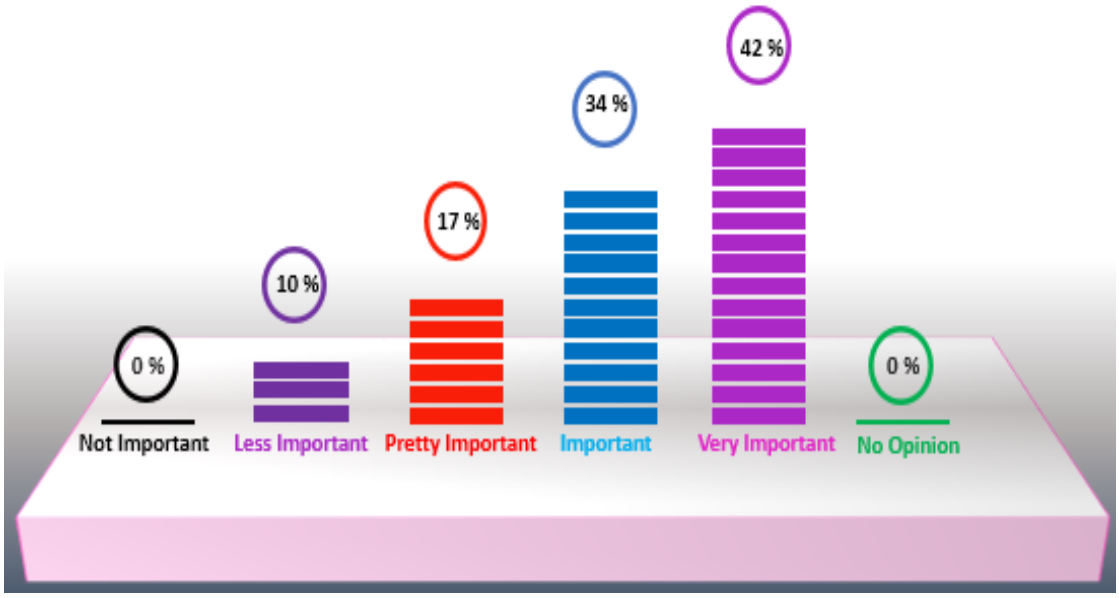


Figure 17: Reputation and Recommendation.

It was also found that: the design of the website is not much important; what matters is the functionality. Correspondingly, on the design of the website only 34% and 28% of the surveyed respondents with were responded on Very important answers and important respectively.

Figure 18: Rating of the design and functionality of a website.

2.4.7 Control and Price

One important way in which information technology is affecting work is by reducing the importance of distance. The Internet is a powerful means to connect buyers and sellers quickly, efficiently, and at a very low cost, regardless of whether there are just a few trading partners or thousands. Sharing product information and enabling online ordering is just the beginning. Essentially, what is transforming online business is the adoption of dynamic pricing as an integral part in the overall eCommerce solution. In this study, the question of "how do you rate the convenience of using internet and the technology?" Was imposed to interviewee where by the majority responded with on Very important (42%) and 34% responded with just important. Thus, inventing new techniques of doing business online would result in attracting more customers especially in developing countries like Tanzania.

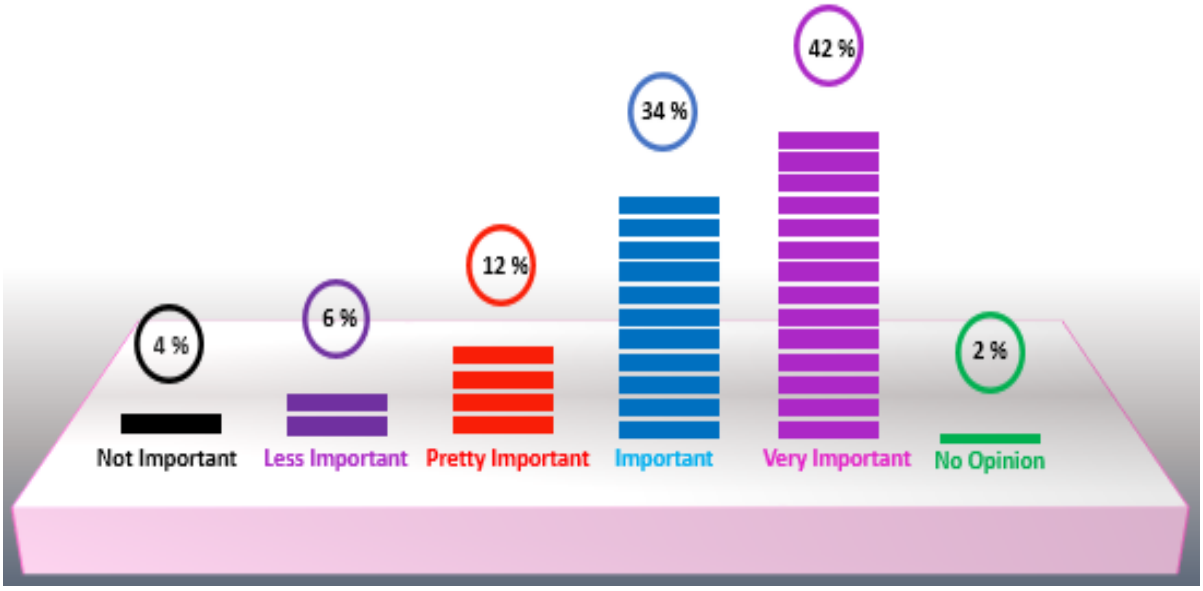


Figure 19: Convenience of using internet and the technology.

It has been found that; the majority of respondents about 56% (equivalent to 83% of 12%, 26% and 56%) answered that price is a very important factor for online shopping (Fig. 20).

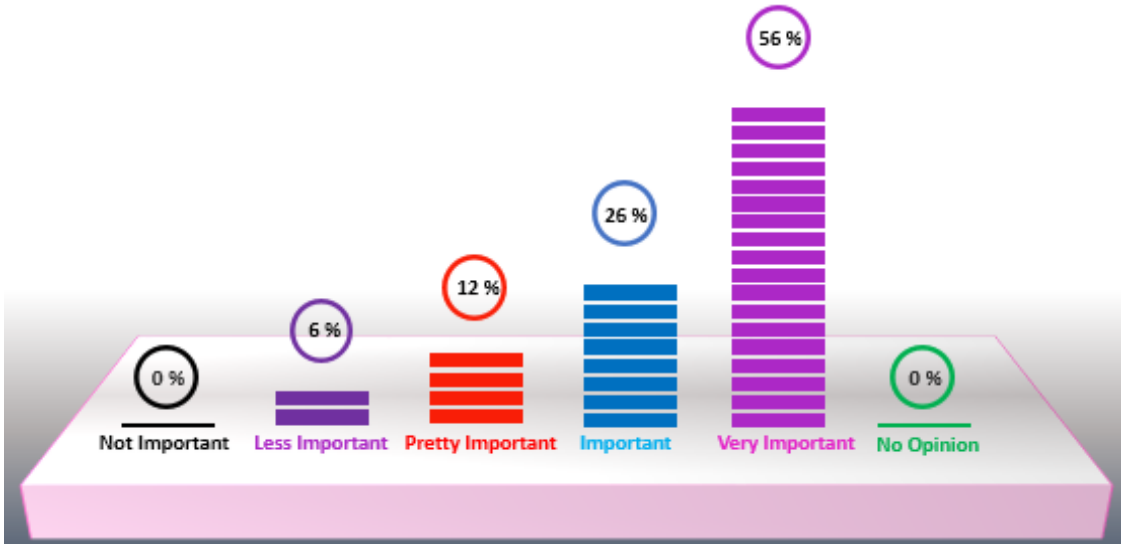


Figure 20: Importance of price of a product/Service.

2.5 Conclusion and Recommendations

This chapter focused on examining the trend of eCommerce in Tanzania. As eCommerce is rapidly growing in developed countries, to the contrary, in developing countries like Tanzania it is completely different. According to this study, trade over the Internet has not been quickly adopted in this region owing to number of infrastructures is the very foundation of eCommerce. Such that the issues of epileptic internet coverage, bandwidth and appropriate technology should be given a lot of priority.

(i) Investment in trainings and other enlightenment programs is vital to attitudinal changes to the public as most of the respondents claim that they have never used this kind of services. This implies that there is need of publicity.

(ii) Adequate attention should be paid to risks and security, which is a *major issue* for consumers to shy away from using eCommerce in general; with their main reason being safety of payment and low trust.

(iii) To ensure eCommerce success, financial and regulatory issues must be tackled. Ecommerce defined simply as electronic delivery of a product or service implies that customs and taxation regulations must be altered.

CHAPTER THREE

Challenges that restrict the Efficiencies of Security Frameworks in eCommerce: A Review[2]

Abstract

Most of the businesses all over the world have a presence on the Internet to offer everything possible. Some of these businesses have succeeded and some have failed spectacularly. The only thing that the successful organizations have in common is that they understand that they are doing eCommerce to make money. Businesses that prefer to perform eCommerce are taking a risk. They are investing in new knowledge and latest ways of providing goods and services expecting to generate a profit from the activity. The jeopardy to the organizations comes from numerous areas: the public may not accept the service, the new clients may not appear, or existing clients may not prefer the new service. Therefore, organizations performing eCommerce have a whole new set of threats and vulnerabilities that should be considered. These new threats and vulnerabilities generate new risks that must be managed. Thus, Security in eCommerce has grown to be inevitable and hence this chapter presents a different set of security challenges facing eCommerce transactions which were investigated, identified and classifies.

3.1 Introduction and Literature Review

Electronic commerce is any economic or business activity that uses Information Communication Technology (ICT) based applications to facilitate the buying and selling of products and services and to facilitate the transactions of trade activities between and among merchants, individuals, governments or other organizations. This includes using ICTs to toughen a company's internal activities, such as logistics, procurement, and human resource and contracts management, information as well as data management, communication functions, and to assist the flow of products between merchants and customers, e.g. marketing, ordering, payment, delivery, and searching for suppliers (Wanjau *et al*., 2012). From economic advantages point of view, eCommerce has several benefits such as increasing market expansion, reduction of product source prices, promotion of productivity, reducing of operation costs and inflation, reducing uncertainty, sharing market information, and aiding in

[2]This chapter is based on the paper: Kenneth Longo Mlelwa and Zaipuna O Yonah. Challenges that Restrict the Efficiencies of Security Frameworks in eCommerce: A Review. International Journal of Computer Science and Information Security 15(3), March 2017

.

distribution channel efficiency and plays a fundamental role in an endogenous economic growth (Molla *et al*., 2006). E-Commerce it can also be a source that develops domestic economy and fast globalization of production, and development of available technology (Sheth and Sharma, 2005). Both Africa and the Middle East experience very specific issues that need to be integrated into world agenda and agreements, where the obstacles are very well understood and have been researched by many (Molla and Licker, 2005; Travica, 2002).

Holistically, e-commerce refers to using technological development to promote everything involving the exchange of business information among computers and humans or traders and customers (Wendy, 2000). Due to that; everyone who is using eCommerce needs to be concerned with the security of their personal information. Thus, this chapter reports are the main constraints that restrict the efficiencies of security frameworks in e-commerce.

3.2 Existing Security Frameworks

Security is clearly defined as the state of being secure that is free from danger and threats, as well as to be protected from adversaries, which are those who would intentionally or unintentionally do harm. E-Commerce security is the protection of information, systems and hardware that store, use and pass on information throughout a digital transaction.

Many existing security frameworks concentrate on three areas; namely: detection by using scanners, prevention by using tools such as proxy and firewall, and recovery using tools regarding cryptography techniques and proper planning. These frameworks specifically address the problems of security and confidence from theoretical and practical perspectives (Jamieson and Cerpa, 2001). The frameworks include those actors that interact with and play the role in Ecommerce or may contribute to its improvement (Fig.21).

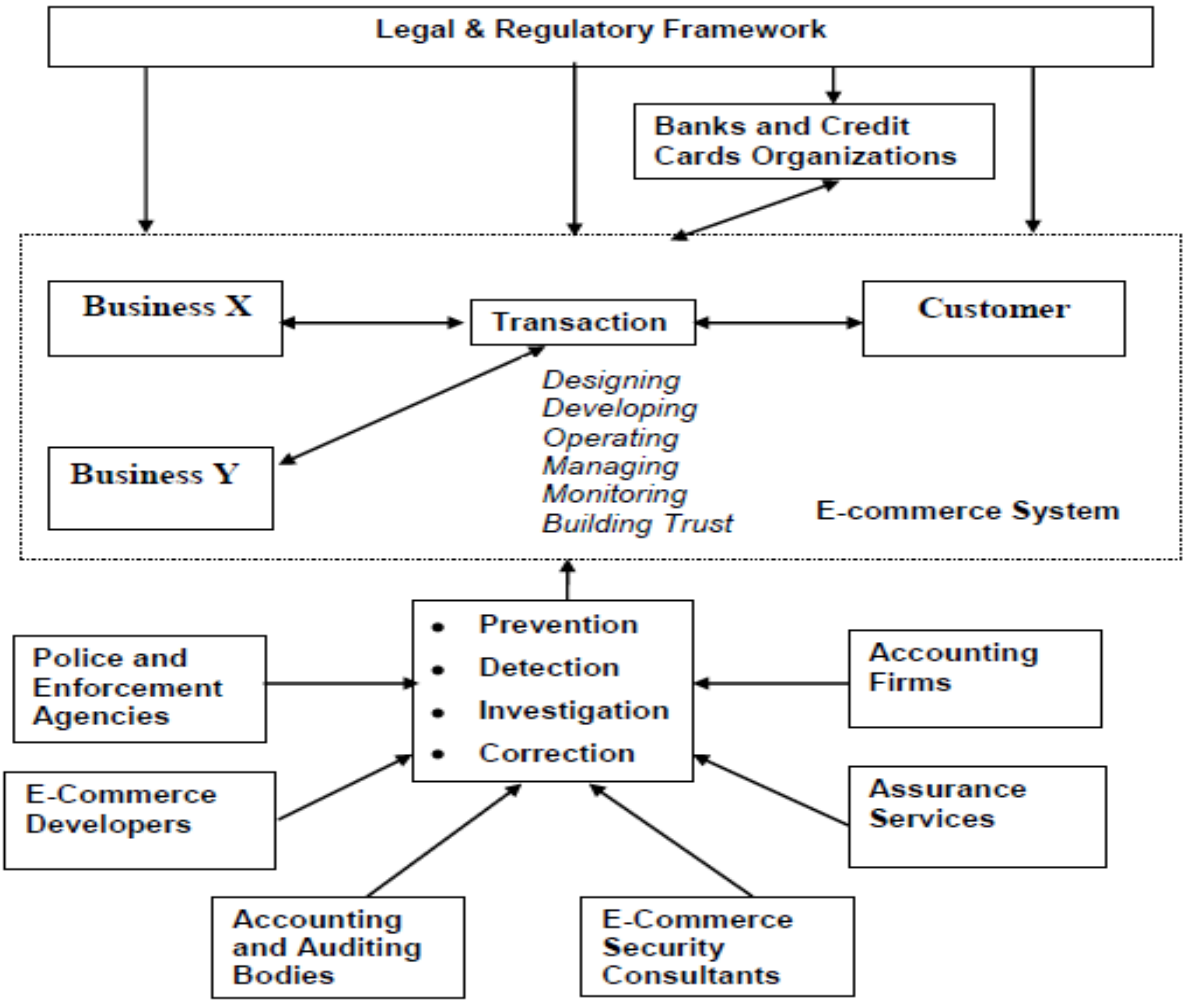


Figure 21: eCommerce Security framework (Jamieson and Cerpa, 2001).

According to the security attacks or threats defined in the X.800 and RFC 2828 documents, security attacks are classified into two: the passive attacks that only involve eavesdropping with motives of obtaining information that is being transmitted, while the other being active attacks that involve modification of the data stream or creation of false stream with motives of obtaining authorization.

3.3 Security Frameworks' Requirements

Generally, eCommerce consists of a chain of events. Several products and techniques are used to secure parts of the chain. With that fact in mind, here under are descriptions of the main categories of security needs:

(i) Authentication; is an assurance that the communicating entity is the one claimed to be.

(ii) Access Control; prevention of unauthorized personnel who misuse resources.

(iii) Data Confidentiality; protection of data from unauthorized disclosure.

(iv) Data Integrity; the assurance that received data is as sent by an authorized entity.

(v) Non-repudiation; protection against denial by one of the parties in a communication.

The majority of eCommerce transaction frameworks consist of four parties; a client, a merchant, a respective bank; and a card issuing bank (Hassler, 2001). A client, i.e. the cardholder, makes a payment using a card issued by the card issuing bank (issuer) for something bought from a merchant. The acquiring bank (acquirer) is the financial institution with which a business has a contractual arrangement for receiving (acquiring) card payments (O'Mahony *et al*., 2001). The underlying payment model is shown in Fig. 22.

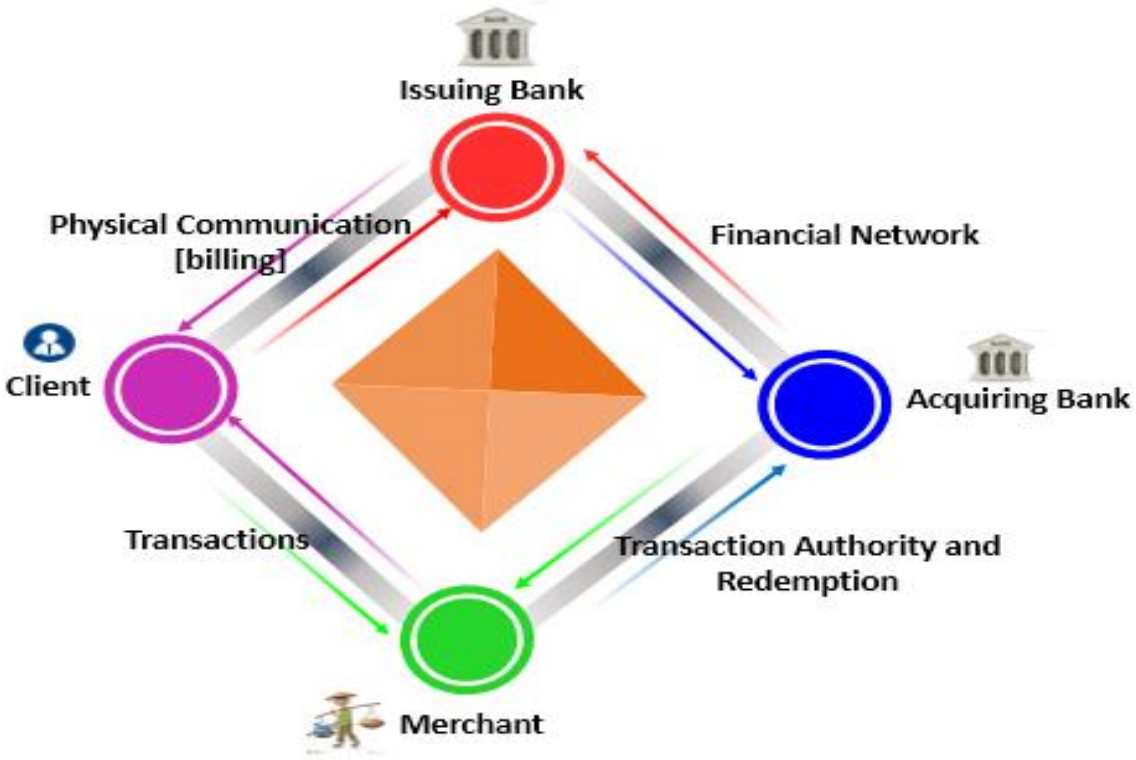


Figure 22: eCommerce payment framework

As shown in Fig. 22 shown; the security requirements for each party vary and as examined. But both acquires and issuers' requirements are combined simply because they're both financial institutions. They are both obliged to abide by the rules of the relevant payment system, and it can reasonably be assumed that they have a similar risk model.

3.3.1 Issuers and Acquires

(i) Non-repudiation: Issuers and acquirers need to ensure that neither clients nor eCommerce merchants can reject their involvement in a transaction (especially when

the transactions involve a reimbursement from merchant to client).

(ii) Authentication has two major levels: high-level and standard. A "personal identifier" (username or name) and something to be recognized (password) are the standard level. If a higher level of security than passwords is needed, users can be required to "have something" and "know something". The "have-something" part includes biometrics (e.g., fingerprints), smartcards and a private or public key infrastructure (PKI) key.

Here the Client authentication is required for the issuers and acquirers in order to prove that it is the client who authorized the payment and that we are dealing with a legitimate cardholder. Or else, a client can deny making a transaction and the issuer may end up being liable for refunding the amount to the client.

(iii) Data integrity means that data are not changed while in transit. It is important to ensure that once details of a transaction have been confirmed, no one can maliciously modify them. Merchants must not be able to alter the amount that a client has agreed to pay.

(iv) Replay protection (Privacy): A malicious merchant should not be able to use a once authorized transaction to obtain a repeat payment. Additionally, merchants should not be able to use an old transaction to request a new payment authorization no matter how many similar transactions the client has made with them. Issuers and acquirers need a mechanism to detect if a transaction has been replayed so that they do not authorize an illegitimate transaction (O'Mahony *et al*., 2001).

3.3.2 Merchants

(i) Non-repudiation: A merchant needs proof that a customer has agreed to pay the amount allied with a deal. A merchant also desires to verify that the client is the genuine cardholder; or else, the merchant can be accountable for refund. This occurs when a client tells his/her issuer that a certain transaction was not made. The card issuer then instantly submits a chargeback to the acquirer to recover the amount from the account of the merchant in question. Within a predefined period of time, the merchant can quarrel the chargeback by providing evidence of, such as, purchase or delivery. Therefore, it is important for merchants to have non-repudiable evidence of the transaction

(ii) Authentication: Merchants need client authentication to make sure that the client is

the legitimate cardholder. Moreover, they need to be sure that they are communicating with the genuine acquirer. Otherwise, an adversary may masquerade as an acquirer and authorize an illegitimate transaction.

(iii) Integrity: No one should be able to change the particulars of a transaction once they have been settled upon. A merchant will not wish to be credited with payment for less than the amount agreed. In addition, an acquirer or issuer should not be able to amend a transaction that has been authorized.

(iv) Replay protection: A malicious client should not be able to present an old proof of purchase to claim for repeat delivery of goods. Likewise, it should not be possible for an acquirer to claim that a merchant has obtained a payment using an old transaction.

3.3.3 Clients

(i) Confidentiality and privacy: Transaction confidentiality, especially card information confidentiality, may be the security service of most concern to users. It is important that a cardholder account details are kept secret from any party except the issuer, since they are the main basis on which Internet payments are made. Moreover, some users may require confidentiality protection for the nature of their transactions

(ii) Integrity: As for the other parties, transaction integrity is important to the client. No one should be able to maliciously modify the transaction details once they have been confirmed. Clients will not want an adversary to change a delivery address, the price, or the description of the merchandise after they have agreed a payment.

(iii) Authentication: A client needs to be sure that he/she is dealing with a trustworthy merchant. When shopping on the Internet, it is relatively easy to be lured into visiting a site which appears to sell something but is actually simply collecting card details. Even though a client may have made a purchase from a site before, it is not always obvious whether the page that is being fetched is authentic.

(iv) Replay protection: Clients need a mechanism to ensure that a malicious merchant or an adversary will not be able to reuse previously authorized payments to make a repeat charge.

(v) Non-repudiation: Clients also require non-repudiation. For example, a proof of payment so that no one involved in the transaction can repudiate that a payment has occurred.

Figure 23**:** Customer and Merchant perspectives on the different dimensions of eCommerce Security

3.4 Most Security Threats in eCommerce Environment

Within an eCommerce framework the key points of that are vulnerable for attack are; Client level, Server level and Communications pipeline sometime refers as Internet communication channels. In this study, Client side, Server side and communication Channels are collective referred to in this study we refer as an eCommerce environment; as shown in Fig. 23.

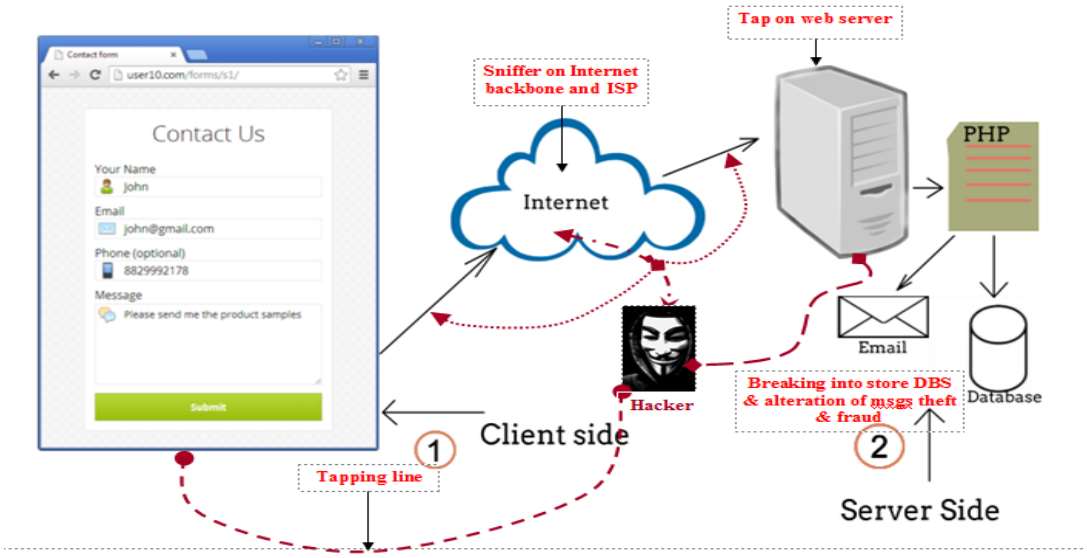


Figure 24: Vulnerable Points in an eCommerce Environment

Client-level security deals with the security from the consumer's desktop system to the eCommerce server. This part of the system consists of the customer's computer and browser

software and the communications link to the server (Maiwald, 2008). As illustrated in Fig. 24, on this part of the system, there are several security issues of concern such as;

(i) The protection of information in transit involving the customer's system and the server

(ii) The safety of information that is saved within the customer's system and

(iii) The protection of the fact that a particular customer made a particular order.

Communications security for e-commerce applications covers the security of information that is involves the client's system and the e-commerce server. This may contain sensitive information such as credit card numbers or site passwords. It may also consist of confidential information that is sent from the server to the client's system such as customer files.

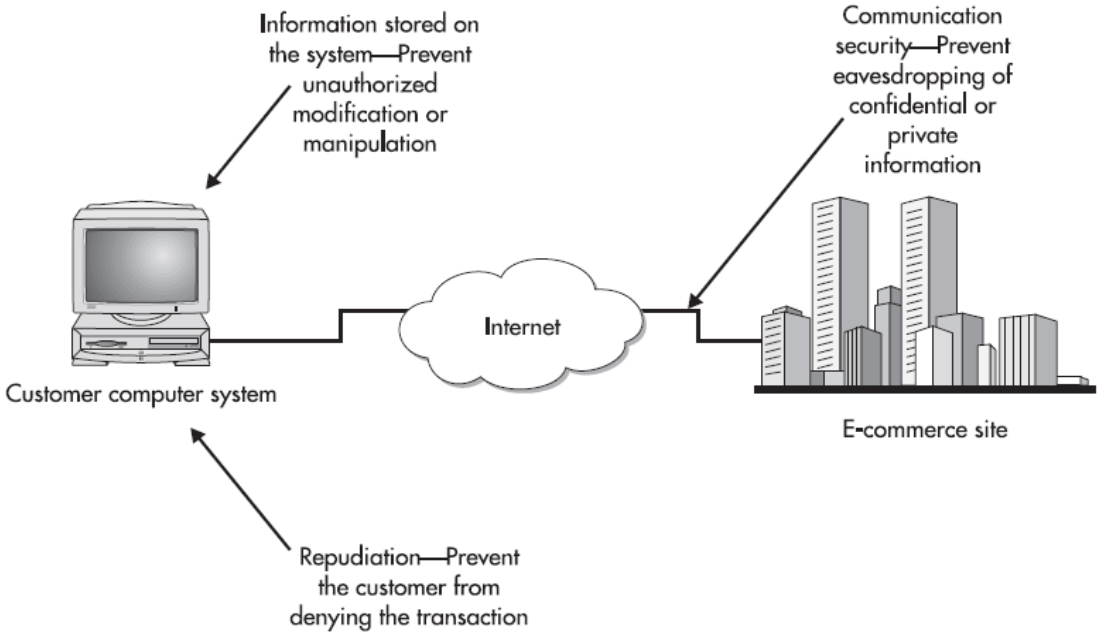


Figure 25: Client-level security components.

A Server-level security consists of the Physical eCommerce server and the Web server software running on it. The eCommerce server itself must be available from the Internet. Access to the system may be limited or open to the public. Again, on this part of the system, there are two issues related to server security:

(i) The security of information stored on the server; and

(ii) The protection of the server itself from compromise.

3.5 Other Security threats

3.5.1 Denial of service attacks

A denial-of-service (DoS) attack is an effort to make a machine or network resource unavailable to its intended users, like temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

A DoS attack is portrayed as an explicit attempt by attackers to prevent genuine users of a service from using that service. There are two common forms of DoS attacks: those that crash services and those that flood services.

The most severe attacks are distributed (Taghavi and Saman, 2013) and in many or most cases include falsifying IP sender addresses (IP address spoofing) so that the site of the attacking machines can neither easily be identified, nor can filtering be done based on the source address.

3.5.2 SQL injection attack

This is a code injection technique used to attack database-driven applications; in which malicious SQL statements are inserted into an entry field for execution.

This type of attack permits attackers to spoof identity, tamper with existing data, cause repudiation issues like voiding transactions or changing balances, permits complete disclosure of all data on the system, devastates the data or make it otherwise unavailable, including becoming an administrator of the database server.

3.5.3 Session hijacking

Session hijacking, also known as cookie hijacking is the utilization of a valid computer session to achieve unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic used to authenticate a user to a remote server. It has particular significance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer.

A mostly preferred method used is the source-routed IP packets. This allows an attacker at point X on the network to participate in a conversation between Y and Z by cheering the IP packets to pass through Y's machine.

If source-routing is turned off, the attacker can deploy a "blind" hijacking, whereby it guesses the responses of the two machines. Therefore, the attacker can send a command, but can

never see the response. Though, a common command would be to set a password allowing access from somewhere else on the net.

3.5.4 Cross-site script (XSS)

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way of knowing that the script should not be trusted and will execute the script. Since it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts sometimes can even rewrite the content of the HTML page.

While XSS can be taken advantage of within VBScript, ActiveX and Flash (although now considered legacy or even obsolete), unquestionably, the most widely abused is JavaScript – primarily because JavaScript is fundamental to most browsing experiences.

3.6 Technology Solution

3.6.1 Repudiation

One big risk allied with the client side (Client-level) of eCommerce is the possibility of a client to repudiate a transaction. Noticeably, if the client actually did not initiate the transaction, the organization should not let it happen. Nevertheless, how does the organization choose whether a client is really who he says he is? The response is through authentication.

The category of authentication that is used to confirm the identity of the client depends on the danger to the organization of making an error. In the case of a credit card purchase, there are established procedures for performing a credit card transaction when the card is not present. These include having the client supply a proper mailing address for the purchase.

If the eCommerce site is providing a service that needs a verification of individuality to access certain information, a credit card may not be suitable. It may be better for the organization to use user IDs and passwords or even two-factor authentication. In any of these cases, the terms of service that are sent to the client should detail the requirements for protecting the ID and password. If the correct ID and password are used to access customer

information, it will be assumed by the organization that a genuine customer is accessing the information. If the password is lost, forgotten, or compromised, the organization should be contacted instantly.

3.6.2 Information stored on the server

The eCommerce server is open to access from the Internet in some way. As a result, the server is at most partly-trusted (un-trusted). An un-trusted system should not store sensitive information. If the server is used to accept credit card transactions, the card numbers should be instantly removed from the system that actually processes the transactions (and that is located in a more secure part of the network). No card numbers should be kept on the server.

3.6.3 Protecting the server from attack

If information must be kept on the e-commerce server, it should be protected from unauthorized access. The way to do this on the server is employ the use of file access controls. Additionally, there are things that can be done to protect the server itself from successful penetration as follows:

(i) **Server location:** Normal server location consists of physical location and its network location. Since the server is more important to any organization thus, it should be located within a physical protected area where by physical access to the server should be protected by a locked cage and separated.

Like the server location, its network location is also important. Fig. 25 illustrates the proper location of the server within the DMZ (a DMZ or Demilitarized zone is a physical or logical sub-network that contains and exposes an organization's external-facing services to a larger and untrusted network, such as Internet). The firewall should be configured so as to only allow access to the eCommerce server on ports 80 (for HTTP) and (for HTTPS). No more services are required for the public to access the eCommerce server and therefore should be stopped at the firewall (Maiwald, 2008).

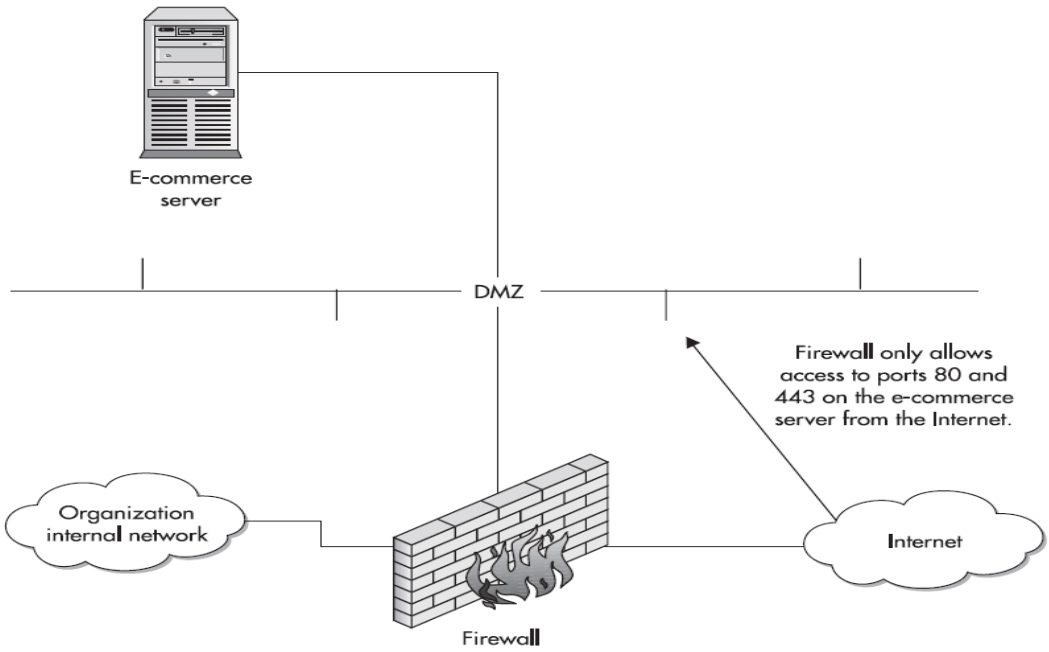


Figure 26: Location of network for the eCommerce server

(ii) Operating system configuration: Normal eCommerce server operating system is configured with security in mind. Choosing an OS depends on number of factors, such as the expertise of the administration staff of an organization. Also, factors like performance requirements and fail-over capabilities must be considered. Again, it is advisable to choose an operating system that the administration staff is familiar with.

The most important step in configuring the server securely is to eradicate or turn off all unnecessary services. The system is chiefly a Web server and, as a result, it must run a Web server (Maiwald, 2008).

The second step is to patch the system. Ensure for the latest patches for the chosen operating system and load them. When the patches are loaded, configure the system to conform to organization policy with regard to password length and change frequency, audit, and other requirements.

Lastly, sooner than the system is declared ready for production, the server should be scanned it for vulnerabilities. Vulnerability scanners can be purchased or freely available, but they must be current.

(iii) Web server configuration

The last component of the server security is the web server itself. There are specific

configuration requirements for web servers; and in general, there are some common configurations that should be made.

Initially, the server software should be upgraded and patched according to the manufacturer's recommendations.

It is a best practice to never run a Web server as root or administrator. If the Web server is successfully penetrated, the attacker will have privileges on the system as the admin of the Web server. In its place, it is advised to create a separate user who owns the Web server and run the server from that account.

Every Web server needs the administrator to define a server root directory. This directory informs the Web server where to find scripts and document files as well as limits the Web server in what files can be accessed via a browser. The Web server root is not supposed to be the same as the system root directory, and it should not comprise configuration and security files that are important to the operating system (Maiwald, 2008)

3.6.4 Protecting Internet communication

There is one reasonable solution to this: encryption. A good number of standard Web browsers contain the facility to encrypt traffic. This is the default solution if HTTPS is deployed rather than HTTP. The encryption of HTTPS will guard the information from the time it leaves the client's computer until the time it reaches the Web server. Since the public has learned of the dangers of someone gaining access to a credit card number on the Internet, HTTPS has become a preferred solution.

When HTTPS is used, a Secure Socket Layer (SSL) connection is made between the client and the server. All traffic over this connection is encrypted.

3.7 Other Protecting Techniques

3.7.1 Password policies

A password policy is a set of rules intended to enhance computer security by encouraging users to employ strong passwords and use them correctly. The policy is often part of an organization's official regulations and may be taught as part of security awareness training. Moreover, the password policy is simply advisory, or the computer systems enforce users to abide by it. Some governments have national authentication frameworks (AlFayyadh *et al*., 2013) that describe requirements for user authentication to regime services, including

requirements for passwords.

3.7.2 Digital signatures and certificates

With the development of technology, many people and organizations are using online documents instead of traditional paper-based documents for their day-to-day activities, and due to that digital signatures and digital certificates support this phenomenon by providing assurance about the validity and authenticity of a digital document.

A Digital signature is a mathematical technique used to confirm and validate the authenticity and integrity of a message, software or digital document. It is equivalent to a handwritten signature or embossed seal but offering extra inherent security. A digital signature is planned to solve the dilemma of tampering and impersonation in digital communications. Digital signatures can offer the added assurances of a proof to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer.

A digital certificate is an electronic "passport" that permits a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI). A digital certificate is sometime referred to as a public key certificate. In order to provide proof that a certificate is legitimate and valid, it is digitally signed by a root certificate belonging to a trusted certificate authority (CA). Operating systems and browsers preserve records of trusted CA root certificates so they can simply verify certificates that the CAs have issued and signed. When PKI is deployed internally, digital certificates can be self-signed.

3.7.3 Firewalls

This is a network security system that scrutinizes and manages the received and leaving network traffic based on predetermined security policy (Noureddine, 2010). A firewall typically establishes an obstacle among a trusted, secure internal network and external network, like the Internet, that is assumed not to be secure or trusted. A firewall may be categorized as either personal firewall or Web Server Firewall.

A personal firewall (sometimes called a desktop firewall) is a software program used to protect a sole Internet-connected computer from intruders. Personal firewall protection is particularly useful for users with "constantly-on" connections such as DSL or cable modem. It also controls network traffic to and from a computer, allowing or disallowing communications based on a security policy. Typically, it works as an application layer

firewall.

Web Server Firewall or Web application firewall is a security policy enforcement point positioned between a web application and the client end point. This functionality can be implemented in software or hardware, running in an appliance device, or in a typical server running a common operating system. It may be a stand-alone device or integrated into other network components (Applicure, 2010). Such web-server firewall protects, web applications the same way a traditional firewall protects a network. It controls the input and output, as well as the access to and from the asset it is protecting.

In contrast to traditional firewalls that usually block access to certain ports or filter by IP address, web application firewalls look at every demand and response within the different web service layers such as HTTP, HTTPS, SOAP, and XML-RPC. The thorough scrutiny of web traffic that web application firewalls perform has also earned them the nickname “Deep Packet Inspection Firewalls” (Applicure, 2010).

3.8 Conclusions

Due to massive development, current technology has paved the way for a secure site design. However, no company can ever claim to be 100% covered by any security measure. Security matters are extremely important for the survival of any eCommerce solution, and for that reason must be constantly analyzed and taken care of. Security problems in eCommerce frameworks are caused by many factors, hence there is need to solve these problems from different aspects, so as to offer a variety of countermeasures as elaborated here under;

Conclusively, this chapter presents a different set of security challenges facing eCommerce transactions which is used as a base of information to determines various requirements necessary for the development of a secure framework for eCommerce transactions as presenting in the chapter four. Chapter four identifies various factors that are needed during the development of the proposed framework, these include technical and non-technical factors.

CHAPTER FOUR

Requirements for Proposed Frameworks for Secure Ecommerce Transactions[3]

Abstract

This chapter proposes the best set of criteria for evaluating frameworks that support eCommerce with security requirements analysis and elicitation, based upon the construction of a context for the system and satisfaction arguments for the security of the system. The novel contribution of this chapter is an information security framework hail as the secure framework, comprising of technical, operational, business, process and maturity models to address information security requirements for eCommerce transactions.

4.1 Introduction

This part introduces the major concepts that will be referred to throughout this chapter, which are eCommerce, Framework and Security.

Electronic commerce (E-commerce, eCommerce or EC) has various definitions[4]. E-commerce can be defined as a commercial exchange system, which makes use of computers, and communication network advancements. It is the use of production information in electronic form instead of paper, for business or government operations. This suggests that e-commerce means using technological advances to promote everything involving the exchange of business information among computers and humans or traders and customers (Mlelwa and Tarimo, 2011).

For the purposes of this chapter, eCommerce is defined as the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet. These business transactions occur either as business-to-business (B-2-B), business-to-consumer (B-2-C), consumer-to-consumer (C-2-C) or consumer-to-business (C-2-B) transactions. It is practical fact that; everyone who is using eCommerce needs to be concerned about the security of personal information. But how such security can be ensured is a mountain to climb and need to be solved; hence, security is a major concern in eCommerce.

A framework can be defined as a set of beliefs, ideas, or rules that is used as the basis for making judgment and decisions (Weik, 2001) in order to provide guidance and governance of

[3] This chapter is based on the paper: Kenneth Longo Mlelwa and Zaipuna O Yonah. Requirement's for Proposed Frameworks for Secure Ecommerce Transactions. Communications on Applied Electronics 6(9):1-15, April 2017.

[4] WIPO report carries a 4-page Annex compiling 10 different definitions

business processes and operations. The IT governance frameworks have been developed to manage IT services, processes and infrastructures to enhance security services such as; access control, confidentiality, integrity, availability and accountability. In this case, IT governance is the responsibility of leaders, security managers and security professionals to ensure that the enterprises IT systems are operated under high standard of information security. Generally, each business varies in the usage of IT governance frameworks and sometimes it may become necessary to combines more frameworks to manage the IT business process (its life Cycle) and operations effectively (Fig. 26).

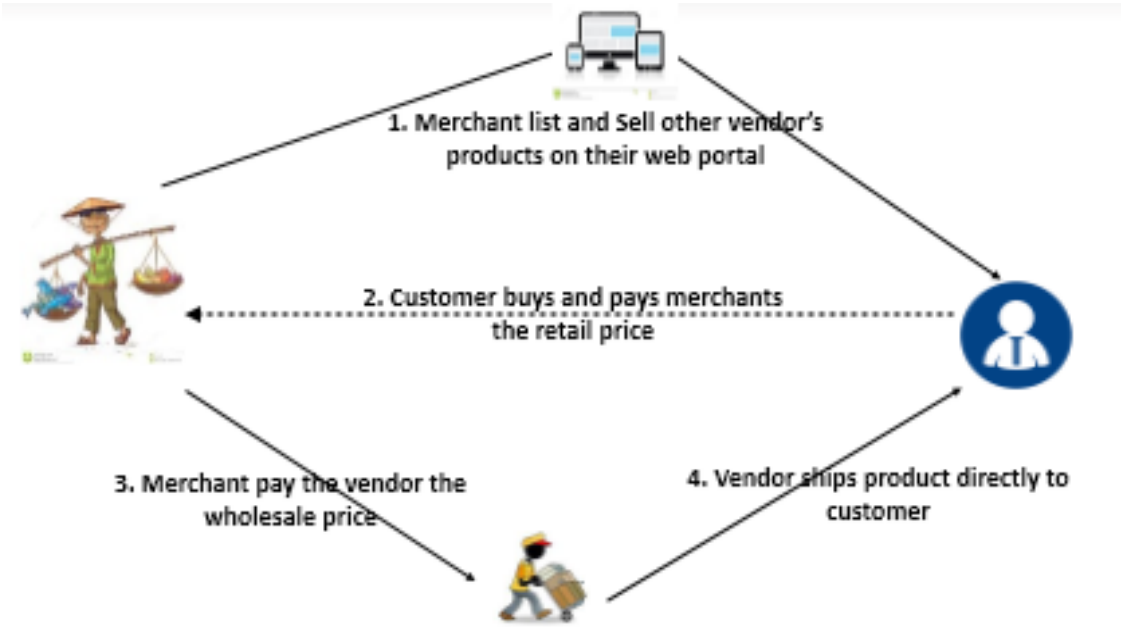


Figure 27: General E-commerce life Cycle

Security refers to the prevention of damage caused by the actions of attackers. Attackers are people who gain by utilizing system failures, intentionally or accidentally provoked. This gain usually results in some damage to the system owner. In the Computer Science and Communications Dictionary (NIST, 2006), Security in information technology has been defined as the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. Information security management is an area that has been addressed through guidelines and standards from various organizations (ISO/IEC, 2005). Technical, operational and management perspectives on information security has been presented in standards and guidelines (OECD, 2002; Talleur, 2000). These guidelines have been put into practical draw on various organizations and are chiefly based on attaining the security goals of Confidentiality, Integrity and Availability (CIA). Additionally, Accountability is now emerging as another important goal

as electronic transactions need to be traceable and parties held accountable for their actions. However, information security depends on the framework in which it is being applied, and the tackling of information security usually begins with a threat assessment and an understanding of the framework in which security is being addressed (Siponen and Willison, 2009; Hayat *et al*., 2007). This chapter particularly looks at information security frameworks for eCommerce transactions.

4.2 Framework Basics

A security framework provides a universal language for understanding, managing, and conveying security risk both within and outwardly. It can be used to help identify and prioritize measures for reducing security risks or threats, and it is a tool for aligning policy, business, and technological approaches to administering the risks. It can also be used to manage security risks across the whole organization, or it can be focused on the rescue of vital services within an organization.

Holistically a framework is a risk-based advance tool for managing information Security risks and is consists of three categories: The Framework hub (or Framework Core), the Framework Implementation Levels and the Framework Profiles. Every framework component emphasizes the relationship between business drivers and information security behavior (NIST, 2014).

Different kind of entities – such as sector harmonizing structures, associations, and organizations, can deploy the Framework for different reasons, including the creation of common Profiles.

4.2.1 Framework Hub

The Framework Hub provides a set of actions to attain specific information security outcomes, and reference examples of direction to attain those outcomes. The Hub is not a check-list of actions to perform. It presents key information security outcomes identified by industry as helpful in managing information security risk. The Hub includes four entities: Functions, Categories, Subcategories, and Informative References, as depicted in Fig. 27:

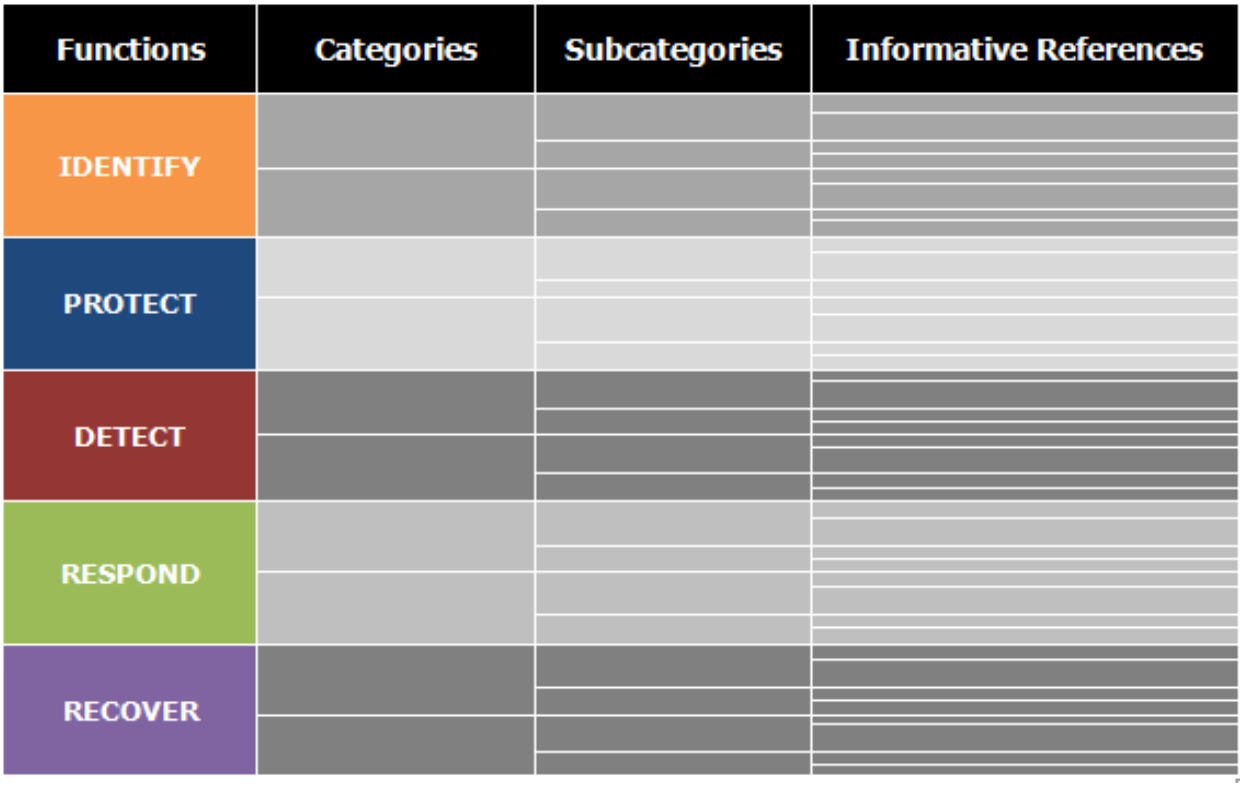


Figure 28: Framework Hub Structure (NIST, 2014)

The Framework Hub entities work mutually as follows:

(i) Function organizes fundamental information security activities at their highest stage. These are Identify, Protect, Detect, Respond, and Recover. They help a business in expressing its management of information security risk by organizing information, enabling risk management decisions, tackling threats, and improving by learning from preceding activities. It also aligns with existing methodologies for incident management and helps to show the impact of investments in information security. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.

(ii) Categories are the subsection of a Function; a set of information security outcomes closely tied to programmatic needs and particular activities. Examples of Categories consist of "Asset Management," "Access Control," and "Detection Processes."

(iii) Subcategories further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category; such as "outside information systems are catalogued," "Data-at-rest is protected;" also "Notifications from detection systems are investigated."

(iv) Informative References are specific sections of regulars, guidelines[5], and practices common among critical infrastructure sectors that demonstrate a method to achieve certain goals associated with every Subcategory. The Informative References presented in the Framework Hub are illustrative and not exhaustive. They are based upon cross-sector guidance mainly frequently referenced throughout the Framework development process.

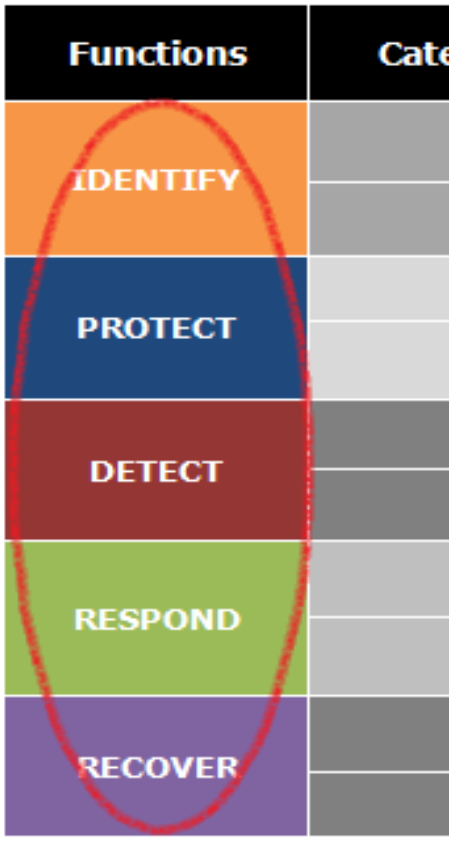


Figure 29: Five framework Hub's functions

The Five Framework Hub's Functions are defined here under and summarized in Fig. 28 (See Fig. 29 for a detailed framework Hub). These Functions are not planned to form a sequential path, or guide to a static preferred final state. Rather, the Functions can be performed in parallel and continuously to form an operational culture that addresses the dynamic information security risk.

[5] NIST developed a Compendium of informative references gathered from the Request for Information (RFI) input, Information security Framework workshops, and stakeholder engagement during the Framework development process. The Compendium includes standards, guidelines, and practices to assist with implementation. The Compendium is not intended to be an exhaustive list, but rather a starting point based on initial stakeholder input. The Compendium and other supporting material can be found at http://www.nist.gov/cyberframework/.

(i) **Identify:** this builds up the organizational understanding to manage information security risk to systems, assets, data, and capabilities. The actions in this Function are foundational for effective use of the Framework. Understanding the business background, the resources that sustain critical functions and the related information security risks permits a business to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Outcome Categories within this Function are: - Asset Management, Business Environment, Governance, Risk Assessment and Risk Management Strategy.

(ii) **Protect:** this builds up and implements the appropriate safeguards to guarantee delivery of critical infrastructure services. This Function supports the ability to contain or limit the impact of a potential information security event. Outcome Categories within this Function are: - Information Protection Processes and Procedures, Awareness and Training, Maintenance, Data Security, Access Control and Protective Technology.

(iii) **Detect:** this builds up and implements the appropriate actions to identify the occurrence of an information security event. This Function enables well-timed discovery of information security events. Such outcome Categories on this Function are: - Anomalies and Events; Detection Processes and Security Continuous Monitoring.

(iv) **Respond:** this builds up and implements the appropriate actions to react regarding a detected information security event. The Respond Function enables the ability to hold the impact of a potential Information security event. Outcome Categories on this Function are: - Communications, Improvements, Response Planning, Mitigation and Analysis

(v) **Recover**: this builds up and implements the appropriate actions to maintain tactics for resilience and to restore any capabilities or services that were impaired due to an Information security event. The Recover Function enables timely recovery to normal operations to reduce the impact from an Information security event. Outcome Categories on this Function include: Communications, Improvements and Recovery Planning

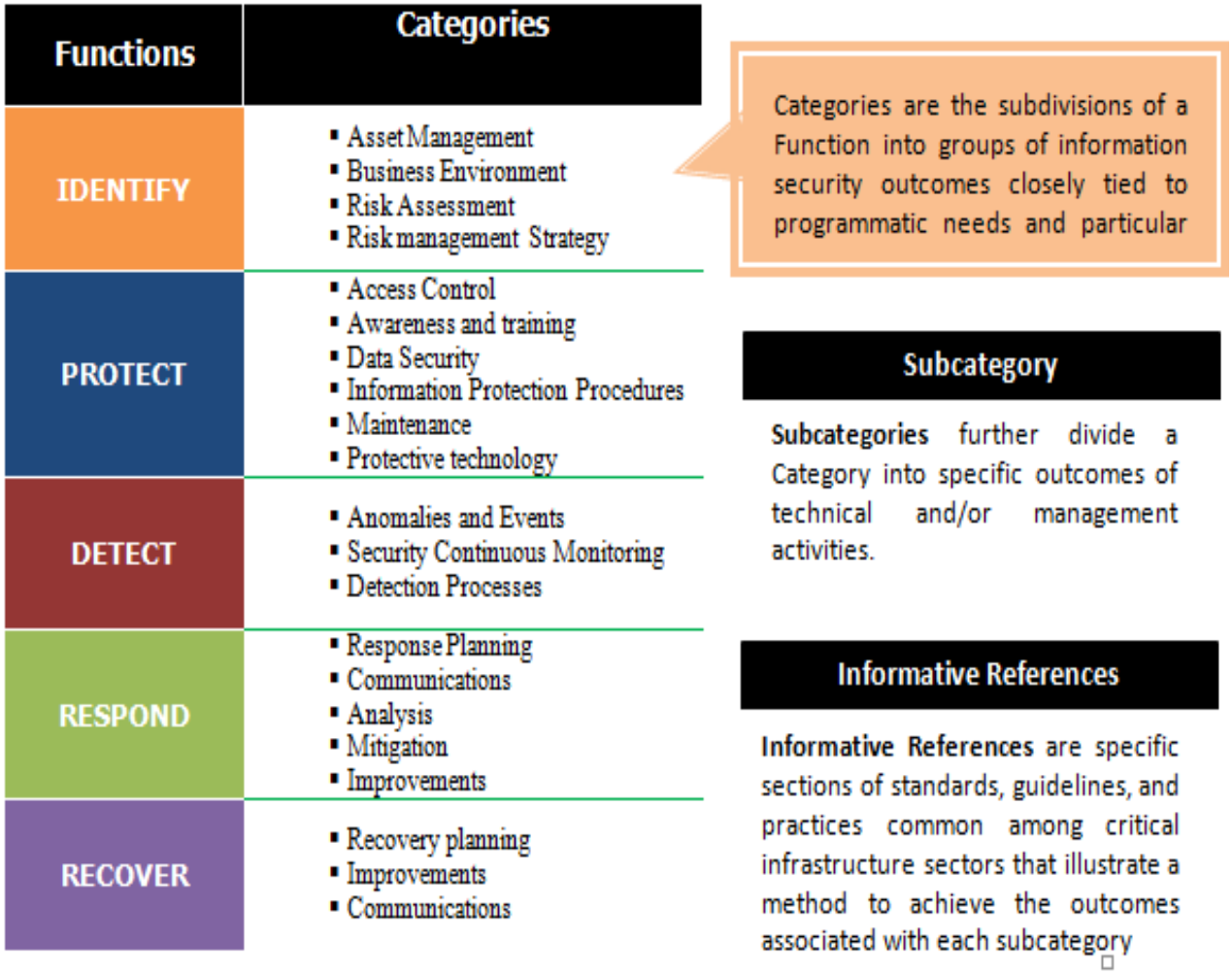


Figure 30: The Framework Hub identifies underlying key Categories and Subcategories for each Function and maps them to Informative references

4.2.2 The Framework Implementation Levels

Framework Implementation Levels show context on how a business views Information security risk and the procedures in place to manage that risk as depicted in Fig. 30. Levels describe the amount risks to which a business' Information security risk management applies to exhibit the characteristics defined in the Framework (e.g., repeatable, adaptive and risk and threat aware). The Levels characterize a business, practices over a range, from Partial (Level 1) to Adaptive (Level 4). These Levels echo a progression from informal, reactive responses to approaches that are agile and risk informed. Throughout the Level selection process, a business should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints (NIST, 2006) as a detail framework implementation levels described in Fig. 31.

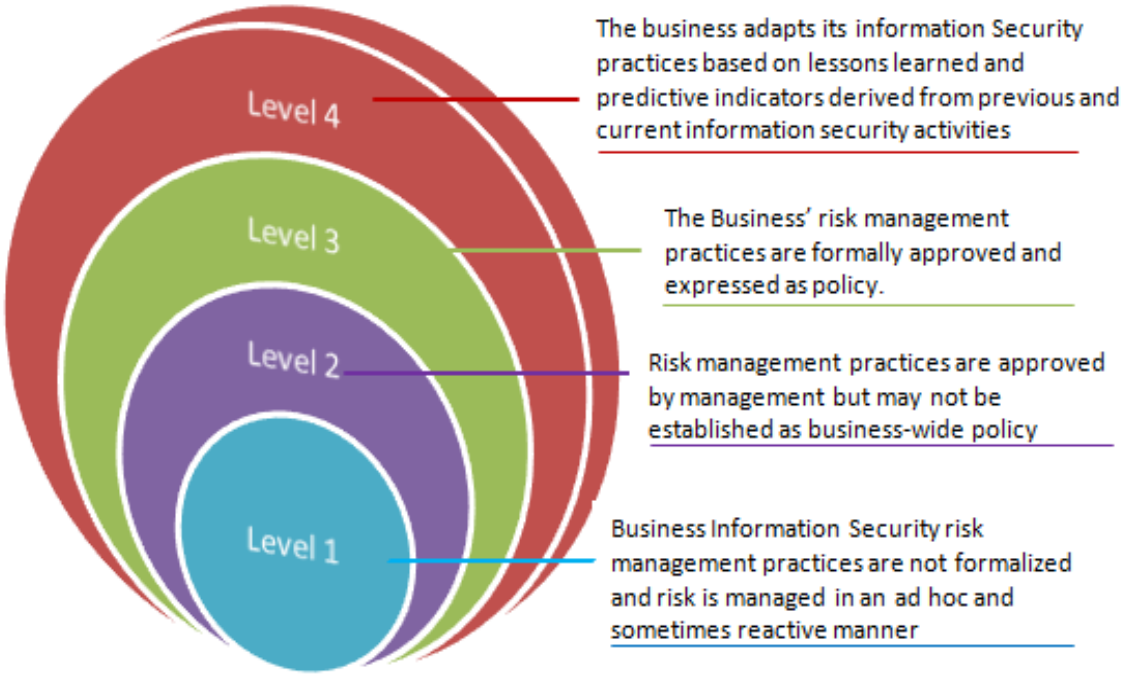


Figure 31: Framework Implantations Levels

(i) Level 1: Partial

(a) Risk Management Process: Business information security risk management practices are not formalized, and risk is managed in an ad hoc and on occasional reactive manner. Prioritization of information security behavior may not be directly informed by business risk objectives, the business/mission requirements or threat environment.

(b) Integrated Risk Management Program: There is inadequate knowledge of information security risk at the business level and the business-wide approach to managing information security risk has not been established. The business implements information security risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The business may not have processes that enable information about security to be shared within the business.

(c) External Participation: A business may not have the processes in place to support in coordination or collaboration with other entities (NIST, 2006).

(ii) Level 2: Risk Informed

(a) Risk Management Process: Risk management practices are accepted by management but may not be established as business-wide policy. Prioritization of information

security behavior is directly informed by business' risk objectives, the business/mission requirements or threat environment.

(b) Integrated Risk Management Program: There is knowledge of information security risk at the business level but business-wide approach to managing information security risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staffs have enough resources to perform their information security duties. And Information security information is shared within the business on an informal basis.

(c) External Participation: The organization knows its role in the larger ecosystem but has not formalized its capabilities to interact and share information externally.

(iii) Level 3: Repeatable

(a) Risk Management Process: The business' risk management practices are formally accepted and expressed as policy. Organizational information security practices are often updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.

(b) Integrated Risk Management Program: There is a business-wide approach to manage information security risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.

(c) External Participation: The business understands its dependencies and partners and receives information from these partners that allow collaboration and risk-based management decisions within the business in response to events.

(iv) Level 4: Adaptive

(a) Risk Management Process: The business adapts its information security practices based on lessons learned and predictive indicators resulting from previous and current information security activities. During a process of continuous improvement incorporating advanced information security technologies and practices, the business actively adapts to a changing information security landscape and responds to evolving and sophisticated threats in a timely manner.

(b) **Integrated Risk Management Program**: There is a business-wide approach to managing information security risk that uses risk-informed policies, processes, and procedures to tackle potential information security events. Information security risk management is part of the business culture and evolves from knowledge of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.

(c) **External Participation**: The business manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve information security before an information security event occurs (NIST, 2006).

	Risk Management Process	Integrated Risk Management Program	External Participation
Partial	o Not formalized o Reactive	o Limited knowledge o Irregular risk management o Private information	No external collaboration
Risk Informed	o Approved practices o Not widely use as policy	o More knowledge o Risk-informed, processes & procedures o Adequate resources o Internal sharing	Not formalized to interact & share information
Repeatable	o Approved as policy o Update regularly	o Business approach o Risk-informed, processes & procedures defined & implemented as intended and reviewed o Knowledge & skills	o Collaborate o Receive information
Adaptive	Continuous improvement	o Risk-informed, processes & procedures for potential events o Continuous knowledge o actively	Actively Shares information

Figure 32: Detailed Framework implementation Levels

4.2.3 A Framework Profile

This Framework Profile (or "Profile") is elaborated as the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization (NIST, 2014). A Profile allows a business to establish a roadmap for reducing information security risk that is well aligned with business and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may prefer to have

multiple profiles, associated with particular components and recognizing their individual needs.

Framework Profiles (Fig. 32) can be used to describe the initials/current state or the expected final/target state of specific information security activities. The Current Profile shows the information security goals that are currently being achieved. The Target Profile shows the goals needed to achieve the expected information security risk management outcomes. These Profiles support business/mission requirements and helps in the communication of risk within and between organizations.

Similarity of Profiles (that is., the Current Profile and Target Profile) may expose gaps to be addressed to meet information security risk management objectives. An action plan to address these gaps can lead to the roadmap described above.

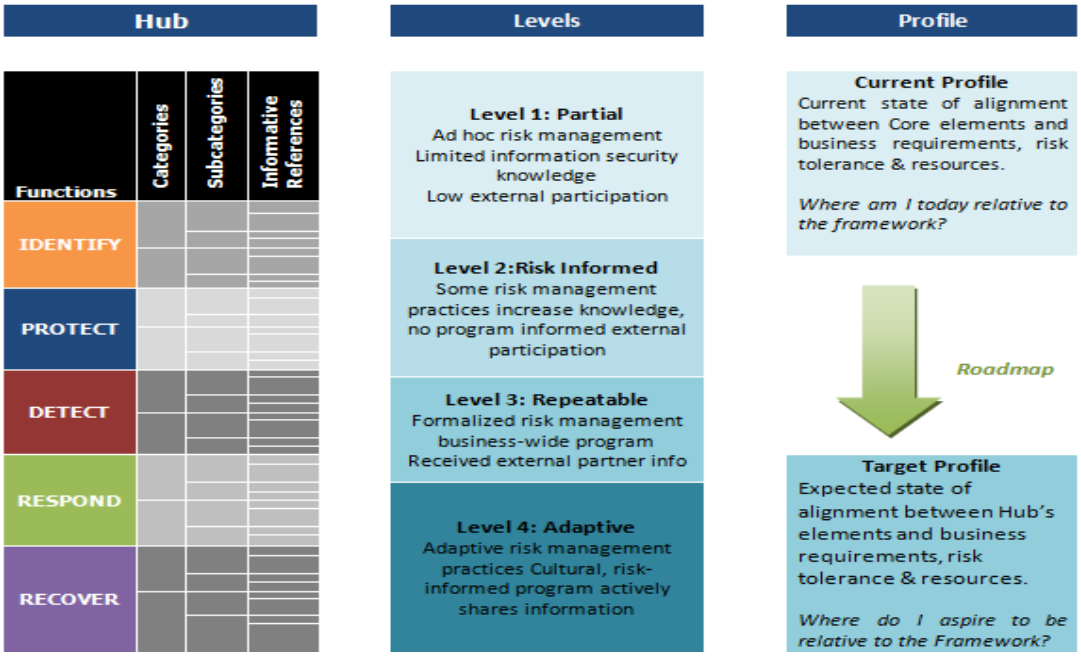


Figure 33: framework Profile

4.3 Standards related to Information Security

The term "*standard*" is at times used within the context of information security policies to differentiate between standards, procedures and written policies. Business Organizations should uphold all three levels of documentation to help secure their environment.

(i) *Information security policies* are high-level rules or statements about protecting systems or people. (For instance, a policy would state that "*Company X will maintain secure passwords*").

(ii) A "*standard*" is a low-level instruction for the various ways the company will implement the given policy. (For instance, "*Passwords will be at least 8 characters, and require at least one number*.")

(iii) A *"procedure*" can describe a step-by-step method to implementing various standards. (For instance, "*Company X will enable password length controls on all production Windows systems*.")

The use of the term "standard" differs from use of the term as it relates to information security and privacy frameworks. From above explanation a reference to the use of standards in addressing information security has been discovered. This part describes standards that are relevant to eCommerce transactions.

Open and freely available standards are referred to where possible. The exemption in standards issued by the ISO (International Organization for Standardization) since this is the de-facto standards body recognized worldwide.

The thorough investigation into use of standards is motivated by the need to develop a novel framework in eCommerce transactions, which need not “re-invent the wheel”, but rather concentrate on those specific mechanisms that will address context sensitive needs. It also addresses some of the barriers to eCommerce including information exchange, resource constraints and technical platforms.

The following section, discuses some of the standards and their relationship to information security for eCommerce transactions.

4.3.1 Non-technical Standards

(i) ISO/IEC 27001 –Information security management: The ISO/IEC 27000 family of standards helps organizations keep information assets secure (ISO/IEC, 2005). They help organizations manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

ISO/IEC 27001 is a well-known standard in the family providing requirements for an *Information Security Management System* (ISMS). An **ISMS** is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. The significance of this standard to eCommerce transactions is that individual Business-organizations involved in an eCommerce transaction should have mechanisms or internal processes to address information security.

(ii) **NIST SP 800 Series:** The U.S. National Institute of Standards and Technology has been building an extensive collection of information security standards and best practices documentation. The NIST Special Publication 800 series was first published in 1990 and has grown to provide guidance on just about each and every aspect of information security. Even though it is not specifically an information security framework, NIST SP 800-53 is a model that other frameworks have evolved from. U.S. government agencies utilize NIST SP 800-53 to comply with the Federal Information Processing Standard's (FIPS) 200 requirements. Even though it is specific to government agencies, the NIST framework could be applied in any other industry and should not be overlooked by companies looking to build an information security program.

(iii) **FIPS PUB 200:** This is the Minimum-Security Requirements for Federal Information and Information Systems (CEN, 2007). This standard can be obtained by downloading free from www.csrc.nist.gov. The standard specifies 17 security areas for **which** federal organizations are required to develop and adopt policies. Some of these that narrate to this chapter are (OASIS, 2010): Access Control, Identification and Authentication, Maintenance, Physical and environmental protection, Systems and Information Integrity, System and Communication protection. This standard address some of the information security requirements presented in this dissertation.

(iv) **Network and Information Security Standards Report, Issue 6.2:** The report identifies the increasing importance of the reliability, availability and security of networks and information systems to the economies in Europe as well as proposes standards to address current security threats. This Report (OASIS, 2010) can be downloaded for free from http://www.cen.eu.

This report is designed to be used by Business-organizations with a curiosity in information security standards and guidelines. These business-organizations may represent stakeholders, small and medium sized enterprises (SMEs) or large organizations, may be governments or may be public interest bodies.

(v) **OECD 81829 2002:** this standard is named Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (OECD, 2002). This standard is available for free from www.oecd.org.

It is outlines nine principles intended to instill a culture of security in organizations. It

also identifies the need for the incorporation of security as an essential element of information systems and networks. These nine principles are (OECD, 2002),

(a) Awareness of the need for information security;

(b) Response to security incidences;

(c) Responsibility for the security of information systems;

(d) Democracy, that is, security of information systems and networks should be compatible with the essential values of a democratic society;

(e) Ethics, that is, respect for the legitimate interest of others; Risk assessment; security design and implementation;

(f) Security management and finally, Reassessment of information security management systems.

4.3.2 Technical Standards

Subsection 4.3.1 presented the standards and guidelines that mostly address the information security management process. For addressing the technical aspects of information security, a survey of existing technical information security standards is presented in this subsection. These surveyed standards are those related to the technical components/mechanisms that can be utilized to implement eCommerce transactions.

(i) EXtensible Access Control Markup Language (**XACML)**; is a policy language that uses XML statements to present access control policies. XACML version 2.0 was ratified as a standard by OASIS in February 2005 (ISO/IT, 2009).

As a published standard specification, one of the goals of XACML is to promote common terminology and interoperability between access control implementations by multiple vendors. XACML is primarily an Attribute-Based Access Control system (ABAC), where attributes (bits of data) associated with a user or action or resource are inputs into the decision of whether a given user may access a given resource in a particular way (see Table 2). Role-based access control (RBAC) can also be implemented in XACML as a specialization of ABAC summarized in Fig. 33.

Table 1: XACML Components

XACML Components	Description
Policy Enforcement Point (PEP)	Point at which access authorization policies are managed
Policy Decision Point (PDP)	Point at which access requests against authorization policies are evaluated before issuing access decisions
Policy Retrieval Point	Point where the XACML access authorization policies are stored, typically a database or the file-system.
Policy Information Policy	The system entity that acts as a source of attribute values (i.e. a resource, subject, environment)
Policy Administration Point	Point at which access authorization policies are managed

EXtensible Access Control Markup Language (XACML) Steps;

(a) A user sends a request which is intercepted by the PEP

(b) The PEP converts the request into a XACML authorization request

(c) The PEP forwards the authorization request to the Policy Decision Point (PDP)

(d) The PDP evaluates the authorization request against the policies it is configured with. If needed it also retrieves attribute values from underlying Policy Information Points.

(e) The PDP reaches a decision (Permit / Deny / Not Applicable / Indeterminate) and returns it to the PEP

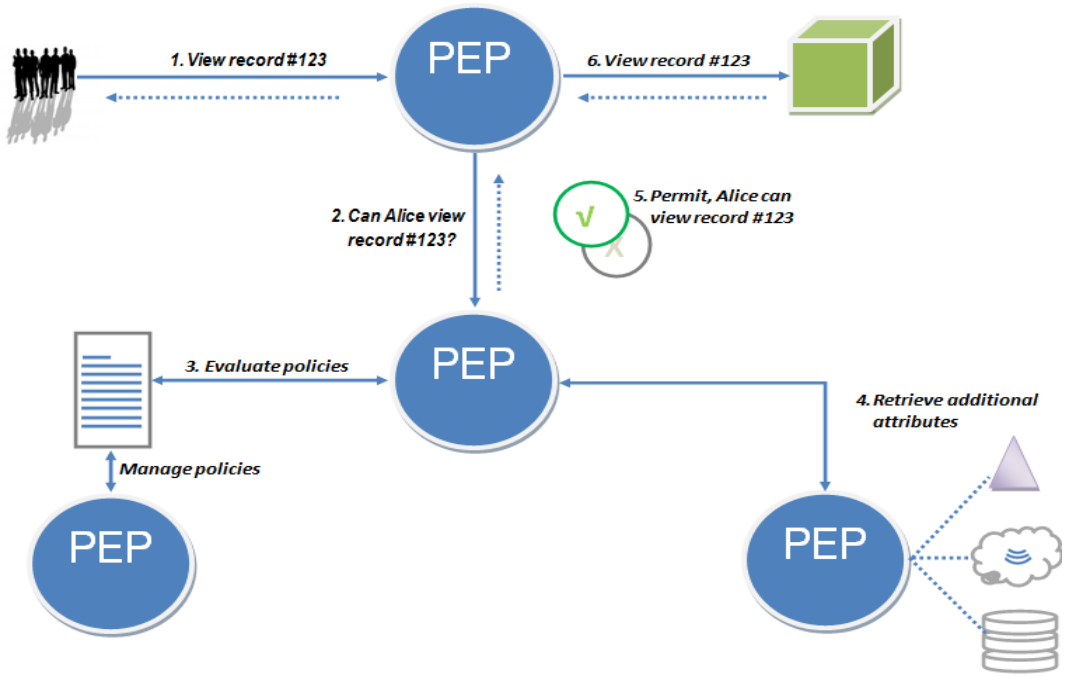


Figure 34: XACML architecture and a sample authorization flow

In the following paragraph, an access control model, based on XACML and using SAML attributes is developed and presented as part of the information security framework for eCommerce transactions.

(ii) Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authorization and authentication data among parties, in particular, between a service provider and an identity provider. Security Assertion Markup Language is a product of the OASIS Security Services Technical Committee (ISO/IT, 2009).

Security Assertion Markup Language assertions are of three categories that are, Authentication assertions, Attribute assertions and Authorization Decision assertions. An assertion is defined as a piece of data regarding either an act of authentication performed on a subject, attribute information about the subject, or authorization data applying to the subject with respect to a specified resource. Assertions are created by a SAML authority, which is a conceptual system entity in the SAML domain model. The web service or user requesting assertions from the SAML authority is called the Requester. These assertions are then utilized in communicating with an entity called a Responder, who utilizes those SAML assertions to respond appropriately to the Requester. In a web services environment, SAML assertions may be carried within a SOAP message. Other than assertions, SAML also consists of protocols, bindings and profiles. Protocols allow service providers to request for assertions, authentication and name identifier registration and mapping. Bindings are the mappings from SAML request-response message exchanges into standard messaging or communication protocols such as SOAP and HTTP. A profile of SAML defines constraints and/or extensions in support of the usage of SAML for a particular application.

The main SAML use case is called Web Browser Single Sign-On (SSO). A user wielding a user agent (normally a web browser) requests a web resource protected by a SAML service provider. The service provider, wishing to know the identity of the requesting user, issues and authentication request to a SAML identity provider through the user agent. The resulting protocol flow is depicted in Fig. 34.

(iii) Web Services (WS) Security Framework: The goal of the WS Security Framework is to have a standard way of managing web services security in transactions derived from entities that might have different security policies/environments. This

framework has been adopted by OASIS as a standard (ISO/IT, 2009) Table 3 summarizes the security standards for Web Services.

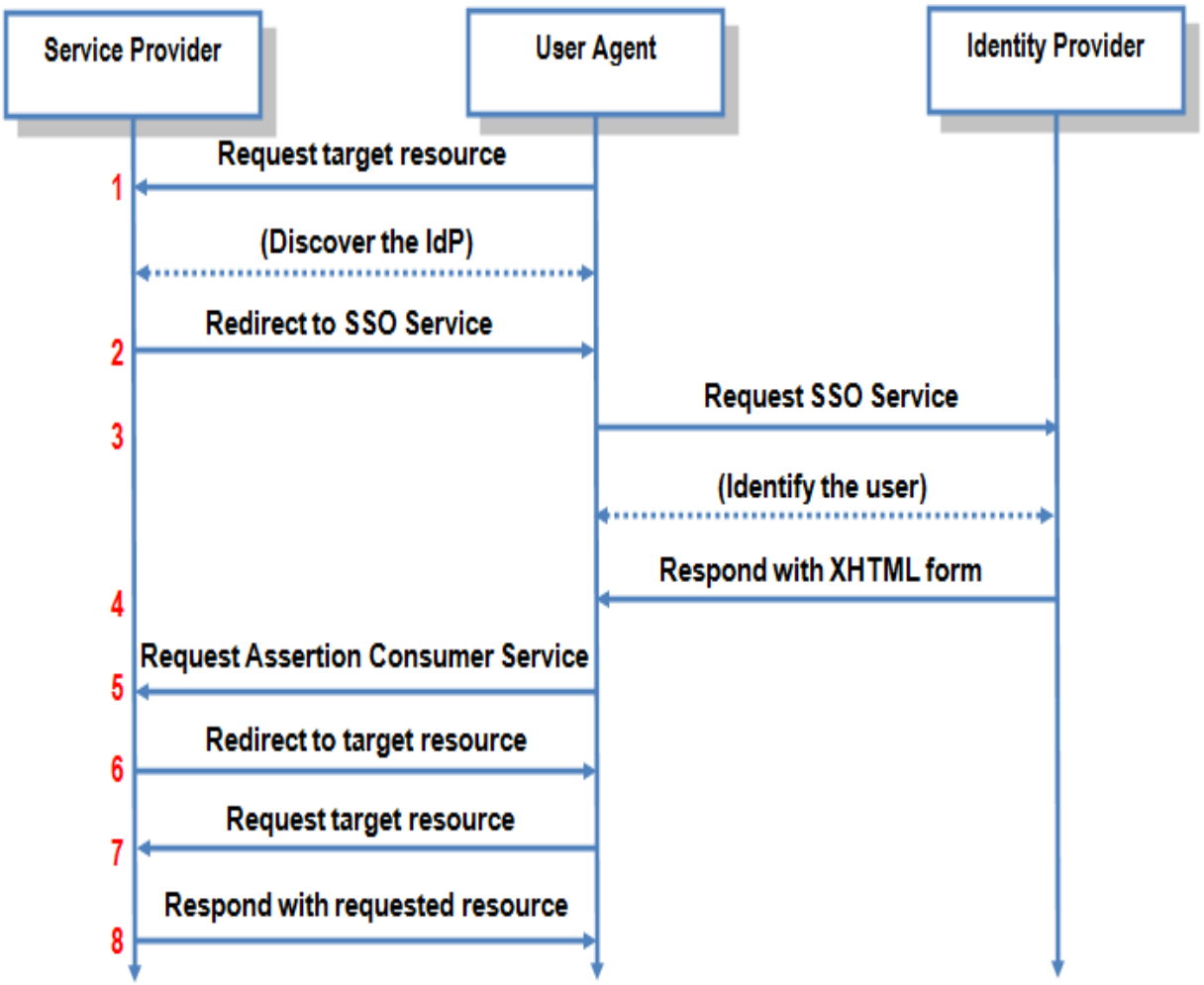


Figure 35: using SAML in a Web browser

Web Service Security Requirements:

The following outlines the Web service security requirements:

(i) Use transport security to protect the communication channel between the Web service consumer and Web service provider.

(ii) Use message-level security to ensure confidentiality by digitally encrypting message parts; integrity using digital signatures; and authentication by requiring username, X.509, or SAML tokens.

Web Services Security framework, is designed to implement and define Web services security in heterogeneous environments, including authentication, authorization, message decryption and encryption, signature generation and validation, and identity propagation across multiple Web services used to complete a single transaction.

Table 2: WS Security Framework Components

WS Security Framework component	Description
SOAP Message Security	Portrayed enhancements to SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies.
Username Token	This describes how a web service consumer can provide a Username Token as a way of identifying the requestor by "username", and optionally using a password to authenticate that identity to the web service producer.
WS-Policy	A Web service provider may define conditions (or policies) under which a service is to be provided. The WS-Policy framework enables one to specify policy information that can be processed by web services applications, such as Oracle WSM.
Kerberos Token	This is a cross-platform authentication and single sign-on system. The Kerberos protocol provides mutual authentication between two entities relying on a shared secret (symmetric keys).
SAML Token	Describes how to use SAML assertions with the WS Security SOAP message specification.
X.509 Certificate	This is a signed data structure designed to send a public key to a receiving party. A certificate includes standard fields such as certificate ID, issuer's Distinguished Name (DN), validity period, owner's DN, owner's public key, to name a few.

The standards and guidelines presented in the foregoing paragraphing tackle security requirements that are applicable in many settings. Recognizing that a successful implementation should take context into consideration, standards organizations have started moving towards investigating context specific standards and guidelines.

4.4 Framework Requirements for Proposed Secure Ecommerce Transactions

The main difficulty with elaborating a framework is that many steps or outputs are unspecified or abstract. To conquer this difficulty, in this study, the framework is instantiated using a combination of Goal-Oriented Requirements Engineering (CEN, 2007) and Problem Frames (OASIS, 2010), describing it in terms of a set of activities.

4.4.1 Security Goals

Security goals are resultant of the business goals of the system (ISO/IT, 2009). A few numbers of actors, operations, and objects will be needed to satisfy the business goals. To rephrase, security goals occur when stakeholders find that they wish to avoid *damage* to some objects in the perspective of the system, be they tangible (e.g., cash) or intangible (e.g., information), that have direct or indirect significance. Objects signified in either way are called *assets*, and the stakeholders normally wish to protect themselves from any damage that might come from abusing these assets.

Security requirements for any system depend on its functions, the types of data it processes, the other systems (if any) with which it communicates, and the environment in which it operates (Dardenne *et al*., 1993).

Damage could not be to the asset itself (direct damage), but instead could be a result of some misuse or abuse of the asset (indirect damage). Examples of indirect damage include damage to reputation due to exposure of flawed hiring policies, loss of contracts results of exposure of pricing or costing details, or loss of trade secrets during the theft of some newly designed widgets. In other words, one is not necessarily protecting assets from damage, but is instead protecting against damage caused by abuse of assets.

The security community has itemized some common security concerns, cataloging them with the letters C, I, A, and more recently a second A (C,I,A,A) (Jackson, 2001) as depicted in Fig. 35:

(i) Confidentiality: ensures that an asset is visible only to actors authorized to see it.

(ii) Integrity: ensures that the asset is not corrupted.

(iii) Availability: ensures that the asset is readily accessible to agents that need it, when they need it.

(iv) Authentication: ensures that the identity of the asset or actor is known. A common example is the simple login.

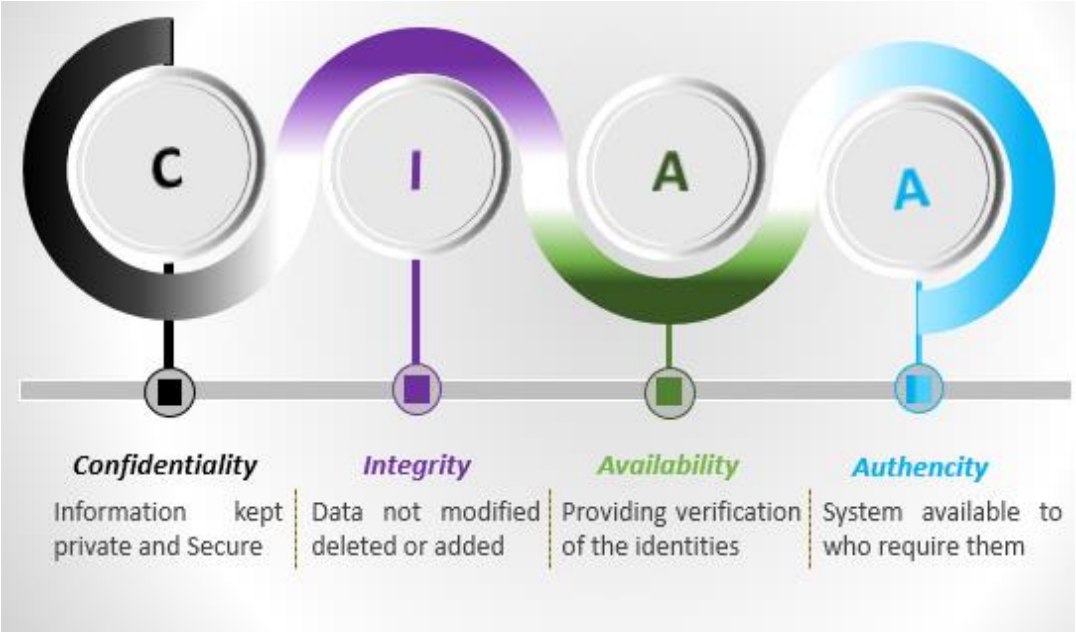


Figure 36: Common Security goals.

Another set of security goals can be originated by combining *Actors*, *management/Operational* control principles and *application/technical* business goals (Fig. 36). Actors here are those who participate during business transactions. These include *Merchants* and *Clients.* Again, Management control principles consist of common security principles; for instance, least privilege and separation of duties (Allen, 2001). Application/technical business goals will determine the applicability of management control principles to the system, such as by defining those privileges that are needed for the application and excluding those that are not.

Figure 37: Other Security Concern

4.4.2 Security requirements

Security requirements can be defined as constraints on the functions of the system, where these constraints functionalize one or more security goals as follows:

(i) They are limitations on the system's functional requirements, rather than themselves being functional requirements.

(ii) They express the system's security goals in functional terms, precise enough to be given to a designer/architect.

The truth is, security requirements are constraints on functional requirements rather than different functional requirements which are vital for validation of the functional requirements. Validating a set of functional requirements in the face of constraints is trouble-free than validating requirements comprising of the original functional requirements and the additional functional requirements appended for security. In the first case, one requires checking only that before the functions are constrained; they still do what they originally were intended to do. In the second case, the system designer decides how the requirements interact and how the interactions are realized. Only after design is complete, one should check to see if functionality has changed beyond acceptability.

4.4.3 Towards a secure framework

The proposed Framework is a process designed to evolve with changes in information security threats, processes, and technologies. This framework visualizes effective security as a dynamic, continuous circle of reaction to all threats and solutions. Thus, businesses that implement this Framework will be better positioned to comply with future security and privacy regulations. At the least, businesses that operate in regulated industries should begin screening how regulators, examiners, and other sector-specific entities are changing their review processes in response to the security Framework.

Based on the foregoing explanation there are some parameters and steps that need to be considered on designing a secure ecommerce transaction. The framework is a unified framework that consists of five models, which are based on the perspectives related to Security goals. These are:

(i) **Technical Model**: The technical model presents technical mechanisms that work together to address the information security requirements for eCommerce transactions.

(ii) **Operational Model:** The operational model presents operational mechanisms that need to be implemented during eCommerce transactions to address information security requirements. The Operational Model makes no assumptions about the technical capabilities of actors, or even that the transactions that are taking place in the eCommerce transactions are entirely electronic transactions.

(iii) **Business Model:** this model presents governance mechanisms that need to be implemented at a policy level within an organization. These include organizational policies, national and regional legislation.

(iv) **Process model**: The process model presents the way that the secure framework can be implemented within an organization and amongst businesses that plan to undertake eCommerce transactions. This process model captures the context whereby resources to carry out whole security implementations at one go may not be available and where there may be lack of coordination across businesses with regards to eCommerce implementations.

(v) **Maturity model:** The maturity model provides a mechanism for businesses to continually measure progress with regards to meeting information security requirements for eCommerce transactions.

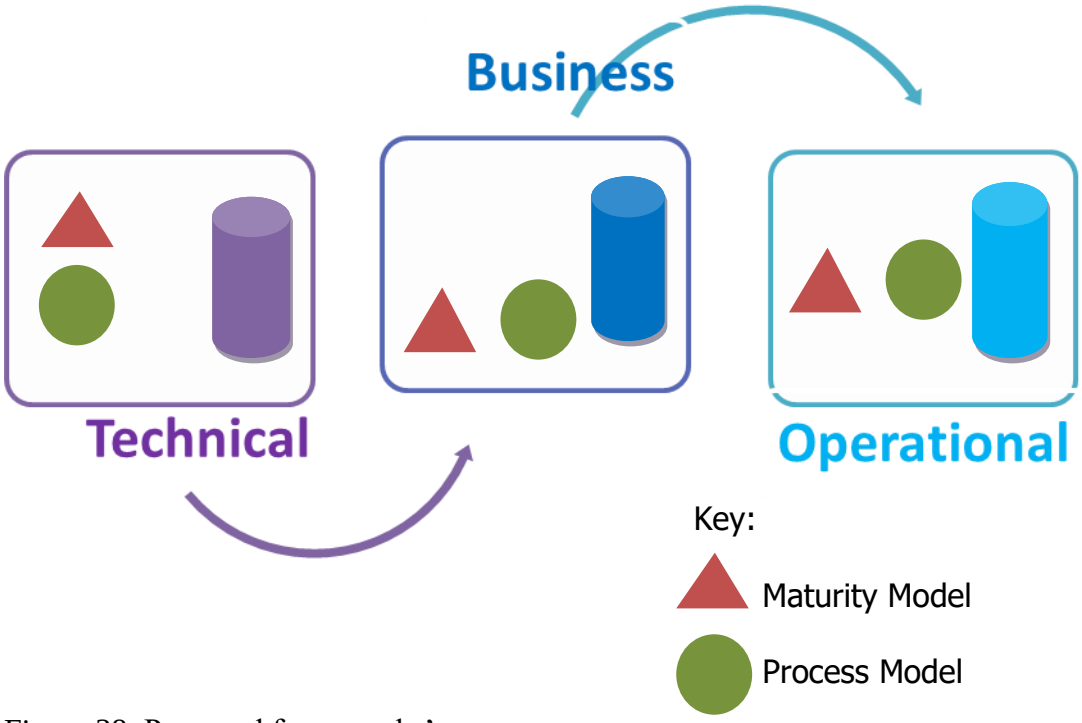


Figure 38: Proposed frameworks' parameters.

Figure 37 depicts the five parameters. Three of them, the technical, business and operational models, appear as pillars and the remaining two models, which are the process and maturity models, are found inside of those pillars. This means that in every model, the technical, operational and business pillars can be applied independently to meet information security requirements for eCommerce transactions, as and when resources are accessible. The process and maturity models help the business to continually move towards a holistic information security framework, by inserting mechanisms in the technical, operational and business models onto each other.

The players in an eCommerce transaction are individual persons and business organization who must comply with national and regional legislation set by Governments and with organizational policies that are set by the businesses. The functions of each of the major players determine who implements the models of the Framework as shown in Table 4.

Table 3: Secure Framework implementation by main Players in a Secure eCommerce Transaction.

Player	Function	Secure model Implemented
Business	Launch legislation and policies that tackle the information security objectives and requirements; approve or accept standards that address the information security requirements.	Business / Organization
Business-Executive	Launch policies within the organization to tackle the information security requirements	
Business-Operational	Set in place operational plans and mechanisms to tackle the information security requirements	Operational
Business-Technical	Apply technical mechanisms to meet information security requirements	Technical

The process model presents steps to implement the business, operational and technical models, while the maturity model allows merchants and businesses to track how their information security practices are growing to fully meet the information security objectives.

These models are independent and can be developed in parallel. The common aspect is that all the models are implemented with similar security objectives and requirements in mind. It serves as the mapping mechanism from one model to another, and the maturity model

provides guidance to ensure that businesses are continually improving towards a holistic information security framework.

The details of every model are presented here under:

(i) Secure technical model

The technical model of a secure framework summarizes technical components that can be used to meet the information security requirements.

Any confirmed solution that can tackle the security requirements can be integrated in the technical model. Currently, four components that can tackle the security objectives are described in more details. These can be deployed by technical team or in collaboration with operational teams. These four components are Attribute Based Access Control; eCommerce Ontologies, SOA and third-Party Trustee.

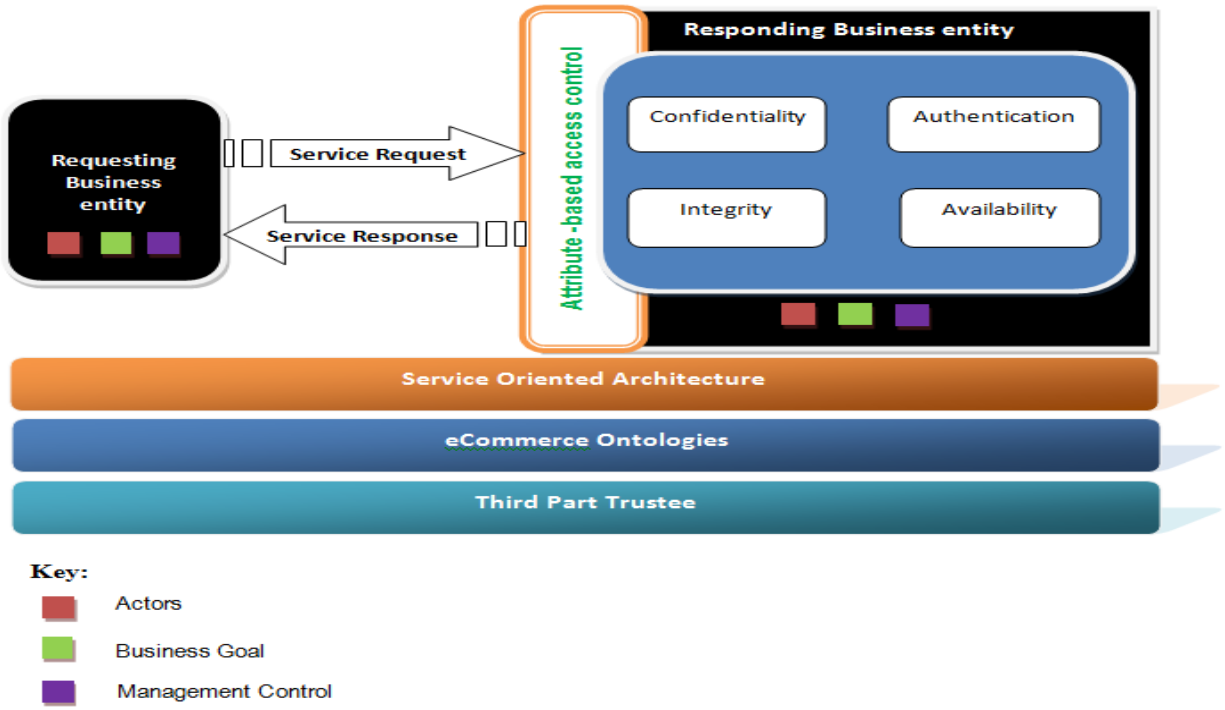


Figure 39: Secure Technical model

The base of Fig. 38 shows the components to be used to meet the eCommerce Information Security: requirements. ABAC is a novel mechanism proposed in this chapter as being particularly suited to eCommerce transactions. The security model components are described in detail in the following paragraph, jointly with implementation guidelines for the technical departments of businesses.

Attribute-based access control (ABAC): defines an access control paradigm whereby access rights are granted to users through the use of policies which combine attributes

together. The policies can use any type of attributes (user attributes, resource attributes, object, environment attributes etc.). This model supports Boolean logic, in which rules contain "IF, THEN" statements about who is making the request, the resource, and the action. For example: IF the requestor is a manager, THEN allow read/write access to sensitive data (Landwehr and Carroll, 1984).

The rationale of the ABAC is that it is a robust access control mechanism that tackles the authorization, access control and privacy security requirements in eCommerce transactions. This mechanism is based on open standards i.e. SAML6 and XACML7 and takes into consideration prevailing legislation. SAML assertions are used for authentication while XACML is used to formulate policies and to provide a rule combining algorithm and delegation in policy decisions.

This is helpful in eCommerce transactions in cases where a service may involve information that crosses legislative domains. One organization can delegate part of the authorization decisions based on the law and policies in the participating organizations. SAML may be used jointly with XACML Authentication, Authorization Decision and Attribute assertions being issued by the Certificate Authority which is part of the operational guidelines.

E-commerce Ontologies: The use of standards such as XACML and SAML as integrated in the ABAC model tackles syntactic interoperability. Ontologies are a helpful tool for attaining semantic interoperability. Ontology is a formal representation of concepts in a domain. The developed ontologies can be deployed to ensure accurate access control decisions in eCommerce transactions. The ontologies will be based on the familiar terminology in the operational model.

The reason of having eCommerce ontology in the secure technical model is to allow the definition of attributes that will be deployed in access control and authorization decisions. In an eCommerce transaction, where there may be no human involvement, an incorrect authorization may be made since an assertion originating from the requesting machine may be interpreted in other way round from the consumer's policies. By using a familiar ontology, semantic interoperability is achieved.

6 Security Assertion Markup Language (SAML, pronounced sam-el) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee.

7 XACML stands for "eXtensible Access Control Markup Language". The standard defines a declarative fine-grained, attribute-based access control policy language, architecture, and a processing model describing how to evaluate access requests according to the rules defined in policies.

Service Oriented Architecture (SOA): A SOA is defined by World Wide Web Consortium (W3C) as a set of components that can be invoked, and whose interface descriptions can be published and discovered. W3C also defines a Web Service as a software system designed to support interoperable machine-to-machine interaction over a network (Pfleeger and Pfleeger, 2002). It has an interface expressed in a format that machines can process. Other systems act together with the Web service in a way prescribed by its description using SOAP messages, typically conveyed using HTTP with XML serialization in conjunction with other Web-related standards. Web Services are used to implement service-oriented architectures.

In an eCommerce transaction, exchanges are typically machine to machine interaction. The reason of a SOA in the Secure Technical Model is to attain the availability security goal, when implemented with web services. Given the fact that web services are technically neutral, a web service produced by a business can be utilized by another business organization regardless of differences in technical platforms in the two businesses.

Third Party Trustee: Third Party Trustee (TPT) contains components that permit parties to communicate securely over public networks with the use of public key cryptography. A certificate authority provides/issues and verifies certificates that are given to the parties during a transaction. For eCommerce transactions, a TPT could be agreed upon to act as a certificate authority for businesses organizations.

The use of PKI in the Secure Technical Model would permit organizations to use the internet as a means of communications, as a result avoiding expensive point to point secure links between businesses

For a sustainable implementation (Table 5), Business organizations can keep the latest advances in access control standards or research that would be useful for eCommerce transactions. The list is not complete but provides a direction and a starting point for those standards and mechanisms are referred to in this model.

Table 4: Supportive Resource for implementing the Secure Technical Model.

Source	Resource	Reason
http://webstore.iec.ch/preview/info_isoiec14516%7Bed1.0%7Den.pdf	ISO/IEC TR14516	Source of information on updates to IT security mechanisms and techniques from ISO and IEC
www.w3c.org	World Wide Web Consortium.	Source of updates on standards associated to web services and web service security
www.protege.stanford.edu	Protégé Ontology development tool from Carnegie Mellon University	Free tool for development of ontologies
www.oasis.org	Organization for the Advancement of Structured Information Standards – OASIS	Source of information on updates to the XACML and SAML standards that form part of the ABAC.

(ii) The business models

This Business model of the proposed framework summarizes policy level mechanisms for tackling the information security requirements for eCommerce transactions. And this has been motivated by the following factors:

(a) An eCommerce transaction typically takes place across more than one organization. Therefore, multiple organizational and security domains may be involved. That is, handling of security must be at a level higher than just an individual organizational level.

(b) The framework must take into consideration the existing legislation, and meanwhile be flexible enough to anticipate new laws or changes to existing legislation.

(c) In many areas, implementation of international frameworks without adaptation has proved not to work, as developing countries need context-sensitive approaches (NIST, 1995).

The components of the business model include of Organizational policies, Regional and National laws and regulations as well as International standards. Every component will have elements that apply to some or all of the information security requirements. The Business model is implemented by top level management in an organization. As illustrated in Fig. 39 Below

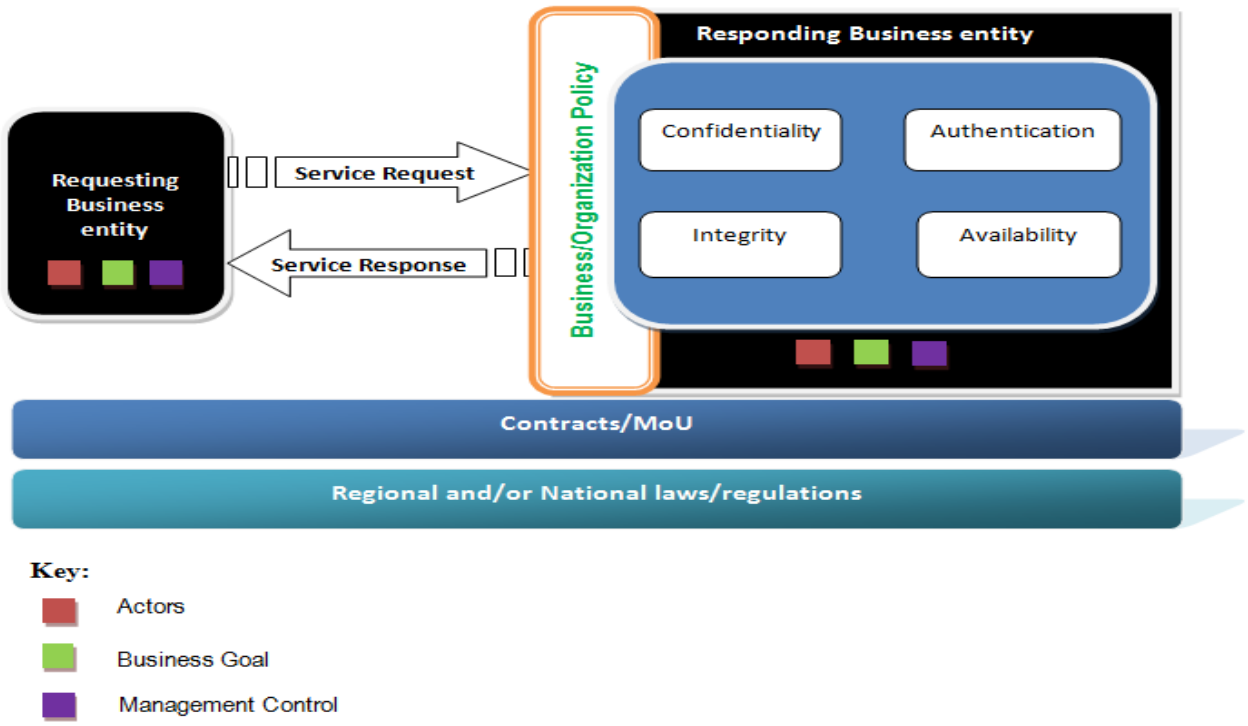


Figure 40: Business Model.

In order to implement the business model, the resources shown in Table 6 may be found helpful in getting updates on mechanisms such as international standards and national legislation.

Table 5: Supportive Resource for implementing the Business Model.

Source	Resource	Reason
www.iso.org	ISO/ IEC 27 000 series of security standards.	Source of security standards issued by ISO and IEC
www.parliament.go.tz www.parliament.go.ke	Legislation of the United Republic of Tanzania, Kenya	Sources of national legislation in Tanzania and Kenya
www.nist.org	National Institute of Standards and Technology	Information security standards and guidelines issued by the United States Government

(iii) Operational model

The Operational Model of the proposed framework summarizes organizational plans and practices that an individual business organization can use to tackle the information security requirements. And this has been motivated by the following factors:

(a) The proposed framework is cognizant of this practice; however, it is necessary for Business organizations to map their initiatives onto policies or legislation as and when they come into effect. This is by matching organizational plans to the required business components that tackle a specific information security requirement.

(b) Technical mechanisms for tackling information security should be backed by organizational practices and plans to allow for addressing of information security holistically.

Operational components include organizational programs and plans, common terminology for eCommerce transactions and certificate authority agreements. This model is implemented by operational departments in individual business organizations and some components are implemented across Businesses as shown in Fig. 40.

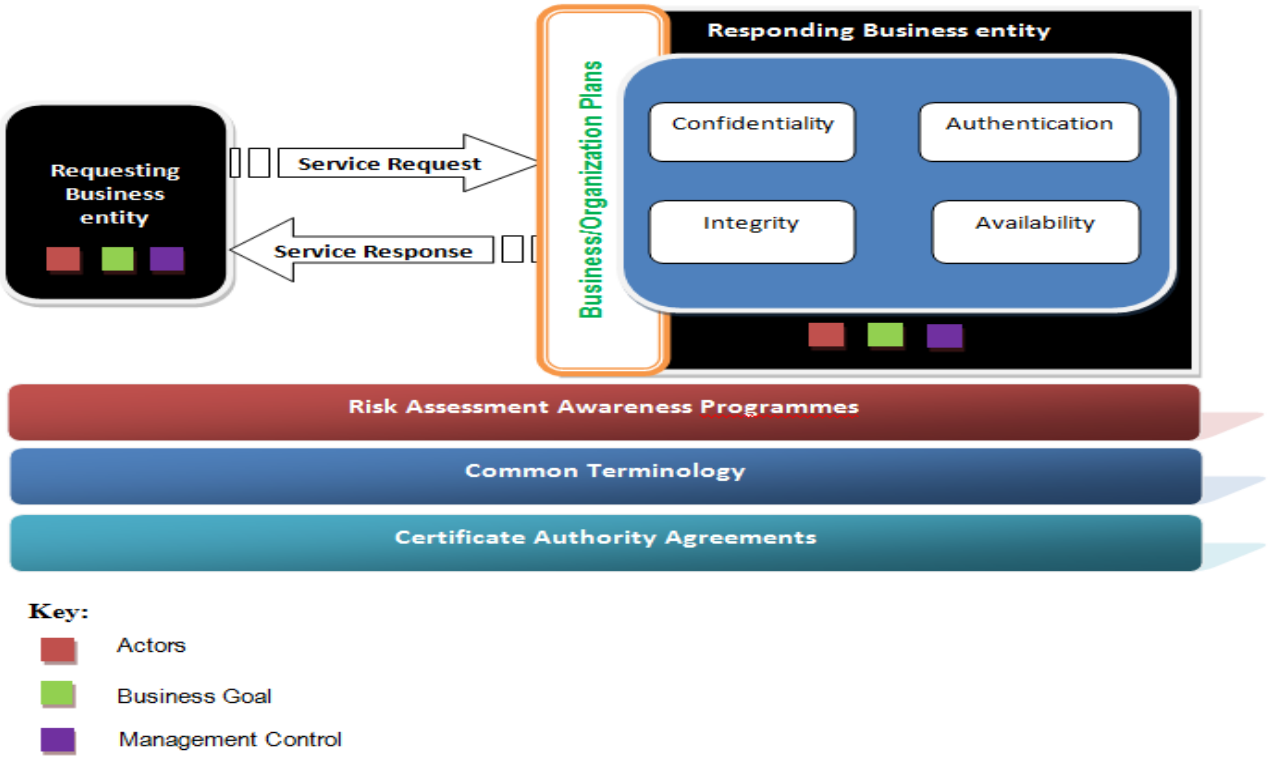


Figure 41: Operational Model

This Model is implemented by operational or business units within organizations. Table 7 shows the supportive resource for implementing the operation model.

Table 6: Supportive Resource for implementing the Operational Model

Source	Resource	Reason
www.isaca.org	Information Systems Audit and Control Association	Source of information on standards and white papers related to audit and risk assessment of information systems
www.cert.org/octave	CERT Program, Software Engineering Institute – Carnegie-Mellon University	Source of information on the OCTAVE Risk assessment methodology

(iv) Process model

The proposed technical, business and operational models represent distinct actors with diverse roles within each Business. For the business organization to move towards the proposed process addressing of information security requirements holistically; there must be introduced to each of three models. The proposed process model allows a business to identify what technical, operational or business mechanisms are in place and use them appropriately in an eCommerce transaction.

This has been motivated by the need to tackle three relative factors discovered which are:

(a) Resource limitation: These include financial constraints due to limited budgets allocated and inadequate ICT skills;

(b) Regulatory or Legal constraints: such as, lack of sufficient legislation and national policy frameworks associated to information security in eCommerce.

(c) Organization Culture constraints: such as unstructured or uncoordinated national government initiatives related to eCommerce.

The tackling of these factors is completed by designing the process model such that it exploits a ‘plug and play’ approach, that each Business organization applies the mechanisms that it can in a model and inserts those onto the corresponding models. Where cultural constraints or resources exist, the implementation continues, and a maturity model is proposed to guarantee continual improvement of business efforts to comprehensively meet information security requirements.

This model consists of two levels that are formally presented using the ebXML[8] (jerichosystems, 2016). The ebXML Business Process Specification Schema (BPSS) was developed specifically for e-business. This process model is relevant to two levels. The first level is an eCommerce transaction between two business entities, and the second level represents any two or more actors in a Business who are putting in place mechanisms to meet up the information security requirements.

At a high level, a Process Model consists of a set of roles collaborating through a set of choreographed Business Transactions by exchanging Business Documents.

These basic semantics of a Business Collaboration are illustrated in Fig. 41. In this case two or more business partners participate in the Business Collaboration through roles. The roles often exchange messages in the context of Business Transactions. Each Business Transaction has one or two predefined Business Document Flows. One or more Business Signals MAY additionally be exchanged as part of a Business Transaction to ensure state alignment of both parties. The Business Collaboration is defined as choreography of Business Transactions performed relative to each other.

Business Collaborations: A Business Collaboration in a Process Model is a set of Business Activities executing Business Transactions among collaborating parties or business partners. Each business partner plays one or more abstract partner roles in the Business Collaboration. The status of the Business Collaboration is logical among the parties interacting in a One-to-One rather than a controlled environment. The virtual status of the Business Collaboration lies with the involved partners. One-to-One collaboration may involve business partners and distributed collaborating parties.

[8] ebXML (Electronic Business XML) is a project to use the Extensible Markup Language (XML) to standardize the secure exchange of business data.

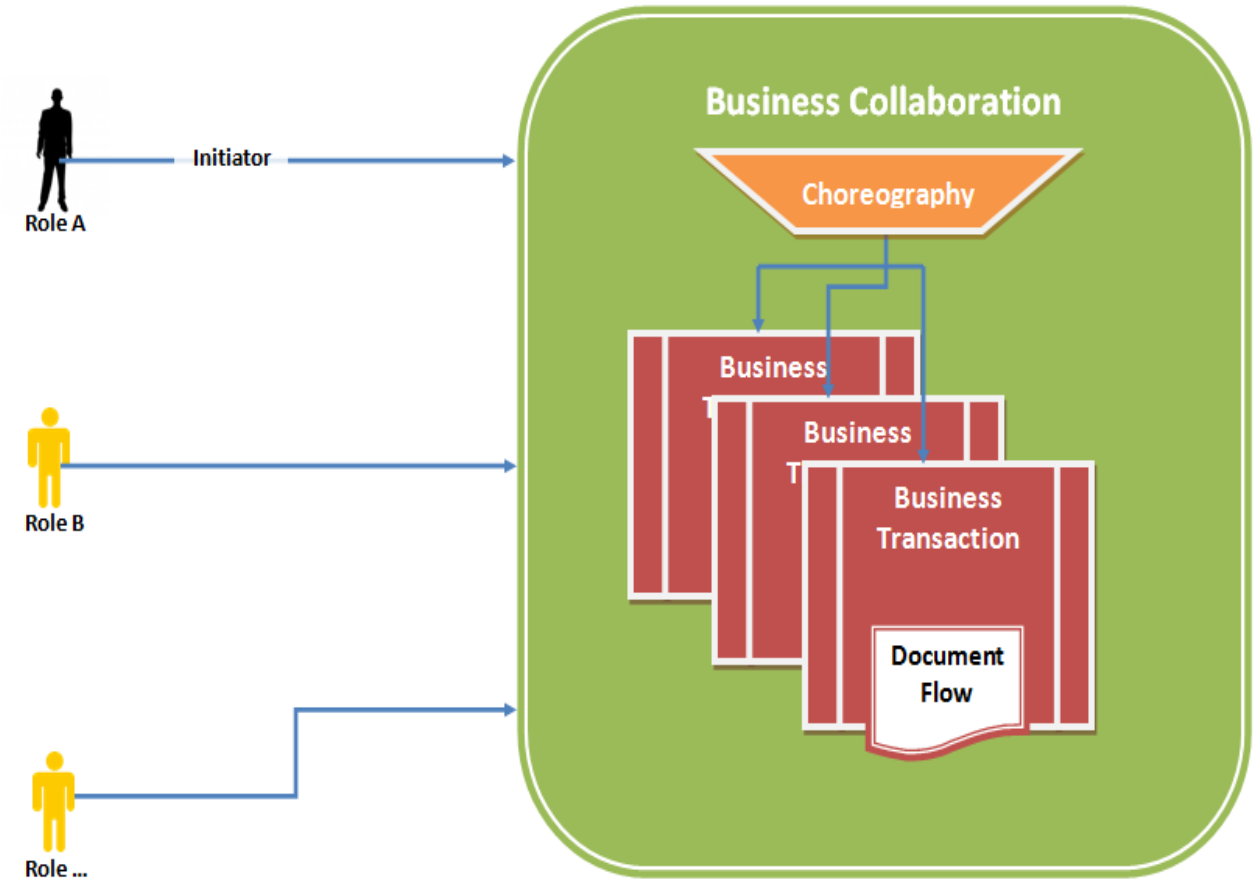


Figure 42: Illustration of Process Model.

Business Transactions: A Business Transaction in a Process Model represents an atomic unit of work that may relate to a trading arrangement among two business partners. The scale of the ebXML technical specification is to articulate more fully the Business Transactions, rather than primarily focusing on their relationship to trading arrangements among business partners.

The Transaction will often either thrive or fail. If it thrives, it may be designated as legally binding among the two partners, or else govern their collaborative activity. If it fails, it is null and void, and every partner must renounce any mutual claim established by the transaction.

Business Document Flows: This is realized as Business Document Flows among the Requesting and Responding parties performing roles. There is often a logical Requesting Business Document, and optionally a logical Responding Business Document, depending on the desired Business Transaction configuration: The actual Business Document definition is achieved by using the ebXML and/or by some methodology contracted by the business partners that have roles in the service collaboration.

Choreography: The process model is definitively characterized by the Business Transaction Choreography. The Business Transaction choreography describes the ordering and transitions among service transactions or sub collaborations surrounded by a binary collaboration. Thus, the choreography in this framework describes how insertion is done across different technical, operational and business mechanisms.

ebXML Implementation: This technical specification must be used wherever software components are being specified to execute a role in an ebXML Business Collaboration. Particularly, this technical specification is projected to provide the business process and document specification for the formation of ebXML trading partner Agreements and Collaboration Protocol Profiles.

However, this technical specification might be used to specify any eCommerce or shared collaboration. It can also be used for non-commerce collaborations, for example, in defining transactional collaborations among non-profit organizations or between applications, within the enterprise.

(v) Maturity model

The principle idea of a maturity model is to recommend a roadmap through which an entity can continually progress towards a set goal. This maturity model is aimed at helping Businesses continually progress information security practices through the secure framework with the aim of achieving a sustainable information security framework for eCommerce transactions (Fig. 42).

In order to design an information security requirements framework for eCommerce transactions, it is necessary to come up with a design that convenes the information security requirements. The discoveries on mechanisms and perspectives that are presented in this chapter are useful to develop blueprint artifacts that form elements of a framework. Blueprint artifacts might be builds, methods, instantiations or models (W3C, 2004). In addition to developing blueprint artifacts, the blueprint processes bases on a proposal by Carlson (Dada, 2006) to include an object blueprint, realization design and a process design in an information systems research initiative purposely to come up with a thriving problem solution. An object blueprint is the intervention necessary to solve the problem. The realization blueprint is guidance on how to implement the object design, and the process design is the techniques and methods to implement the object blueprint.

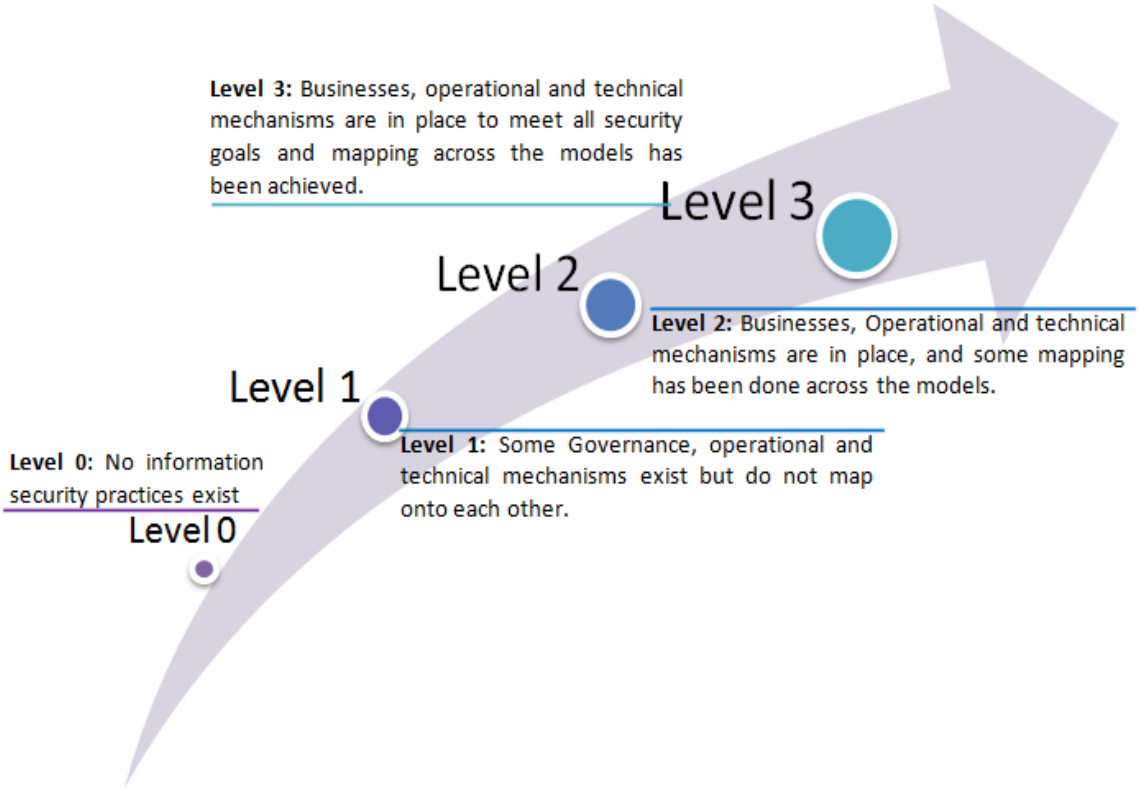


Figure 43: Illustration of Levels in a Maturity Model

The primary three models include mechanisms or components that tackle the meeting of information security requirements declared in this chapter. For every model, guidelines on implementation of the model are developed and helpful resources to be deployed by the implementing Businesses are included. This forms the attainable design. The Process Model fine points a process cycle through which businesses can implement the Technical, Operational and Business Model whereas the Maturity Model summarizes how the businesses can gradually progress on their aptitude to meet the Information Security requirements over time.

4.5 Conclusion and Discussion

This chapter has presented an information security framework for eCommerce transactions. The framework contains of five (5) models which are technical, business, operational, process and maturity models.

The basic tenets of the framework are simple – each actor in this framework must recognize their role; and do whatever is possible to address common security objectives. An insertion across models is done whenever each actor is addressing a security requirement. This process leads to a continual raising of information security awareness and a transfer towards holistic

handling of information security even where resources are limited and where there is little or no co-ordination within business or organization. For the technical, operational and business models, useful resources and implementation guidelines are presented so as to ease implementation. The inserted process model with its 'Plug and Play' implementation approach suits the framework where flexibility in approach is required to take into consideration the culture of un-coordinated initiatives, and at the same time, the limited resources.

The next chapter proposed the Novel framework for secure eCommerce transactions based on the foregoing chapter and were implemented the developed framework as summarized in Fig. 43.

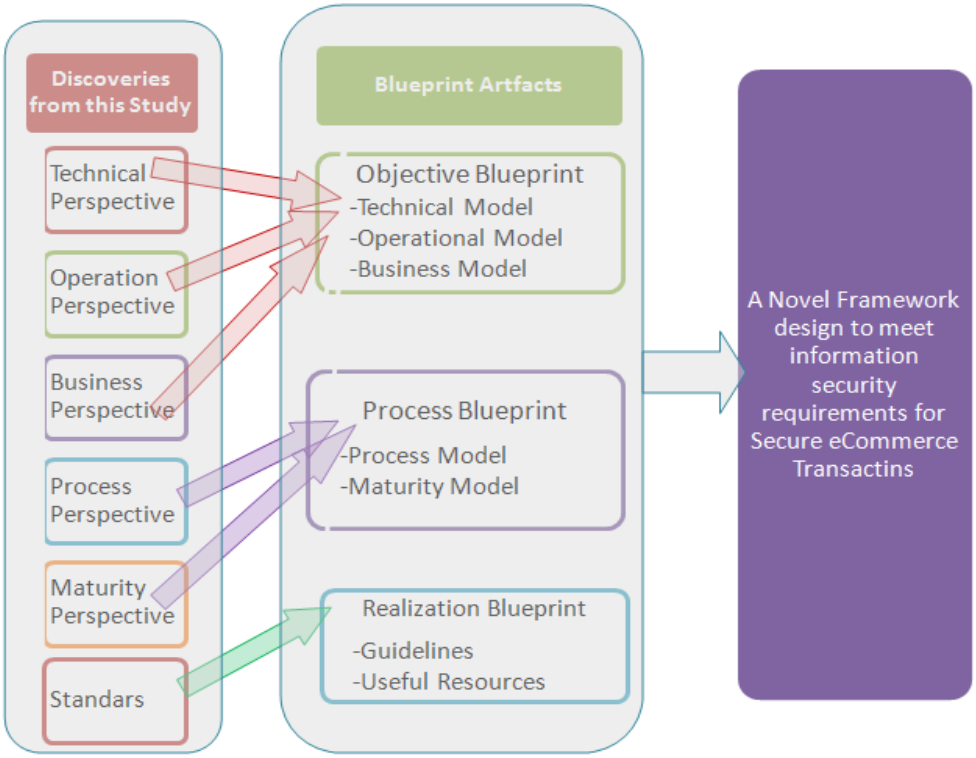


Figure 44. The design processes the resultant framework.

CHAPTER FIVE

A Novel Framework for Secure E-Commerce Transactions[9]

Abstract

E-commerce is now a trend and a must in many business sectors. In line with this eCommerce trend, many businesses use the internet to transact their business and to share information among trading partners. It is for this reason a proper and clear security must be defined to guarantee secure eCommerce transactions. This chapter proposes a novel framework that integrates secure technical, Business/organization, Operation security parameters, policy, customers and merchants as stakeholders in business for proper and secure information exchange. The framework points out the relationship among different parameters. With this framework, secure eCommerce transactions can be achieved.

Keywords: Pretty Good Privacy (PGP), Secure Electronic Transaction (SET), Security Protocols, Secure Socket Layer (SSL), trusted third party.

5.1 Introduction

Security and privacy are two key concerns to be addressed when deploying information and communication technologies (ICT). Coincidentally eCommerce shares security concerns with other technologies in information security frameworks. Unfortunately, privacy concerns have been found, revealing a lack of trust in a variety of frameworks, including those for electronic health records, social networking and e-recruitment technologies; and this has directly influenced users (Niranjanamurthy, 2013).

An information security framework is a synchronized system of behaviors and tools for monitoring transactions and data that are extended to where data utilization occurs, thereby providing end-to-end security (Vahradsky, 2012).

Ecommerce Security framework is a subset of the Information Security framework and is particularly applied to the components that influence eCommerce that include Data Security, Computer security and communication channel of the Information Security framework. Security in eCommerce has its own nuances and is one of the maximum visible security components that influence the end user during their daily transactions and interactions with businesses that are conducted on the global network (Internet), which is un-trusted.

[9] This chapter is based on the paper: Kenneth L. Mlelwa, Zaipuna O. Yonah A Novel Framework for Secure E-Commerce Transactions. International Journal of Cyber-Security and Digital Forensics (IJCSDF) Vol. 6, No. 2 92-100 Jun - 2017

Thus, confidentiality is needed throughout the transmission of transaction information and the information should be kept protected (Secure) against all kind of threats. Linked concepts and business practices symbolize opportunities for opening new domestic and international business enterprises. On the contrary, as Cyber space is used more and more as a platform for eCommerce transactions, security turns out to be a crucial issue for Internet applications. Security has become as an increasingly significant issue in the growth of any eCommerce organization. The purge of trust in eCommerce applications may result into sensible business clients and operators to give up the use of the Internet for now and slip back to traditional ways of doing business. Increasing access to sensitive information and replay are some familiar threats that hackers impose to eCommerce platforms (Berlin, 2007). Security protections embody with the safeguarding of availability, confidentiality and integrity of data (Barnes, 2002). These three canons of information security are occasionally symbolized in the Authentication, Integrity and Confidentiality Triad as in Fig. 44.

Figure 45: The Authentication, Confidentiality and Integrity Triad.

The Security community has documented the common security concerns as Access Control, Privacy/Confidentiality, Authentication, Non-Repudiation, Integrity and Availability. This chapter proposes a novel framework that integrates several parameters including customers and merchants as stakeholders in business to guarantee secure eCommerce transactions. The

chapter is organized as follows: the next section discusses a related work regarding the eCommerce study in secure transaction followed by problem statements, which explore common technologies for secure eCommerce transactions with their pitfalls. In Section 5.4, the new proposed novel framework is introduced and discussed. In Section 5.5, the developed secure plug-in for implementation of the proposed framework is presented. In Section 5.6, shows how the developed security plug-in can be used as a protection against security threats, and its results in Section 5.7 and finally Section 5.8 concludes the chapter.

5.2 Related Works

Almost all security frameworks have cons and pros. There is no one-best-fits- all frameworks that would work for every organization. Businesses and Organizations are simply too varied, ranging from large multi-national businesses with numerous databases to small private businesses that are largely self-contained. And the IT staffs within those firms vary widely when it comes to training and expertise.

The regulatory background has become more complex because organizations habitually find themselves required to comply with several regulations and industry mandates. As new threats emerge, standards and regulations persist to grow in number and complexity. Now-days, many laws have penalties for data violation including for not meeting timely notifications of those who are affected. The most important factor of security frameworks is to defend vital systems and the processes that provide those operations.

Without a doubt, any online transaction requires clients to reveal a huge quantity of sensitive private information to the merchants, introducing themselves at significant risk. Understanding (indeed, even precisely defining) trust on the consumer side is now essential and necessary for the continuing development of eCommerce.

The main reason of Web security is to safeguard and meet the security expectations of users and providers. Therefore, generally security in web technology is concerned with client-side security, server-side security, and secure transmission of information (Onieva, 2008) as summarized in Fig. 45.

(i) Server-side security deals with the practices and techniques that protect the Web server software and hardware from break-ins, Web site vandalism and denial of service attacks.

(ii) Client-side security deals with the practices and techniques that protect user's privacy and the integrity of the user's computing system.

(iii) Secure transmission is concerned with the practices and techniques that will assure protection from eavesdropping and intentional message modification (Onieva, 2008).

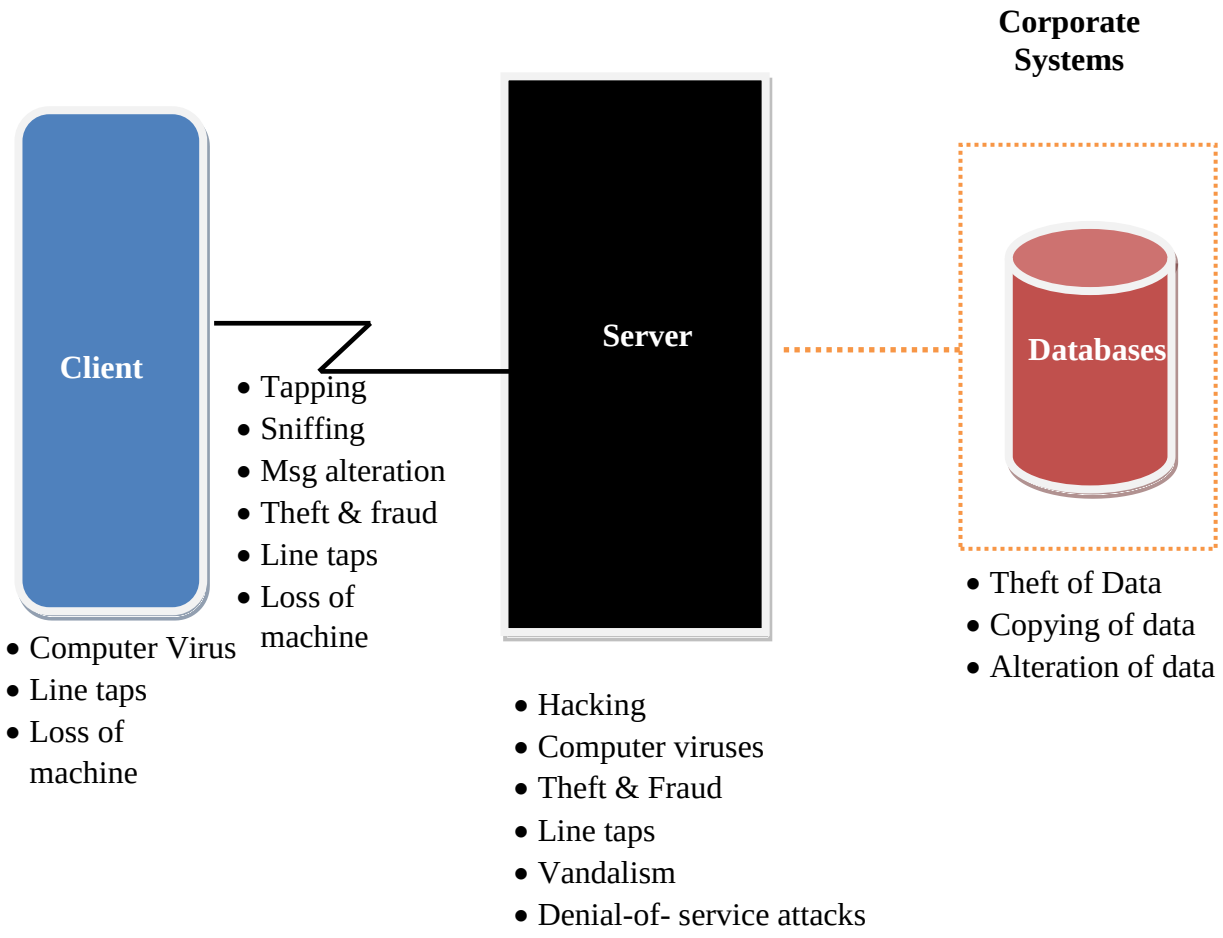


Figure 46: Security attacks on eCommerce Application.

Determining threats is a mountain to climb as well as time consuming but secure approach cannot be built without understanding the threats that may occur throughout the transaction communication. It is not easy to decide on a specific technology for tackling these threats. But it is known that the threats that can break eCommerce security are clarified as follows:

(i) Man-in-the-middle attack
(ii) Reply attack
(iii) Repudiation threat
(iv) Data Tampering attack and
(v) Information disclosure threat

Other researchers have been discussing security aspects in eCommerce, as a software solution aligned with Secure Electronic Transfer (SET) or Secure Socket Layer (SSL) technologies for encryption of data transmissions. SSL protocols allow transmission of encrypted data across the Internet by running above the traditional TCP/IP protocols (Ghosh, 1998).

Essentially, the SSL guards the communication between a server and client and provides authentication to both parties for the purpose of securing communication. It also provides a point-to-point security. It is for this reason that storage of sensitive data in repositories or databases makes eCommerce systems ideal targets (Ghosh, 1998). Unfortunately, hackers target data repositories due to availability of data on a single place.

Secure Socket Layer permits many key exchange algorithms, however some other algorithms like Diffie-Hellman key exchange have no certificate concept (Zhiguang, 2004). This is not compliant to an eCommerce security.

5.3 Problem Statements

The most common security protocols used in eCommerce secure framework are Pretty Good Privacy (PGP), Secure Socket Layer (SSL) and Secure Electronic Transaction (SET). But, these Common security protocols when deployed for the purpose of achieving eCommerce objectives have own pitfalls.

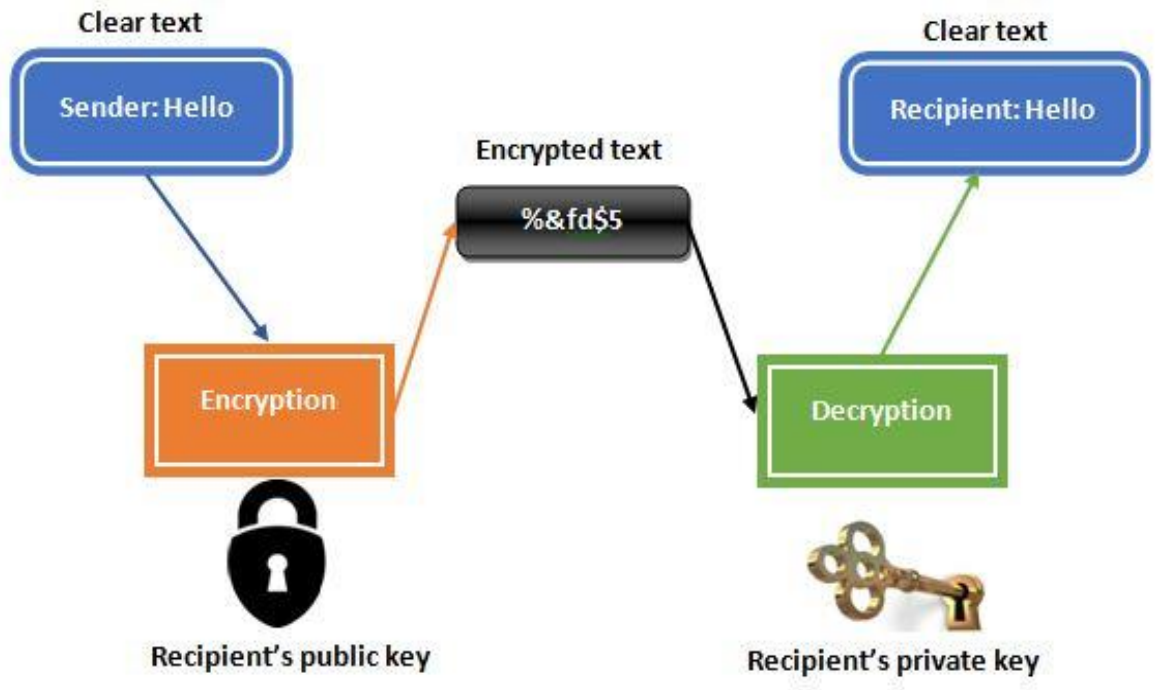


Figure 47: PGP Based E-commerce Cryptography (Al-Slamy, 2008).

Pretty Good Private (Fig. 46) has been considered to provide security to eCommerce (Al-Slamy, 2008). It is a software that combines several high-quality protocols and existing public-key encryption algorithms into one package for protection, file transfer and reliable electronic mail. Pretty Good Private not only provides encryption of data, but also data compression, digital signatures and smooth compatibility with email systems.

Pretty Good Private is pretty well-liked now, especially in the e-mail systems, but it is not full proof solution for eCommerce because it provides Confidentiality and Authentication only which are pretty good enough for email security and not for eCommerce security. Pretty Good Privacy cannot deal with Reply and Man-in-the-Middle attacks in eCommerce transactions.

In order to have a strong security framework, some security parameters must be kept in mind. Normally the main security objectives are Authentication, Confidentiality and Integrity.

However, for internet and web related applications, major security objectives include protection against non-repudiation, man-in-the-middle and reply attacks. That's why this chapter aimed to propose an eCommerce security framework capable of guiding to achieve major security objectives against common threats known as pinpointed in the Table 9.

Table 7: Comparison of; Security Objective vs eCommerce protocol.

Security Threat	**eCommerce Protocol**		
	SSL	**PGP**	**SET**
Confidentiality	YES	YES	YES
Non-Repudiation	*NO*	*NO*	*NO*
Integrity	YES	YES	YES
Replay Attack	*NO*	*NO*	*NO*
Man-in-the-Middle Attack	*NO*	*NO*	*NO*

5.4 The Proposed Framework

The proposed framework integrates different security parameters, policy and general business ingredients thus making it a Novel security Framework for eCommerce Transactions. To achieve this, security requirements analysis was conducted, and the results were used in proposing the framework. The framework is intended to facilitate and enhance security in eCommerce by providing a clear way of interactions, security measures and general

awareness. The proposed framework is divided into three sub frameworks namely; Secure Technical framework, Business/Organization framework and Operation Model (Mlelwa and Yonah, 2017).

5.4.1 Secure Technical Parameters

This sub framework is considered as the technical part of the main framework (Fig. 47), which consists of the following components (Mlelwa and Yonah, 2017):-

(i) **Customer/Merchant:** these are the main actors throughout an entire eCommerce transaction. These actors will be initiating all activities inside this sub framework.

(ii) **Security Objectives/Goals:** this **component** consists of Authentication, Non-Repudiation, Integrity as well as Reply and Man-in-the-Middle Attack handling components.

(iii) **Third Party Trustee:** this includes parameters that permit parties to communicate securely over public networks with the use of public key cryptography.

(iv) **Service Oriented Architecture (SOA):** in an eCommerce transaction, interactions are typically machine-to-machine exchange. The main reason of having a SOA in these Parameters is to achieve the availability security objective/goal, when deployed with web services. Simply because web services are technically unbiased. As a result, a web service produced by any business can be utilized by another business organization regardless of differences in technical platforms in the two businesses.

(v) **Attribute-based access control:** defines an access control paradigm whereby access rights are granted to users through the use of policies that combine attributes together.

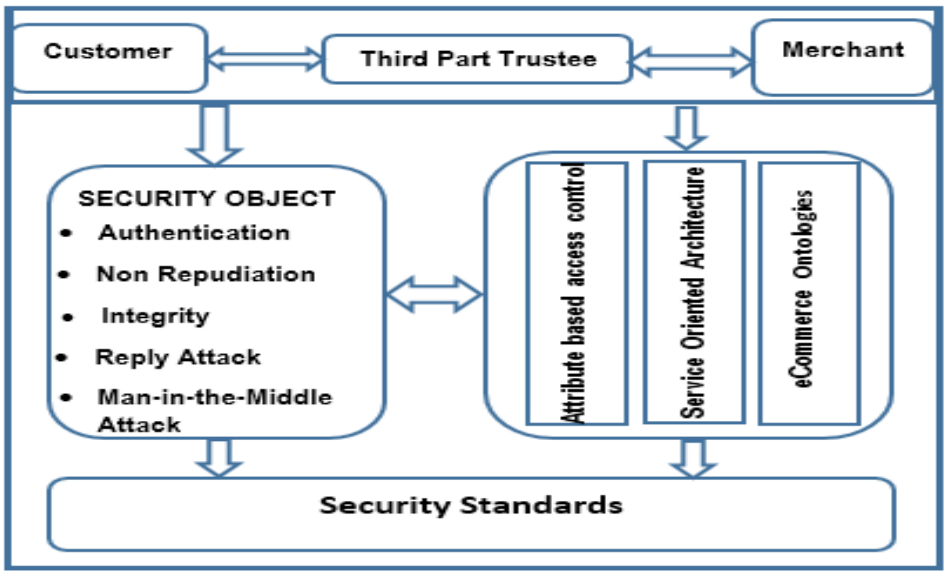


Figure 48: Secure Technical Parameters.

5.4.2 Business Parameters

The Business or Organization Parameters sub-framework sum-ups policy level mechanisms for tackling the information security requirements for eCommerce transactions. Its parameters consist of Business/Organizational plan, Regional and National laws and regulations, Contract/MoU as well as a Policy. This normally is implemented by top level management in an organization, as illustrated in Fig. 48.

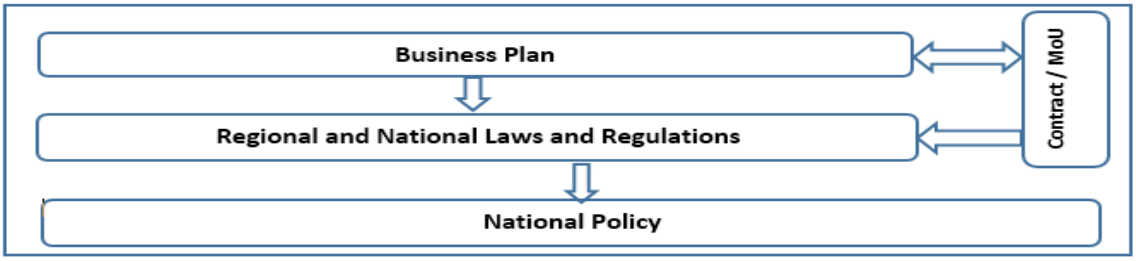


Figure 49: Secure Business Parameters.

Since an eCommerce transaction normally takes place across more than one business organizations then the framework should take into consideration the existing legislation and at the same time be flexible enough to accommodate new laws/changes to existing legislation.

5.4.3 Operation Parameters

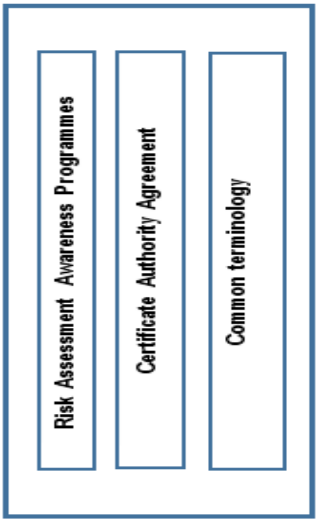


Figure 50: Secure Operation Parameters.

The Operation Parameters sub-framework as illustrated in Figure 49 summarizes organizational plans and practices that an individual business organization can use to satisfy the information security requirements. Its parameters include organizational programs and plans, common terminology for eCommerce transactions and certificate authority agreements. This model is implemented by operational departments in individual organizations and some components are implemented across businesses.

5.4.4 The Framework

The relationship between the proposed security factors is also indicated in Fig. 50. The purpose of the proposed novel framework is to enhance security in eCommerce by including several security factors resulting from prior security requirements analysis (Mlelwa and Yonah, 2017).

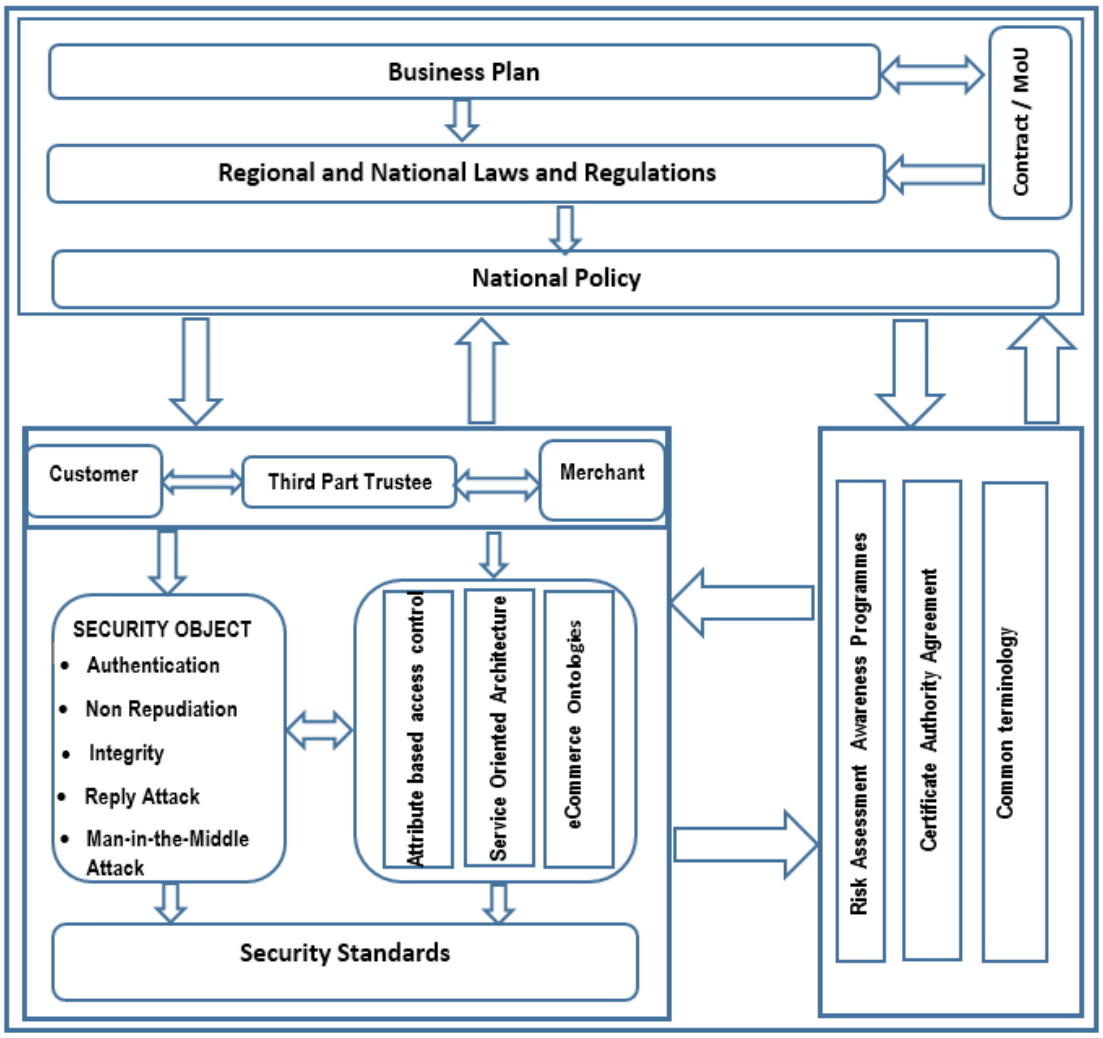


Figure 51: Proposed Collaboration framework for secure eCommerce Transactions

NB: *Arrows Shows the relationship*

All these three sub-frameworks cannot work independently, they need to be coordinated between one entity and another as in Operational sub-framework certificate Authority Agreement, which is supposed to be working simultaneously based on the Contract/MoU parameter found at the level of business sub-framework; where by this collaboration should be done without violating the regional or/and national laws and regulations. Therefore, for this framework to work perfectly all these sub-frameworks need to be aligned and working in a collaborative way to achieve all five objectives as in Table 9.

Table 8: Comparison of; Security Objectives vs eCommerce protocols for the new proposed unified protocol

Security Threat	**eCommerce Protocol**			
	SSL	**PGP**	**SET**	**USP**
Confidentiality	YES	YES	YES	YES
Non-Repudiation	*NO*	*NO*	*NO*	YES
Integrity	YES	YES	YES	YES
Replay Attack	*NO*	*NO*	*NO*	YES
Man-in-the-Middle Attack	*NO*	*NO*	*NO*	YES

5.5 Implementation and Testing

Based on proposed Novel framework (Fig. 50), a security plug-in was developed aiming to achieve secure eCommerce transactions. The developed plug-in consists of three entities, namely; customer, merchant and third-party trustee (TPT).

Prior to commencing an eCommerce transactions, merchant and customer parts must be registered by the Third-Party trustee (TPT); which will provide tokens for transaction to all customers and Merchants parts involved with sending data. Thus, when each customer and Merchant gets their transactions tokens then both parties start to communicate. And this proposed framework will offer protection against all these security attacks.

Table 9: Customer, merchant conversation steps

Steps	Customer actions	Third party trustee actions	Merchant actions
(i)	Customer requests token from TPT (third party trustee) EKU (TPT) [IDC, ReqC, Time, KUC, NC]	TPT sends a token to customer TC=EKR (TTP) [IDC, ReqC, Time, KUC, NC]	When merchant receives customer token, then merchant would have to request for an issuance of token to TPT. EKU (TPT) [IDM, Time, KUM, NM]
(ii)	Customer sends token to merchant TC→M	TPK provides a token to merchant and encrypts it. TM=EKR (TTP) [IDM, Time, KUM, NM]	Merchant sends token to customer TM →C
(iii)	Customer sends information to merchant Eku (M) [NC, EKR (C) [IDC, Time, NC]]		Merchant sends information to customer Eku (C) [NM, EKR (M) [IDM, Time, NM]]
(iv)	Customer acknowledgement passed to merchant		Merchant acknowledgement passed to customer

Table 10: Notations for Customer and merchant conversation steps

Notation	Description
TPT	Third Party trustee
TC	Token Issues to Customer
TM	Token Issues to Merchant
NC	Nonce generated by Client
NM	Nonce generated by Merchant
Time	Time Stamp
IDC, IDM	Identity of Client and Merchant
EKR (C), EKR (M)	Private encryption using private keys of Client and Merchant
EKU (C), EKU (M)	Public encryption using public keys of Client and Merchant

Using the tabulated steps as illustrated in Table 10 (Table 11 Shows the abbreviation of various notation used in Table 10) results into transactions such that a merchant and a customer share a bunch of information for the purpose of recognizing each other and solve future disputes (if any) in regard to an eCommerce transaction.

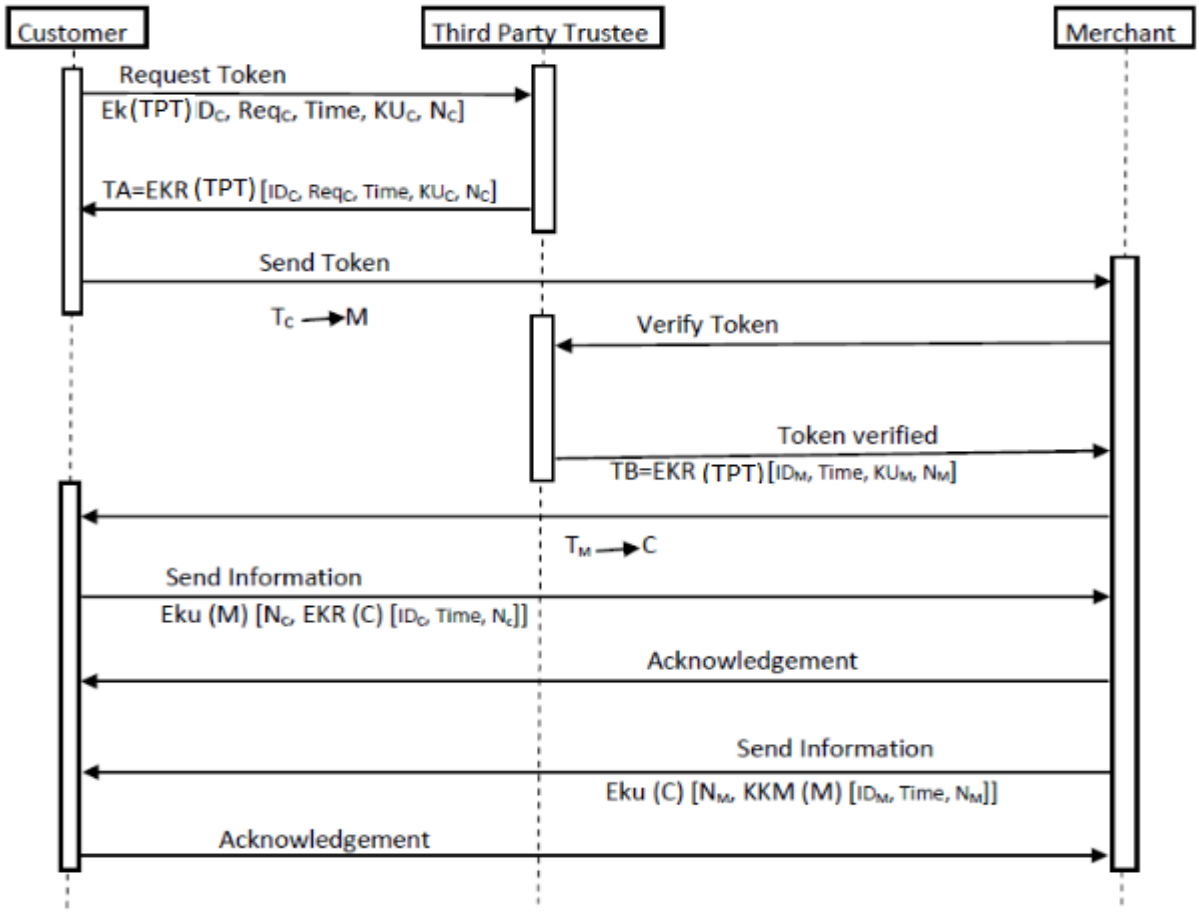


Figure 52: Customer, merchant conversation Sequence Diagram

5.6 Protection against Security Threats

The proposed eCommerce security framework is designed with the capacity to overcome all major security objectives as described in Fig. 51, as follows:

5.6.1 Authentication

In this scenario; Customer sends ID, nonce and time that is signed by customer using private key and then encrypts the whole package by public key of Merchant (step 3). Merchant decrypts the package with its private key. After decrypting the Customer Package, the merchant will access the customer ID; as the package is signed by private key of customer. This way, the Merchant can determine that customer is Authentic.

5.6.2 Reply Attack

In the case of key exchange, a reply attack can take place, which is easily solved in the proposed solution. For example; a reply attack can take place in step 1. The un-trusted party can grab the token requested by the user and there after reply to the TPT for getting a fake token. But since the requested token contains ID, time and nonce; the TPT can use this information to easily recognize it as a replay attack, and the request produced by unauthorized party will be discarded.

5.6.3 Integrity

In order to solve the integrity issue; on the customer part the hash code is produced using SHA-1, of which is encrypted with the customer's private key. The encrypted hash code is combined with the original transaction message and then sent to the merchant. Then the merchant part splits the hash code from the message and decrypts it with the customer's public key. At the same-time, the merchant will have to analyze the hash code of the received transaction message using the same SHA-1 algorithm. Transaction message will be received correctly if the analyzed hash code and decrypted hash code will be the same.

5.6.4 Non-repudiation

Both customer and Merchant get their tokens from TPT, which contains their IDs, Nature of request, time of issuance of token, their respective public keys and a nonce (produced by the customer and Merchant correspondingly). The third-party trustee will keep a copy of the novel request for the token sent by the customer and merchant (see step 1 in Table 10 on customer and merchant columns) and a copy of the transaction tokens issued to them. As a result, a Non-Repudiation problem can be solved using the third-party trustee.

5.6.5 Man-in-the-Middle Attack

This kind of attack happens when three entities are involved (server, client and UNTRUSTED third party) during a transaction session. UNTRUSTED third-party positions itself between the client and the server on the network and learns about the traffics that are coming from client to server and from server to client. Using this security plug-in developed based on the proposed security framework; Third Party Trustee (TPT) generates a token that comprises of ID, Public key, issuer name, Hash code, Nonce and token appended with the Third-Party Trustee private key. The client checks the token novelty by examining the signature and name of the issuer.

5.7 Results

A security plug-in[10] (algorithms) was developed purposely to secure an eCommerce transaction based on proposed novel framework.

The developed algorithm was implemented using the java programming language. The implementation procedure consists of transactional parameters. First; is the root entity (the Main parameter) and the others are customer and merchant parameters. The main parameter acts as an interface for the other two parameters. The parameters concerned in the transaction need an authentic token via a security plug-in to the main parameter. Meanwhile, the root entity offers genuine tokens to both transaction parameters through the developed plug-in. The parameters involved in the transaction, requests for authentic token via security mechanism plug-in. Again, the main entity provides an authentic token to all transaction entities through plug-in security module. Fig. 51 depicts the implementation process in detail.

In order to secure an eCommerce transaction, plug-in generates tokens that are used by both the customer and merchant. Tokens have different parameters such as serial number, subject, hash code, issue name and public key. Customer and merchant first confirm the authenticity of tokens and then start to communicate in a secure domain shown in a couple of conversation's Diagrams in Fig. 52 and 55.

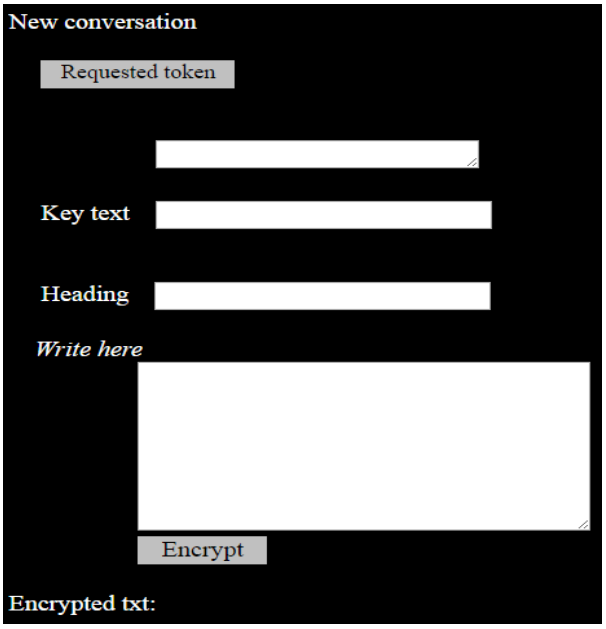
Figure 53: The case when customer and Merchant haven't started to communicate.

When the customer starts to converse with merchant, the customer requests a token from TPT. Then TPT sends a token to customer side; and the customer sends the message to merchant with a token received from TPT.

Fig. 53 shows two sides of merchant side where by on the left-hand side the customer has not yet requested for a new token; while on the right hand side the customer has been provided with a token, which was requested before, and hence used the token given to send an encrypted message to merchant side.

[10] The developed plug-in is in GUI for the purposely of elaboration, plug-in normally are not in a graphic user interface

Before requested for a token



After requested for a token

Figure 54: The case of Customer side before and after requesting for a token from TPT.

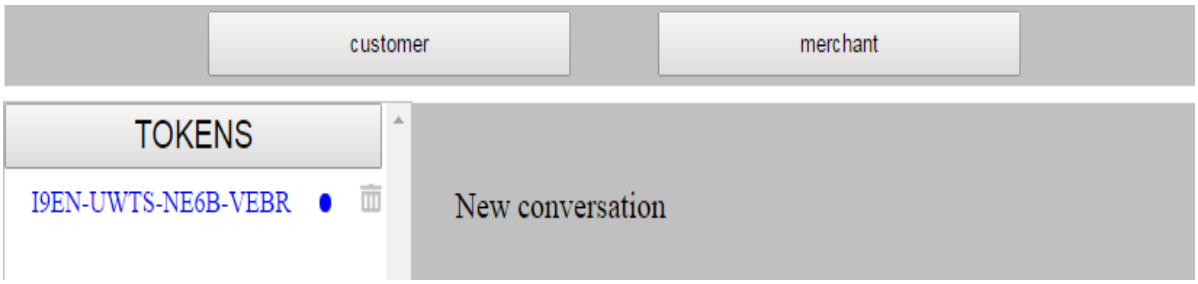


Figure 55: Merchant's side received a token from customer.

After the customer sends his encrypted message to merchant's side, the merchant will receive the token which was initially provided by TPT to customers (Fig. 54).

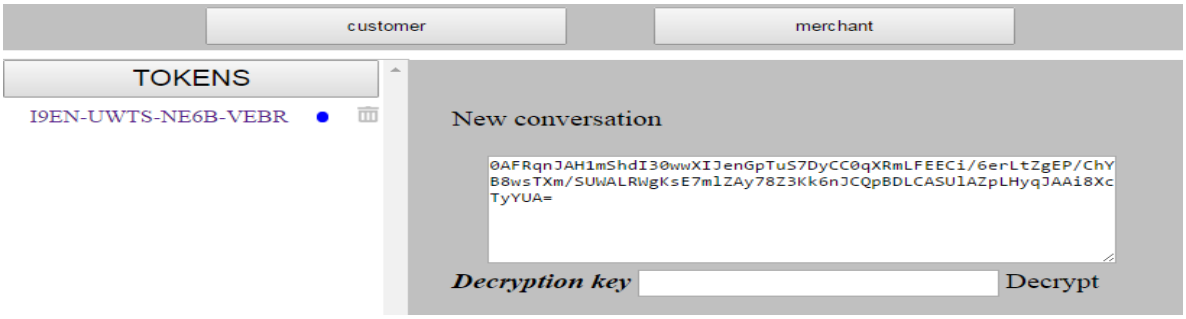


Figure 56: The case when a Merchant receives encrypted message from customer.

After the merchant receives a token from customer (Figure 55), he will decide to open it with the help of the decryption key that was used by the customer to encrypt the message. The decrypted message will show the time at which the message was sent; as shown in Fig. 56.

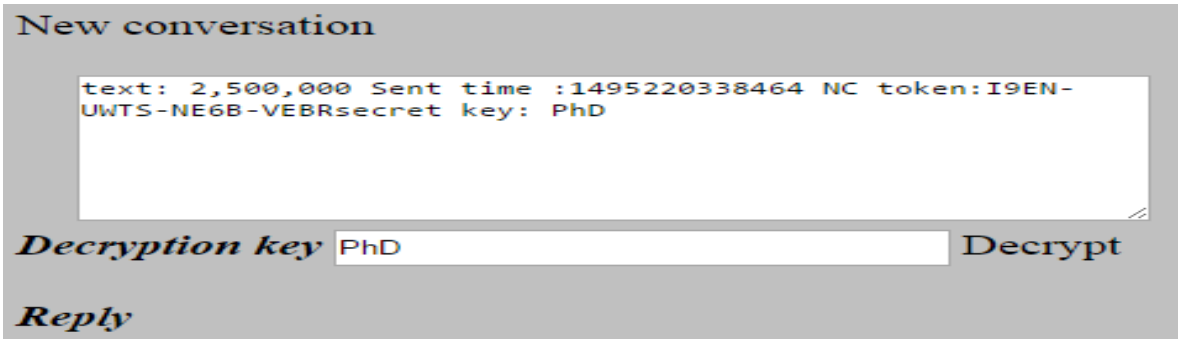
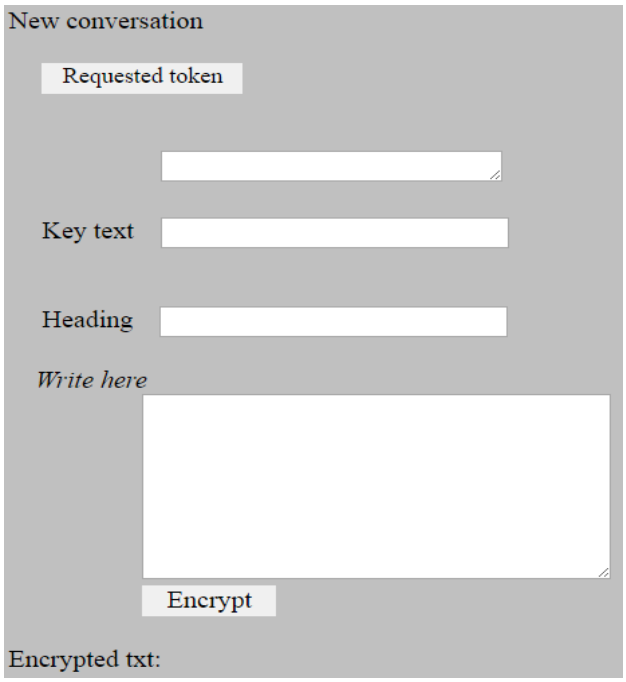


Figure 57: Merchants side with the decrypted message

Once a message has been decrypted the merchant will decide to acknowledge the receipt of the message to customer, with the help of a TPT just like customer does a merchant will have to request a token from a third party to finish the conversation with customer side.

Before a merchant requested for a token



After a merchant requested for a token

Figure 58: Merchants side before and after requesting for a token from TPT.

The plug-in encodes the package to pass on over the communication channel and then decodes it at receiving side to achieve the original data. It also provides authentication and integrity verification to customer and merchant packages to protect against threats.

After exchange of tokens between customer and merchant, the application stores the tokens in XML data files to eradicate non-repudiation problem in the future.

5.7 Conclusion

Online business (eCommerce) in developing countries especially in Tanzania is still at infant level and in its formative stages of development; however, with this speed of development over the past years, it is a clear signal of its enormous potential for conducting online business. These new opportunities, however, come accompanied with many concerns and questions about security issues that need to be resolved.

As such, security remains to be a major concern for eCommerce. It is an impediment to expanding e-commerce services and business. Due to this, consumers need protection beside fraudulent, unfair and misleading business practices, including when things go wrong, to be able to gain redress. Regularly, organization/companies need to safeguard themselves against attacks to guarantee data integrity, confidentiality, authenticity and including some other major attacks like Reply and Man-in-the-middle Attacks of data domain. Hence, it is necessary to occasionally review the regulatory framework so that consumers have effective protection when conducting eCommerce transactions. Equally necessary, eCommerce companies will need to develop and adopt a set of industry standards as addressed in the proposed framework to protect consumer privacy as a way of supplementing the formal legal obligations. Further, eCommerce businesses can build trust at an individual level by implementing industry best practices, which are underpinned by the proposed security framework that are enforceable.

There are many issues concerned in securing eCommerce Transactions e.g. Privacy, Access Control, Integrity, Non-Repudiation and Confidentiality. These concerns are still been potential ongoing research problem. The Internet, which is the crucial medium used for conducting eCommerce transactions, is not planned to handle transactions securely. In this chapter an approach has been recommended, which covers Authentication, Non-Repudiation and Integrity security objective in a secure manner.

In this chapter secure eCommerce Protocol is proposed to provide protection against attacks. This Novel framework for secure eCommerce transactions is presented a new security framework to address security issues that face eCommerce consumers, merchant's organizations and policy makers along three dimensions security, privacy and trust based on security objectives/goals. It also outlines several managerial policy and technical implications that will have to be taken into consideration going forward.

CHAPTER SIX

General Discussions, Conclusions and Recommendations

6.1 Overview

The insights acquired from the literature survey were mutual combined with data collected on chapter two through observations of current information security practices in both businesses and organizations as presented in chapter three and involved an interview with stake holders. From these, the study conceptualized a novel framework for secure eCommerce transactions. The framework recognizes the need for eCommerce transactions to be conscious of national policies and legislation, will at the same time complying with businesses / organizational policies. At the technical party, for a country that has limited resources like Tanzania, the technical model recognizes the existence of tried and test mechanisms, mainly those based on open internationally accepted standards.

The eCommerce secure framework consists of three sub-frameworks namely Technical, Operational and Business. The business Parameters sub-framework includes Business plan, Regional and national laws and regulations, Contract / MoU and Policy. The operational Parameters sub-framework includes Risk assessment awareness programme, Certificate authority agreement and Common terminology. The technical Parameters sub-framework includes technical mechanisms to address the security requirements and is implemented by Information Technology departments within business organization. The components of each sub-framework are gleaned from chapter three and matched to security objectives and requirements that are applicable to the eCommerce transactions. The detailed framework is depicted in Table 11.

Table 11: A details proposed collaboration framework for secure eCommerce Transactions.

SECURITY OBJECTIVE / GOAL	SECURITY REQUIREMENT	PARAMETERS		
		Business	***Operational***	***Technical***
Confidentiality	Authentication Authorization and Access Control Privacy	• International Standards, • Laws and Regulations, • Organizational Policies	• Risk Assessment • Certificate Authorities • Metadata definitions • Awareness Sessions	• Ontologies • Attribute based Access control using XACML & SAML attributes • Passwords
Integrity	Data Integrity	• International Standards, Organizational Policies	• Certificate Authorities	• Encryption, SSL
Availability	Availability	• Business Continuity Policies (BCP)	• Power Management • Business Continuity Plans • Interoperability frameworks	• SOA, Web Services, Uninterruptible Power Supply (UPS)
Accountability	Trust & Non-Repudiation	• Laws and Regulations, • Contractual Agreements and MoUs	• Certificate Authorities	• Digital Signatures, Certificates, • PKI

6.2 General Discussions

This Section summarizes the research study on A Novel Framework for Secure eCommerce Transactions. This study was guided by four sub studies corresponding to the specific objectives and research questions presented in Chapter One, Section 1.3. Study two and three are linked very closely to each other and therefore are discussed altogether. The discussions on the achieved results from those four studies are presented in a in this Chapter, Section 6.1:

(i) What is the ecommerce trend in developing countries?

The study reported in this dissertation has found that aptitude for growth of eCommerce in developing countries especially Tanzania is promising. Some findings show that there is a growing awareness towards the online industry. It is noted that customers prefer non tangible goods i.e. services over tangible products. Well-developed eCommerce websites are doing excellent job but still there are some factors that are inhibiting users from purchasing online.

Based on the survey results it is confirmed that, for a client to accept eCommerce, it is very important that the benefits of using this commercial medium (e.g. convenience, savings in time and transaction costs) significantly outshine possible risks. Undeniably, the customer

freedom to select suitable vendors needs to be associated with greater anxieties regarding financial risk, trust and privacy. This is since private users are directly involved in the commercial exchange; they are using their own equipment, spending their own money and giving sensitive information about themselves as individuals. There are still a range of factors to be looked upon to cater the needs of the customer who is the driving force for eCommerce. Therefore, based on the survey results it can be concluded that SECURITY is the most important factor in conducting eCommerce businesses.

(ii) What are the current issues and challenges facing security in eCommerce frameworks? And

(iii) What are the main security risks/threats that are imposed on eCommerce security frameworks?

Generally, eCommerce refers of using technological development to support everything involving the exchange of business information among computers and humans or traders and customers. Thus; everyone who is using eCommerce needs to be concerned about the security of their personal information. As reported in chapter 2 and 3 of these dissertations, it was necessary to determine the main constraints that restrict the efficiencies of security frameworks in e-commerce.

Holistically; eCommerce consists of a chain of events. Several products and techniques are used to secure parts of the value chain. As a result, five main categories of security needs were identified, namely:

(a) Authentication, for assurance that the communicating entity is the one claimed to be.

(b) Access Control, for prevention of unauthorized personnel who misuse resources.

(c) Data Confidentiality, for protection of data from unauthorized disclosure.

(d) Data Integrity, for the assurance that received data is as sent by an authorized entity.

(e) Non-repudiation, for protection against denial by one of the parties in a communication.

Furthermore, in eCommerce frameworks the key points which are vulnerable for attack are; Client level, Server level and Communications pipeline sometime refers as Internet communication channels. In this study, these key points are referred to as the eCommerce environment.

Research findings as reported in chapter two and three show that the main challenge restricting the efficiency eCommerce is how to protect against security threats especially from Confidentiality, Non-repudiation, Integrity, Replay and Man-in-the-Middle Attacks. Additionally, research results show that most of the technologies used in protecting eCommerce transactions cannot be used to achieve all security objectives. As a result, there's a need of having a holistic framework which will help the developers to develop a security mechanism to cover all these five threats.

(i) What are the information requirements for secure eCommerce transactions?

Normally it's too difficult to elaborate a framework since many of its steps or outputs are unspecified or abstract. To address this difficulty, a combination of Goal-Oriented Requirements Engineering and Problem Frames, were used to insatiate the proposed security framework by describing it in terms of a set of activities.

The proposed Framework refers to a process designed to evolve with changes in information security threats, processes, and technologies. This Framework visualizes effective security as a dynamic, continuous circle of reaction to all threats and solutions. Thus, businesses that implement this Framework will be better positioned to comply with future security and privacy regulations. At the least, businesses that operate in regulated industries should begin screening how regulators, examiners, and other sector-specific entities are changing their review processes in response to the security Framework.

Based on the foreground explanations, there are parameters and steps that need to be considered when designing a secure eCommerce transactions framework; the proposed novel framework is a unified framework, consisting of five models that are based on specified Security goals. These models are:

(a) **Technical model**: this presents technical mechanisms that work together to address the information security requirements for eCommerce transactions.

(b) **Operational model**: this presents operational mechanisms that need to be implemented during eCommerce transactions.

(c) **Business Model**: this presents governance mechanisms that need to be implemented at a policy level within an organization.

(d) **Process model**: This presents the way the secure framework can be implemented within an organization and amongst businesses that plan to undertake eCommerce transactions.

(e) **Maturity Model**: this provides a mechanism for businesses to continually measure progress with regards to meeting information security requirements for an eCommerce transaction.

In order to design an information security framework for eCommerce transactions, it is essential to come up with a blueprint that summons the information security requirements. The discoveries on mechanisms and perspectives that are presented in this dissertation have been used to develop blueprint artifacts that form elements of the framework.

6.3 Conclusion

Though eCommerce in Tanzania is in its early stages of development, its amazing growth over the past five years is a clear indication of its enormous potential for conducting business. These new opportunities, however, come accompanied with a large number of concerns and questions that need to be resolved. This dissertation has presented some of the challenges that face eCommerce consumers, organizations and policy makers.

It is confirmed in this study that, security is a chief concern for eCommerce sites and consumers alike. They are an important obstacle to expanding eCommerce services and business. Due to this, consumers require protection against misleading, unfair business practices and fraudulent, when transactions go wrong, to be able to gain redress. In addition, companies require protecting themselves in areas of confidentiality, data integrity, and authenticity of data. Is pointed that it is necessary to occasionally review the regulatory framework so that consumers have effective protection when engaging in electronic commerce. Again, eCommerce companies will require developing and adopting a set of industry standards to protect consumer privacy as a way of supplementing the formal legal obligations. Also, eCommerce businesses can build trust at an individual level by executing industry best practices, which are underpinned by clear social expectations and legal obligations that are enforceable.

However; there is no “one-size–fits-all” solution when it comes to selecting a security framework. Organization / Institutions must carefully weigh the pros and cons of each. Choosing the best security framework is not easy. It needs adequate research and buy-in from Organizations or institution’s decision makers. The Novel security frameworks proposed in this dissertation provide varying styles and degrees of protection, with differing approaches, but they all seek to accomplish the same goal: rigorously provide security of information

systems from threats that will continue to increase in the coming decades. Selecting a security framework is critical. Given the escalating threats to eCommerce businesses and the potential for catastrophic data loss and damages to a businesses' reputation there is no time to equivocate. Organizations or businesses operating without a security framework must implement the best one.

6.4 Recommendations

Based on the findings reported in this dissertation, it is hereby recommended that:

6.4.1 Government

This dissertation found that most of the user are hesitating to do online transaction due to security issues; and this is because the national ICT policy remain silent for online payment, as a result payment-gateway for online business it a mountain to climb.

The study also found that ICT infrastructure in Tanzania are still at early stage, Government institutions should intervene to smooth the online business including lowering tax for bandwidths.

6.4.2 Organization / Business and Policy Makers

This dissertation suggests that businesses organizations practicing electronic commerce should formulate policies that promote information confidentiality as well as increasing the funds allocated for managing threats against information confidentiality. And this include creation of awareness and train staff and consumers on information security services.

Again, an organization need to emphasize on a development of a risk assessment necessary to asses all security objectives discussed on Chapter five, Section 5.6 confidentiality.

6.4.3 Directions for future research.

In parallel with this developed framework, the most natural continuation of this research would be to take the proposed framework even further as depicted here under.

(i) The Framework can be further validated, simply because validation was not in our plan and we think this will be done in a future research as well as enhanced and substantiated in the context of actual use or in larger scale experiments. It would be an interesting long-term study to observe the effect of the proposed framework in a real

life system on the market, to observe their relevance in a longer span of time, and to track down their development.

(ii) Further work on secure eCommerce framework should try to resolve potential threats to their validity especially in Mobile Commerce. On the one hand, in the future study; Security in Mobile Commerce (M-Commerce) Transactions should be much emphasized as M-Commerce is becoming a new trend in online business and therefore the framework can be used differently than in the presented study.

Another way of the application and implementation of the security framework can improve a chance to avoid mono-operation bias, i.e. applying the security framework only in one way. This can also help to refine the details of the framework for secure eCommerce (including M-Commerce) transactions.

(iii) The National ICT policy of 2016 did not cover clearly the issue of eCommerce transaction, as in Section **1.1.11 E-Transactions** state that:

> "*Currently, there are limited e-transaction services such as e-commerce due to lack of local credit cards and supportive legal framework appropriate for e-business promotion. Most significantly, the legal framework does not provide adequate safeguards to create an environment of trust for e-business transactions to take place. Consequently, financial institutions and businesses at large are not able to set up provisions for supporting e-transactions for their own, and each other's clients."* (TMWTC, 2016).

Thus, there is a need of another framework for further study which should be aligned with the National policy specifically for eCommerce transactions.

(iv) A promising direction of future research is in a human error, as with the development of Technology and the new way of tackling security issues in eCommerce human error has become inevitable thus the researcher recommend more study on this area (Human error) since this study did not cover this aspect.

In generally, more fundamental research is required on appropriate methods for testing the security framework of eCommerce Transactions. This is, of course, a very large research area in its own.

REFERENCES

AlFayyadh, B., Thorsheim, P., Josang, A., and Klevjer, H. (2013). *Improving Usability of Password Management with.* [Online] Available at: http://folk.uio.no/josang/papers /ATJK2012-SARSSI.pdf [Accessed 10th February 2016].

Allen, J. (2001). *"CERT System and Network Security Practices," in Proceedings of the Fifth National Colloquium for Information Systems Security Education (NCISSE'01).* George Mason University, Fairfax.

Al-Slamy, N. M. A. (2008). E-Commerce Security. *International Journal of Computer Science and Network Security,* May.Volume vol. 8.

Anon. (2015). *Internet Usage Statistics for Africa.* [Online] Available at: http://www.internetwordstart.com/af/tz.html

Applicure. (2010). *Web Application Firewall.* [Online] Available at: http://www.applicure.com/solutions/web-application-firewall [Accessed 10 January 2016].

Barnes, C. (2002). *Hack Proofing Your Wireless Networks.* Rockland: Syngress Publishing.

Berlin, D. (2007). Information Security Perspetcive on Internet. In: *E-Commerce Infrastructure.*

Bjorck, F. (2004). *Institutional theory: a new perspective for research into IS/ IT security in organizations.* Hawai International Conference on System Sciences.

CCK. (2012). *Quarterly sector statistics report fourth quarter of the financial year 2012 / 13,* Nairobi: Communications Commission of Kenya.

CEN. (2007). *Network and Information Security Standards Report. Final Version,* ICT Standards Board.

Corporation, C. (2006). *Online payment fraud trends merchant practises & benchmarks.* 7th annual online fraud report report.

Dada, D. (2006). The Failure of e-Government in Developing Countries: A Literature Review. *The Electronic Journal of E-Government in Developing Countries,* Issue 26.

Dardenne, A., van Lamsweerde, A. and Fickas, S. (1993). "Goal-Directed Requirements Acquisition" Science of Computer Programming. *Elsevier,* 20(1-2), pp. 3 - 50.

Digit, S. (2011). *Digitsmith.* [Online] Available at: http://www.digitsmith.Com/ecommerce-definition.html [Accessed 10 March 2015].

Elofe, J. and Elofe, M. (2003). *Information security management – a new Paradigm.* SAICSIT.

Eurostat (2010). *Ecommerce contribution in Europe.* [Online] [Accessed 18 March 2015].

Evans, R. (2002). *E-commerce, competitiveness and local and regional governance in Greater Manchester and Merseyside: A preliminary assesment.* Urban Studies.

Frank, T. (2013). *China's cross-border e-commerce tops $375 billion in 2012*. Internet Retailer.

Garbade, M. (2011). Differences in Venture Capital Financing of U.S., UK, German and French Information Technology Start-ups A Comparative Empirical Research of the Investment Process on the Venture Capital Firm Level.. *GRIN Verlag GmbH,* Issue ISBN 3-640-89316-6, p. p.31.

Ghosh, A. (1998). *E-commerce Security, Weak links, Best Defenses.* New York: John Wiley.

Ghosh, A. K. (1998). E-Commerce security: No Silver Bullet. *IFIP Conference Proceedings.* Volume 142, pp. 3 - 16.

Hassler, V. (2001). *Security Fundamentals for E-commerce.* Artech House Publisher.

Hayat, Z., Reeve, J. and Boutle, C. (2007). Ubiquitous security for ubiquitous computing. *Information Security Technical Report.* 3(12), pp. 172 - 178.

ISO/IEC (2005). *Information technology -- Security techniques-Code of practice for information security management.*. Geneva, International Organization for Standardization..

ISO/IT (2009). *Information Security Management Guidelines for Telecommunications Organizations Based on ISO.*

IWS (2015). *Internet World Stats.* [Online] Available at: http: www. internetworldstats. Com /starts1.html [Accessed 5 April 2015]

IWS (2015). *List of current* TISPA members:. [Online] Available at: http://www.tix.or.tz /tispa/members.html [Accessed 2 April 2015].

Jackson, M. (2001). *Problem Frames.*Addison Wesley.

Jamieson, R. and Cerpa, N. (2001). *A Research Framework for Risk, Security, Trust and Assurance within an Electronic Commerce Domain.* CACS Conference.

Jerichosystems. (2016). *ABAC (Attribute Based Access Control).* [Online] Available at: www.jerichosystems.com [Accessed 11 07 2016].

Joshi, J., Aref, W., Ghafoor, A. and Spafford, E. H. (2001). Security Model for web based Application. *ACM*, pp. 44(2):38-44.

Koc, C. K., December 2, (1999). *"Next Generation E-Commerce Security" Information Security Laboratory*.

Kuchinskas, S. (2015). *Fraud Chewing E-Commerce Profits.* [Online] Available at: http://www.internetnews.com/ec-news/article.php/3563061

Kvale, S. (1996). *InterViews: An introduction to qualitative research interviewing.* Calfonia: Sage Publication.

Landwehr, C. E. and Carroll, J. M. (1984). *"Hardware Requirements for Secure Computer Systems: A Framework,"*. Oakland, 1984 IEEE Symposium on Security and Privacy.

Maiwald, E. (2008). *Network Security; A beginner's guide.* 3rd ed. Dreamtech press.

Manyika, J. (2013). *Lions go digital: The Internet's transformative potential in Africa.* McKinsey & Company.

Marczyk, R., Dematteo, D. and Festnger, D. (2005). *Essentials of research design and methodology.* s.l.:John Wiley & Sons.

Menezes, P. C. (1996). *Handbook of Applied Cryptography.* CRC Press.

Mills, A. J., Gabrielle, D. and Elden, W. (2010). *Encyclopedia of Case Study Research.* Calfonia: Sage Publication.

Miniwatts (2015). *Tanzania's Internet users hit 9m.* [Online] Available at: http://www.thecitizen.co.tz/News/Business/Tanzania-s-Internet-users-hit-9m/1840414-2254676-120nonw/index.html [Accessed 2 April 2015].

Mlelwa, K. L., Chachage, B. and Yonah, Z. O. (2015). E-Commerce Trend in Developing Countries: A case Study of Tanzania. *International Journal of Computer Applications,* 1(125), pp. 27-33.

Mlelwa, K. L. and Tarimo, C. (2011). *eCommerce Awareness and its impact on the Small Scale Tourism,* Dodoma, Tanzania: Unpublished Dissertation for Award of MSc Degree at UDoM..

Mlelwa, K. L. and Yonah, Z. O. (2017). Requirement's for Proposed Frameworks for Secure Ecommerce Transactions. *Communications on Applied Electronics* , 6(9), pp. 1-15.

Molla, A. and Licker, P. S. (2005). Perceived EReadiness factors in E-Commerce adoption: An empirical investigation in a developing country. *International Journal of Electronic Commerce,* 1(10), pp. 83-110.

Molla, A., Taylor, R. and Licker, S. (2006). Ecommerce Diffusion in Small Island Countries: the Influence of Institution in Barbados.. *The Electronic Journal of Information Systems in Developing Countries,* 28(2), pp. 1-15.

Myers, M. (2009). *Qualitative research in Business Management.* 2nd ed. ISBN: 978-1-4129-2166-4.

Niranjanamurthy M, and Dharmendra, Chahar. (2013) ,"The study of E-Commerce Security Issues and Solutions", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 7, July 2013

NIST. (1995). *An Introduction to Computer Security: The NIST Handbook.* Special Pub SP 800-12 ed. National Institute of Standards and Technology.

NIST. (2006). Minimum Security Requirements for Federal Information and Information Systems. In: *National Institute of Standards and Technology*. Computer Security Division..

NIST. (2014). *Framework for Improving Critical Infrastructure Cybersecurity.*

Noureddine, B. (2010). Security of mobile communications. In: *Boca Raton.* CRC Press, pp. 32-33.

OASIS. (2010). *OASIS Standards and Other Approved Work.* [Online] Available at: http://www.oasis-open.org/specs/[Accessed on 15 June 2016].

OECD. (2002). *OECD Guidelines for the Security of Information Systems and Networks.* [Online] Available at: http://www.oecd.org/dataoecd/16/22/15582260.pd f[Accessed 13 June 2016].

Ogundeji, O. A. (2014). *E-commerce becomes a force in African retail market.* [Online] Available at: http://www.pcworld.com/article/2855252/ecommerce-becomes-a-force-in-african-retail-market.html [Accessed 9 March 2015].

O'Mahony, D., Peirce, M. and Tewari, H. (2001). *Electronic Payment System for E-Commerce.* Artech House Publisher.

Onieva, J. A. (2008). Multiparty Nonrepudiation: A Survey. *ACM Computing Surveys,* 41(1,5), pp. 5.1-5.42.

Pfleeger, C. P. and Pfleeger, S. L. (2002). *Security in Computing,* Prentice Hall.

Robert, O. (2010). *China's migration to eCommerce,* Forbes.

Robert, Y. K. (2014). *Case Study Research: Design and Methods.* 5th ed. Calfonia: Sage Publication.

Robinson, J. (2010). *UK's internet industry worth £100bn.* [Online] [Accessed 21 December 2015].

Saunders, M., Lewis, P. and Thornhill, A. (2007). *Research Methods for Business Students,*. 4th ed. Harlow: Pearson Education.

Semeijn, J. (2005). E-services and offline fulfillment: How e-loyalty is created. *Managing Service Quality,* 2(15(2): 182-194).

Shelly, G. (2002). *Systems analysis and design.* p.10.ISBN 0-538-47443-2 ed. Boston: Cengage Learning.

Sheth, J. N. and Sharma, A. (2005). International emarketing: Opportunities and issues. *Internetional Marketing Review,* 6(22), pp. 611-622.

Siponen, M. and Willison, R. (2009). Information security management standards: Problems and solutions.. *Information & Management* , Volume 46, pp. 267 - 270.

Stallings, W. (2003). *Cryptography and Network Security.* 3rd ed.

Steven, M. (2014). *Here are all the must-see numbers on Alibaba ahead of record-breaking IPO,* Tech in Asia.

Taghavi, Z. and Saman. (2013). *A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks.* [Online] [Accessed 2 July 2016].

Talleur, T. (2000). *E-Commerce and Cybercrime. A Business Forum.*

Tanzania Ministry of Works, Transport and Communication (2016). *National Information and Communications Technology Policy Report*. Government Printer, Dodoma, Tanzania. 09 pp.

Travica, B. (2002). Diffusion of electronic commerce in developing countries: The case of Costa Rica. *Journal of Global Information Technology Management,* 1(5), pp. 4-24.

Vahradsky, K. (2012). Cloud risk: 10 principals and a framework for assessment. *ISACA,* Volume 5, pp. 1-12.

W3C. (2004). *Web Services Glossary.* [Online] Available at: http://www.w3.org/TR/ws-gloss/[Accessed 15 July 2016].

Wanjau, K., Macharia, R. and Ayodo, E. (2012). Factors Affecting Adoption of Electronic Commerce among Small Medium Enterprises in Kenya: Survey of Tour and Travel Firms in Nairobi. *International Journal of Business, Humanities and Technology,* 2(4), p. 76.

Weik, M. (2001). Computer Science and Communication Dictionary. *Springer.*

Wendy, C. (2000). *The Global information Society.* Chichester: John Wiley & Sons Ltd.

WHO. (2013). *E-commerce in developing countries: Opportunities and challenges for small and medium- sized enterprises.,* s.n.

Wright, X. a. P. (2003). E-Commercializing Business Operations. *Communication of ACM,* Feburary, Volume vol.46. , pp. pp 83-87.

yStart.com. (2013). *Africa B2C e-commerce report 2013,* yStart.com.

Zhiguang, Q. L. (2004). A survey of E-commerce Security. *Electronic Science and Technology of China* , 2(3).

APPENDICES

Appendix 1: Introduction Letter

Kenneth L. Mlelwa
P.O. Box 9193
Dar es Salaam
Tanzania

Dear Sir/Madam,

I am undertaking a PhD research project to develop a novel framework for secure eCommerce Transactions. To this end, I kindly request you to complete the following short questionnaire. It should take no longer than 15 minutes of your time.

The information provided by you shall remain confidential and shall be reported in summary format only.

Please return the completed questionnaire to me by email (mlelwak@nm-aist.ac.tz) or to the person who handed it to you.

Should you have any queries or comments regarding this questionnaire, please contact by phone on +255 713 227455 or email: kennethmlelwa@gmail.com.

Yours sincerely

Kenneth L. Mlelwa

PhD Student

Appendix 2: Questionnaire

1) Are you...? (*Mark only one oval)*

- ○ Male
- ○ Female

2) Your age... (*Mark only one oval.)*

- ○ 18 - 25 years
- ○ 26 - 30 Years
- ○ 31 - 40 Years
- ○ 41 - 60 Years
- ○ Over 60 Years

3) Your level of education (*Mark only one oval.)*

- ○ Secondary School or below?
- ○ College certificate/Diploma
- ○ Bachelor's
- ○ Masters or Above

4) What is your attitude towards purchasing goods/ services over internet? (*Mark only one oval.)*

- ○ Positive
- ○ Negative
- ○ No Opinion

5) What are the main barriers which keep you away from shopping online? (*Mark only one oval.)*

- ○ Safety of payment
- ○ Low trust level of online store / Brand
- ○ Value added tax customs / Customs duty
- ○ High Shipping cost Refund Policy Warranty and Claims Delivery too Slow
- ○ Other:

6) What products do you normally purchase online? (*You can select more than 1*)

- ○ Books

- ○ Electronics goods (Mobile phones, laptop, camera etc)
- ○ Clothes
- ○ Music, Software
- ○ Other:

7) For how long have you been shopping online? (*Mark only one oval).*

- ○ Less than a year
- ○ One to three years
- ○ More than three years

8) Main Reason for online Shopping? (*Mark only one oval).*

- ○ Price
- ○ Convenient & Time saving
- ○ Fast Shipping
- ○ Trust
- ○ Brand conscious
- ○ Friend Referral

9) Do you go to a retail store first before making your final purchase online? (*Mark only one oval).*

- ○ Yes
- ○ No

A) SECURITY AND PRIVACY

10) How do you rate security and reliability of the payment systems? (*Mark only one oval).*

- ○ Not important at all
- ○ Less important
- ○ Pretty important
- ○ Important
- ○ Very important
- ○ No opinion

11) How do you rate about information on how security work? (*Mark only one oval).*

- ○ Not important at all

- ○ Less important
- ○ Pretty important
- ○ Important
- ○ Very important
- ○ No opinion

12) How do you rate the knowledge of your personal information that you fill when ordering is handled? (*Mark only one oval)*

- ○ Not important at all
- ○ Less important
- ○ Pretty important
- ○ Very important
- ○ No opinion

B) GUARANTEE AND CUSTOMER SERVICES

13) How do you rate standard terms in connection to the order form? (*Mark only one oval.)*

- ○ Not important at all
- ○ Less important
- ○ Pretty important
- ○ Important
- ○ Very important
- ○ No opinion

14) How do rate about the confirmation on the order and purchase? (*Mark only one oval.)*

- ○ Not important at all
- ○ Less important
- ○ Pretty important
- ○ Important
- ○ Very important
- ○ No opinion

15) How do you rate the possibilities of asking question and getting help directly online or by telephone? (*Mark only one ova*)

- ○ Not important at all
- ○ Less important
- ○ Pretty important
- ○ Important
- ○ Very important
- ○ No opinion

C) WEBSITE AND BRAND

16) How do you rate the Product's brand? (*Mark only one oval.)*

- ○ Not important at all
- ○ Less important
- ○ Pretty important
- ○ Important
- ○ Very important
- ○ No opinion

17) How do you rate reputation and recommendations? (For example, in media, family or friends) *Mark only one oval.*

- ○ Not important at all
- ○ Less important
- ○ Pretty important
- ○ Important
- ○ Very important
- ○ No opinion

18) How do you rate the design and functionality of the website? (*How the website looks like*)

Mark only one oval.

- ○ Not important at all
- ○ Less important
- ○ Pretty important
- ○ Important
- ○ Very important

- ○ No opinion
- ○ Control and Price

19) How do you rate about the convenient with using internet and the technology? (*Mark only one oval.)*

- ○ Not important at all
- ○ Less important
- ○ Pretty important
- ○ Important
- ○ Very important
- ○ No opinion

20) How do you rate the price of the product and/or service? (*Mark only one oval.)*

- ○ Not important at all
- ○ Less important
- ○ Pretty important
- ○ Important
- ○ Very important
- ○ No opinion

Appendix 3: Code for Security Plug-in Using WS-Security for Case Study Transaction

The following are three files for Security-Plugin used to implement a secure framework for the eCommerce transaction described in the case study in chapter five.

i) Index File

```
<?php require_once('src/token.php');
require('src/connection.php');
require('src/ciphering.php');
require('src/deciphering.php');
require('src/security.php');
require('src/insertion.php');
?>
<!doctype html>
<html lang="en-US">
	<head>
		<!-- Meta tags & title /-->
			<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
			<meta name="viewport" content="width=device-width, initial-scale=1, maximum-
		scale=1">
			<meta name="robots" content="all,index,follow" />
			<title>security plugin</title>
			<meta name="description" content="Create a sticky navigation bar that remains
		fixed to the top after scroll" />
			<link rel="stylesheet" type="text/css" href="css/styles.css" /> <!-- Main stylesheet /--
		>
			<script src='js/getting_ready.js'></script>
			<script src='js/encrypt_decrypt.js'></script>
	</head>
	<body>
		<section id="screen">
		<div class='main_'><br/><br/><br/>
		<?php
		 if(isset($_GET['val']))
		 {	$clk= $_GET['val'];
		    if($clk=='customer')
			{		require_once('src/customer.php');
			}
			else
			{		require_once('src/merchant.php');
			}
		 }
		?>
		</div>
		   <nav >
			<ul>
					<li><a href="index.php?val=customer"><button
		style='width:250px;text-align:left;color:#000000;height:35px;text-
		align:center;'>customer</button></a></li>
					<li style='width:50px;text-align:left;color:#000000;'></li>
					<li><a href="index.php?val=merchant"><button
		style='width:250px;text-align:left;color:#000000;height:35px;text-
		align:center;'>merchant</button></a></li>
				</ul>
		</nav>
```

```
                </section>
        </body>
</html>
```

ii) CSS File

```
* {margin:0px; padding: 0;}
a {text-decoration: none;}
/* This class is added on scroll */

.main_ {    width:850px;background:#F000;color:#000000;height:384px;  }
#logo {                 height:150px;width:150px;float:right;                                   }
body {              color: #fff;font-family: 'open-sans-bold'; font-size: 20px;text-align: center;
            }
nav {       width: 840px;
                        position: absolute; top:15px; height: 45px; z-index: 1;background:#C0C0C0;box-
                        shadow:0 0 0 4px;                                   }
nav li {    display: inline-block;
                        padding: 5px 0px;                                                                   }
nav li a {  color: #757575;
                        text-transform: uppercase;                                                          }
section {   height: 100vh;
            }
/* Screens Settings */
#screen {
                        background:url("../imgs/_1.png") left no-repeat transparent;width:100%;margin-
                        left:15%;                               }
```

iii) Security File

```
import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;
import org.apache.commons.codec.binary.Base64;
public class Security {
            public static String encrypt(String input, String key){
              byte[] crypted = null;
              try{
                SecretKeySpec skey = new SecretKeySpec(key.getBytes(), "AES");
                  Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
                  cipher.init(Cipher.ENCRYPT_MODE, skey);
                  crypted = cipher.doFinal(input.getBytes());
                }catch(Exception e){
                        System.out.println(e.toString());
                }
                return new String(Base64.encodeBase64(crypted));
            }
            public static String decrypt(String input, String key){
                byte[] output = null;
                try{
                  SecretKeySpec skey = new SecretKeySpec(key.getBytes(), "AES");
                  Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
                  cipher.init(Cipher.DECRYPT_MODE, skey);
                  output = cipher.doFinal(Base64.decodeBase64(input));
                }catch(Exception e){
                  System.out.println(e.toString());
                }
                return new String(output);
            }
              public static void main(String[] args) {
```

```
            String key = "1234567891234567";
            String data = "example";
System.out.println(Security.decrypt(Security.encrypt(data, key), key));
            System.out.println(Security.encrypt(data, key));
          }
}
```

iv) encrypt_decrypt File

```
Combine bytes of each col of state S [§5.1.3]
 * @private
 */
Aes.mixColumns = function(s, Nb) {
  for (var c=0; c<4; c++) {
  var a = new Array(4);  // 'a' is a copy of the current column from 's'
    var b = new Array(4);  // 'b' is a•{02} in GF(2^8)
    for (var i=0; i<4; i++) {
      a[i] = s[i][c];
      b[i] = s[i][c]&0x80 ? s[i][c]<<1 ^ 0x011b : s[i][c]<<1;
    }
    // a[n] ^ b[n] is a•{03} in GF(2^8)
  s[0][c] = b[0] ^ a[1] ^ b[1] ^ a[2] ^ a[3]; // {02}•a0 + {03}•a1 + a2 + a3
  s[1][c] = a[0] ^ b[1] ^ a[2] ^ b[2] ^ a[3]; // a0 • {02}•a1 + {03}•a2 + a3
  s[2][c] = a[0] ^ a[1] ^ b[2] ^ a[3] ^ b[3]; // a0 + a1 + {02}•a2 + {03}•a3
  s[3][c] = a[0] ^ b[0] ^ a[1] ^ a[2] ^ b[3]; // {03}•a0 + a1 + a2 + {02}•a3
  }
  return s;
};
/**
 * Xor Round Key into state S [§5.1.4]
 * @private
 */
Aes.addRoundKey = function(state, w, rnd, Nb) {
  for (var r=0; r<4; r++) {
    for (var c=0; c<Nb; c++) state[r][c] ^= w[rnd*4+c][r];
  }
  return state;
};
/**
 * Apply SBox to 4-byte word w
 * @private
 */
Aes.subWord = function(w) {
  for (var i=0; i<4; i++) w[i] = Aes.sBox[w[i]];
  return w;
};
/**
 * Rotate 4-byte word w left by one byte
 * @private
 */
Aes.rotWord = function(w) {
  var tmp = w[0];
  for (var i=0; i<3; i++) w[i] = w[i+1];
  w[3] = tmp;
  return w;
};
// sBox is pre-computed multiplicative inverse in GF(2^8) used in subBytes and keyExpansion [§5.1.1]
```

```
Aes.sBox =  [0x63,0x7c,0x77,0x7b,0xf2,0x6b,0x6f,0xc5,0x30,0x01,0x67,0x2b,0xfe,0xd7,0xab,
0xca,0x82,0xc9,0x7d,0xfa,0x59,0x47,0xf0,0xad,0xd4,0xa2,0xaf,0x9c,0xa4,0x72,
/* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - */
/* AES implementation in JavaScript                    (c) Chris Veness 2005-2016
/*   MIT Licence                                                                  */
/* www.movable-type.co.uk/scripts/aes.html                                        */
/* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - */
/* eslint no-redeclare: 0 */
'use strict';
/**
 * AES (Rijndael cipher) encryption routines,
 * Reference implementation of FIPS-197 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
 * @namespace                                                                     */
var Aes = {};
/**
 * AES Cipher function: encrypt 'input' state with Rijndael algorithm [§5.1];
 *   applies Nr rounds (10/12/14) using key schedule w for 'add round key' stage.
 * @param   {number[]}   input - 16-byte (128-bit) input state array.
 * @param   {number[][]} w - Key schedule as 2D byte-array (Nr+1 x Nb bytes).
 * @returns {number[]}   Encrypted output state array.
 */
Aes.cipher = function(input, w) {
   var Nb = 4;               // block size (in words): no of columns in state (fixed at 4 for AES)
var Nr = w.length/Nb - 1; // no of rounds: 10/12/14 for 128/192/256-bit keys
   var state = [[],[],[],[]];  // initialise 4xNb byte-array 'state' with input [§3.4]
   for (var i=0; i<4*Nb; i++) state[i%4][Math.floor(i/4)] = input[i];
   state = Aes.addRoundKey(state, w, 0, Nb);
   for (var round=1; round<Nr; round++) {
      state = Aes.subBytes(state, Nb);
      state = Aes.shiftRows(state, Nb);
      state = Aes.mixColumns(state, Nb);
      state = Aes.addRoundKey(state, w, round, Nb);
   }
   state = Aes.subBytes(state, Nb);
   state = Aes.shiftRows(state, Nb);
   state = Aes.addRoundKey(state, w, Nr, Nb);
   var output = new Array(4*Nb);  // convert state to 1-d array before returning [§3.4]
   for (var i=0; i<4*Nb; i++) output[i] = state[i%4][Math.floor(i/4)];
   return output;
};
/**
 * Perform key expansion to generate a key schedule from a cipher key [§5.2].
 * @param   {number[]}   key - Cipher key as 16/24/32-byte array.
 * @returns {number[][]} Expanded key schedule as 2D byte-array (Nr+1 x Nb bytes).
 */
Aes.keyExpansion = function(key) {
   var Nb = 4;            // block size (in words): no of columns in state (fixed at 4 for AES)
var Nk = key.length/4; // key length (in words): 4/6/8 for 128/192/256-bit keys
  var Nr = Nk + 6;       // no of rounds: 10/12/14 for 128/192/256-bit keys
   var w = new Array(Nb*(Nr+1));
   var temp = new Array(4);
   // initialise first Nk words of expanded key with cipher key
   for (var i=0; i<Nk; i++) {
      var r = [key[4*i], key[4*i+1], key[4*i+2], key[4*i+3]];
      w[i] = r;
   }
   // expand the key into the remainder of the schedule
```

```
    for (var i=Nk; i<(Nb*(Nr+1)); i++) {
      w[i] = new Array(4);
      for (var t=0; t<4; t++) temp[t] = w[i-1][t];
      // each Nk'th word has extra transformation
      if (i % Nk == 0) {
        temp = Aes.subWord(Aes.rotWord(temp));
        for (var t=0; t<4; t++) temp[t] ^= Aes.rCon[i/Nk][t];
      }
      // 256-bit key has subWord applied every 4th word
      else if (Nk > 6 && i%Nk == 4) {
        temp = Aes.subWord(temp);
      }
      // xor w[i] with w[i-1] and w[i-Nk]
      for (var t=0; t<4; t++) w[i][t] = w[i-Nk][t] ^ temp[t];
    }
    return w;
};

/**
 * Apply SBox to state S [§5.1.1]
 * @private                */
Aes.subBytes = function(s, Nb) {
    for (var r=0; r<4; r++) {
      for (var c=0; c<Nb; c++) s[r][c] = Aes.sBox[s[r][c]];
    }
    return s;
};
/**
 * Shift row r of state S left by r bytes [§5.1.2]
 * @private
 */
Aes.shiftRows = function(s, Nb) {
    var t = new Array(4);
    for (var r=1; r<4; r++) {
    for (var c=0; c<4; c++) t[c] = s[r][(c+r)%Nb];  // shift into temp copy
        for (var c=0; c<4; c++) s[r][c] = t[c];         // and copy back
  }// note that this will work for Nb=4,5,6, but not 7,8 (always 4 for AES):
    return s;  // see asmaes.sourceforge.net/rijndael/rijndaelImplementation.pdf
};
/**
 *       0xb7,0xfd,0x93,0x26,0x36,0x3f,0xf7,0xcc,0x34,0xa5,0xe5,0xf1,0x71,0xd8,0x31,
0x04,0xc7,0x23,0xc3,0x18,0x96,0x05,0x9a,0x07,0x12,0x80,0xe2,0xeb,0x27,0xb2,
0x09,0x83,0x2c,0x1a,0x1b,0x6e,0x5a,0xa0,0x52,0x3b,0xd6,0xb3,0x29,0xe3,0x2f,
0x53,0xd1,0x00,0xed,0x20,0xfc,0xb1,0x5b,0x6a,0xcb,0xbe,0x39,0x4a,0x4c,0x58,
0xd0,0xef,0xaa,0xfb,0x43,0x4d,0x33,0x85,0x45,0xf9,0x02,0x7f,0x50,0x3c,0x9f,
0x51,0xa3,0x40,0x8f,0x92,0x9d,0x38,0xf5,0xbc,0xb6,0xda,0x21,0x10,0xff,0xf3,
0xe0,0x32,0x3a,0x0a,0x49,0x06,0x24,0x5c,0xc2,0xd3,0xac,0x62,0x91,0x95,0xe4,
0xe7,0xc8,0x37,0x6d,0x8d,0xd5,0x4e,0xa9,0x6c,0x56,0xf4,0xea,0x65,0x7a,0xae,
0xba,0x78,0x25,0x2e,0x1c,0xa6,0xb4,0xc6,0xe8,0xdd,0x74,0x1f,0x4b,0xbd,0x8b,
0x70,0x3e,0xb5,0x66,0x48,0x03,0xf6,0x0e,0x61,0x35,0x57,0xb9,0x86,0xc1,0x1d,
0xe1,0xf8,0x98,0x11,0x69,0xd9,0x8e,0x94,0x9b,0x1e,0x87,0xe9,0xce,0x55,0x28,
0x8c,0xa1,0x89,0x0d,0xbf,0xe6,0x42,0x68,0x41,0x99,0x2d,0x0f,0xb0,0x54,0xbb,
// rCon is Round Constant used for the Key Expansion [1st col is 2^(r-1) in GF(2^8)] [§5.2]
Aes.rCon = [ [0x00, 0x00, 0x00, 0x00],
             [0x01, 0x00, 0x00, 0x00],
             [0x02, 0x00, 0x00, 0x00],
             [0x04, 0x00, 0x00, 0x00],
```

```
            [0x08, 0x00, 0x00, 0x00],
            [0x10, 0x00, 0x00, 0x00],
            [0x40, 0x00, 0x00, 0x00],
            [0x80, 0x00, 0x00, 0x00],
            [0x1b, 0x00, 0x00, 0x00],
            [0x36, 0x00, 0x00, 0x00] ];
/* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - */
if (typeof module != 'undefined' && module.exports) module.exports = Aes; // ≡ export default Aes
/* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - */
/*        MIT Licence  */                                                  /* www.movable-
type.co.uk/scripts/aes.html                                               */
/* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - */
/* eslint no-redeclare: 0 *//* global WorkerGlobalScope */
'use strict';
if (typeof module!='undefined' && module.exports) var Aes = require('./aes.js'); // ≡ import Aes from
'aes.js'
/**
 * Aes.Ctr: Counter-mode (CTR) wrapper for AES.
 * This encrypts a Unicode string to produces a base64 ciphertext using 128/192/256-bit AES,
 * and the converse to decrypt an encrypted ciphertext.
 * See http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
 * @augments Aes
 */
Aes.Ctr = {};
/**
 * Encrypt a text using AES encryption in Counter mode of operation.
 * Unicode multi-byte character safe
 * @param   {string} plaintext - Source text to be encrypted.
 * @param   {string} password - The password to use to generate a key for encryption.
 * @param   {number} nBits - Number of bits to be used in the key; 128 / 192 / 256.
 * @returns {string} Encrypted text.
 * @example
 * var encr = Aes.Ctr.encrypt('big secret', 'pāşšŵōřđ', 256); // 'lwGl66VVwVObKIr6of8HVqJr'
 */
Aes.Ctr.encrypt = function(plaintext, password, nBits) {
  var blockSize = 16;  // block size fixed at 16 bytes / 128 bits (Nb=4) for AES
    if (!(nBits==128 || nBits==192 || nBits==256)) throw new Error('Key size is not 128 / 192 / 256');
    plaintext = String(plaintext).utf8Encode();
    password = String(password).utf8Encode();
    // use AES itself to encrypt password to get cipher key (using plain password as source for key
    // expansion) - gives us well encrypted key (though hashed key might be preferred for prod'n use)
    var nBytes = nBits/8;  // no bytes in key (16/24/32)
    var pwBytes = new Array(nBytes);
    for (var i=0; i<nBytes; i++) {  // use 1st 16/24/32 chars of password for key
    pwBytes[i] = i<password.length ?  password.charCodeAt(i) : 0;     }
    var key = Aes.cipher(pwBytes, Aes.keyExpansion(pwBytes)); // gives us 16-byte key
key = key.concat(key.slice(0, nBytes-16));  // expand key to 16/24/32 bytes long
    // initialise 1st 8 bytes of counter block with nonce (NIST SP800-38A §B.2): [0-1] = millisec,
    // [2-3] = random, [4-7] = seconds, together giving full sub-millisec uniqueness up to Feb 2106
    var counterBlock = new Array(blockSize);
var nonce = (new Date()).getTime();  // timestamp: milliseconds since 1-Jan-1970
    var nonceMs = nonce%1000;
    var nonceSec = Math.floor(nonce/1000);
    var nonceRnd = Math.floor(Math.random()*0xffff);
    // for debugging: nonce = nonceMs = nonceSec = nonceRnd = 0;
    for (var i=0; i<2; i++) counterBlock[i]   = (nonceMs  >>> i*8) & 0xff;
    for (var i=0; i<2; i++) counterBlock[i+2] = (nonceRnd >>> i*8) & 0xff;
    for (var i=0; i<4; i++) counterBlock[i+4] = (nonceSec >>> i*8) & 0xff;
```

```
    // and convert it to a string to go on the front of the ciphertext
    var ctrTxt = '';
    for (var i=0; i<8; i++) ctrTxt += String.fromCharCode(counterBlock[i]);
    // generate key schedule - an expansion of the key into distinct Key Rounds for each round
    var keySchedule = Aes.keyExpansion(key);
    var blockCount = Math.ceil(plaintext.length/blockSize);
    var ciphertext = '';
    for (var b=0; b<blockCount; b++) {
      // set counter (block #) in last 8 bytes of counter block (leaving nonce in 1st 8 bytes)
      // done in two stages for 32-bit ops: using two words allows us to go past 2^32 blocks (68GB)
    for (var c=0; c<4; c++) counterBlock[15-c] = (b >>> c*8) & 0xff;
    for (var c=0; c<4; c++) counterBlock[15-c-4] = (b/0x100000000 >>> c*8);
      var cipherCntr = Aes.cipher(counterBlock, keySchedule);  // -- encrypt counter block --
      // block size is reduced on final block
      var blockLength = b<blockCount-1 ? blockSize : (plaintext.length-1)%blockSize+1;
      var cipherChar = new Array(blockLength);
      for (var i=0; i<blockLength; i++) {
        // -- xor plaintext with ciphered counter char-by-char --
        cipherChar[i] = cipherCntr[i] ^ plaintext.charCodeAt(b*blockSize+i);
        cipherChar[i] = String.fromCharCode(cipherChar[i]);       }
      ciphertext += cipherChar.join('');
      // if within web worker, announce progress every 1000 blocks (roughly every 50ms)
      if (typeof WorkerGlobalScope != 'undefined' && self instanceof WorkerGlobalScope) {
        if (b%1000 == 0) self.postMessage({ progress: b/blockCount });
      }
    }
    ciphertext =  (ctrTxt+ciphertext).base64Encode();
    return ciphertext;                                                                  };
/**
 * Decrypt a text encrypted by AES in counter mode of operation
 * @param   {string} ciphertext - Cipher text to be decrypted.
 * @param   {string} password - Password to use to generate a key for decryption.
 * @param   {number} nBits - Number of bits to be used in the key; 128 / 192 / 256.
 * @returns {string} Decrypted text
 * @example
 *   var decr = Aes.Ctr.decrypt('lwGl66VVwVObKIr6of8HVqJr', 'pāşšŵōřđ', 256); // 'big secret'
 */
Aes.Ctr.decrypt = function(ciphertext, password, nBits) {
    var blockSize = 16;  // block size fixed at 16 bytes / 128 bits (Nb=4) for AES
    if (!(nBits==128 || nBits==192 || nBits==256)) throw new Error('Key size is not 128 / 192 / 256');
    ciphertext = String(ciphertext).base64Decode();
    password = String(password).utf8Encode();
    // use AES to encrypt password (mirroring encrypt routine)
    var nBytes = nBits/8;  // no bytes in key
    var pwBytes = new Array(nBytes);
    for (var i=0; i<nBytes; i++) {
      pwBytes[i] = i<password.length ?  password.charCodeAt(i) : 0;    }
    var key = Aes.cipher(pwBytes, Aes.keyExpansion(pwBytes));
    key = key.concat(key.slice(0, nBytes-16));  // expand key to 16/24/32 bytes long
    // recover nonce from 1st 8 bytes of ciphertext
    var counterBlock = new Array(8);
    var ctrTxt = ciphertext.slice(0, 8);
    for (var i=0; i<8; i++) counterBlock[i] = ctrTxt.charCodeAt(i);
    // generate key schedule
    var keySchedule = Aes.keyExpansion(key);
    // separate ciphertext into blocks (skipping past initial 8 bytes)
    var nBlocks = Math.ceil((ciphertext.length-8) / blockSize);
```

```
    var ct = new Array(nBlocks);
    for (var b=0; b<nBlocks; b++) ct[b] = ciphertext.slice(8+b*blockSize, 8+b*blockSize+blockSize);
    ciphertext = ct;  // ciphertext is now array of block-length strings
    // plaintext will get generated block-by-block into array of block-length strings
    var plaintext = '';
    for (var b=0; b<nBlocks; b++) {
        // set counter (block #) in last 8 bytes of counter block (leaving nonce in 1st 8 bytes)
        for (var c=0; c<4; c++) counterBlock[15-c] = ((b) >>> c*8) & 0xff;
        for (var c=0; c<4; c++) counterBlock[15-c-4] = (((b+1)/0x100000000-1) >>> c*8) & 0xff;
       var cipherCntr = Aes.cipher(counterBlock, keySchedule);  // encrypt counter block
        var plaintxtByte = new Array(ciphertext[b].length);
        for (var i=0; i<ciphertext[b].length; i++) {
            // -- xor plaintext with ciphered counter byte-by-byte --
            plaintxtByte[i] = cipherCntr[i] ^ ciphertext[b].charCodeAt(i);
            plaintxtByte[i] = String.fromCharCode(plaintxtByte[i]);       }
        plaintext += plaintxtByte.join('');
        // if within web worker, announce progress every 1000 blocks (roughly every 50ms)
        if (typeof WorkerGlobalScope != 'undefined' && self instanceof WorkerGlobalScope) {
            if (b%1000 == 0) self.postMessage({ progress: b/nBlocks });
        }
    }
    plaintext = plaintext.utf8Decode();  // decode from UTF8 back to Unicode multi-byte chars
    return plaintext;                                                                    };
/* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*/
/* Extend String object with method to encode multi-byte string to utf8
 * - monsur.hossa.in/2012/07/20/utf-8-in-javascript.html
 * - note utf8Encode is an identity function with 7-bit ascii strings, but not with 8-bit strings;
 * - utf8Encode('x') = 'x', but utf8Encode('ça') = 'Ã§a', and utf8Encode('Ã§a') = 'ÃƒÂ§a'*/
if (typeof String.prototype.utf8Encode == 'undefined') {
    String.prototype.utf8Encode = function() {
        return unescape( encodeURIComponent( this ) );                    };
}
/* Extend String object with method to decode utf8 string to multi-byte */
if (typeof String.prototype.utf8Decode == 'undefined') {
    String.prototype.utf8Decode = function() {
        try {
            return decodeURIComponent( escape( this ) );
        } catch (e) {
            return this; // invalid UTF-8? return as-is                  }
    };
}
/* Extend String object with method to encode base64
 * - developer.mozilla.org/en-US/docs/Web/API/window.btoa, nodejs.org/api/buffer.html
 * - note: btoa & Buffer/binary work on single-byte Unicode (C0/C1), so ok for utf8 strings, not for general
Unicode...
 * - note: if btoa()/atob() are not available (eg IE9-), try github.com/davidchambers/Base64.js */
if (typeof String.prototype.base64Encode == 'undefined') {
    String.prototype.base64Encode = function() {
        if (typeof btoa != 'undefined') return btoa(this); // browser
        if (typeof Buffer != 'undefined') return new Buffer(this, 'binary').toString('base64'); // Node.js
        throw new Error('No Base64 Encode');
    };
}
/* Extend String object with method to decode base64 */
if (typeof String.prototype.base64Decode == 'undefined') {
    String.prototype.base64Decode = function() {
        if (typeof atob != 'undefined') return atob(this); // browser
```

```
        if (typeof Buffer != 'undefined') return new Buffer(this, 'base64').toString('binary'); // Node.js
        throw new Error('No Base64 Decode');
    };
}
/* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*/if (typeof module != 'undefined' &&
module.exports) module.exports = Aes.Ctr;
/* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*//*  Web worker to encrypt/decrypt files using AES
counter-mode            (c) Chris Veness 2016
/*   MIT Licence                                                                                                          */
/* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*/
importScripts('js/addons/aes.js');
importScripts('js/addons/aes-ctr.js');
/**
 * Web worker to encrypt/decrypt files using AES counter-mode.
 * @param {string} msg.data.op - 'encrypt' or 'decrypt'.
 * @param {File}   msg.data.file - File to be encrypted or decrypted.
 * @param {string} msg.data.password - Password to use to encrypt/decrypt file.
 * @param {number} msg.data.bits - Number of bits to use for key.
 * @returns {ciphertext|plaintext} - Blob containing encrypted ciphertext / decrypted plaintext.
 * @example
 *   var worker = new Worker('aes-ctr-file-webworker.js');
 *   var file = this.files[0];
 *   worker.postMessage({ op:'encrypt', file:file, password:'L0ck it up ŝaf3', bits:256 });
 *   worker.onmessage = function(msg) {
 *     if (msg.data.progress != 'complete') {
 *       $('progress').val(msg.data.progress * 100); // update progress bar
 *     }
 *     if (msg.data.progress == 'complete') {
 *       saveAs(msg.data.ciphertext, file.name+'.encrypted'); // save encrypted file
 *     }
 *   }
 * Note saveAs() cannot run in web worker, so encrypted/decrypted file has to be passed back to UI
 * thread to be saved.
 * TODO: error handling on failed decryption
 */
onmessage = function(msg) {
    switch (msg.data.op) {
        case 'encrypt':
            var reader = new FileReaderSync();
            var plaintext = reader.readAsText(msg.data.file, 'utf-8');
            var ciphertext = Aes.Ctr.encrypt(plaintext, msg.data.password, msg.data.bits);
           // return encrypted file as Blob; UI thread can then use saveAs()
            var blob = new Blob([ciphertext], { type: 'text/plain' });
            self.postMessage({ progress: 'complete', ciphertext: blob });
            break;
        case 'decrypt':
            var reader = new FileReaderSync();
            var ciphertext = reader.readAsText(msg.data.file, 'iso-8859-1');
            var plaintext = Aes.Ctr.decrypt(ciphertext, msg.data.password, msg.data.bits);
    // return decrypted file as Blob; UI thread can then use saveAs()
     var blob = new Blob([plaintext], { type: 'application/octet-stream' });
            self.postMessage({ progress: 'complete', plaintext: blob });
            break;
    }
};
```