Securing E-Commerce: Methods and Models in E-Transactions

SENIOR THESIS

Prepared in partial fulfilment of the requirements for

CSC 4387 Computer Science Senior Seminar

Dr. Elva J. Jones, Research Advisor

By

Derrick Murphy II

Option

Information Security

November 9, 2017

Computer Science Department

Winston Salem State University

Winston-Salem, NC

Securing E-Commerce: Methods and Models in E-Transactions

TABLE OF CONTENTS

PAGE

LIST OF ILLUSTRATIONS II

ABSTRACT III

INTRODUCTION 1

CHAPTER

1. LITERATURE REVIEW
   1. Electronic Commerce 2
      1. E-commerce Infrastructure 2
      2. Digital Cash 4
   2. Computing / Technology Policy 6
      1. Transborder data flow 6
      2. Government technology policy 7
   3. Security and Privacy 8
      1. Security Services 8
      2. Software and Application Security 10
   4. Statistical Analysis Methods 12
      1. Descriptive Statistics 12
      2. Hypothesis Test Statistics 13
2. RESEARCH DESIGN
   1. Research Objectives 13
      1. Research Problem 14
      2. Variables and Hypotheses 14
      3. Related Work 14
   2. Experiment Design 15
      1. Experiment Description 15
      2. Data Collection Design 16
   3. Data Analysis Design 17
      1. Descriptive Statistics Design 17
      2. Hypothesis Test Statistics Design 18
3. RESEARCH FINDINGS
   1. Experiment Results 19
      1. Materials and Procedures 19
      2. Comparison to Related Work 19
   2. Data Analysis Results 20
      1. Descriptive Data Analysis 20
      2. Hypothesis Test Data Analysis 20
   3. Discussion Findings 20
4. CONCLUSIONS
   1. Conclusions 21
   2. Implications for Future Research 21
5. BIBLIOGRAPHY 22
6. APPENDICES 23
7. ACKNOWLEDGEMENTS 24

LIST OF ILLISTRATIONS

PAGE

1. Figure 1 (Schema of Prototype) 3
2. Figure 2 (Sample of Website Application) 4
3. Figure 3 (Sample enterprise vulnerability topology) 9
4. Figure 4 (Sample scoring of online selling) 10
5. Figure 5 (Timeline of coin’s lifetime) 11
6. Figure 6 (Clustered Column Descriptive Statistics) 12
7. Figure 7 (Hypothesis Test) 13
8. Figure 8 (Experiment Flowchart) 15
9. Figure 9 (Data Collection) 16
10. Figure 10 (Scatter Plot Descriptive Statistics) 17
11. Figure 11 (Hypothesis Test Statistics Design) 18
12. Figure 12 (Java Breach Simulation) 19

ABSTRACT

In this paper the topic of Electric Commerce was researched extensively (e-commerce). E-Commerce is defined as commercial transactions conducted electronically on the internet. The explanation of e-commerce in this paper has been introduced encompassing six specific topics of the broader space. These are E-Commerce Infrastructure, Digital Cash, Transborder Data flow, Government Technology Policy, Security Services, and Software and Application Security. The research uncovered implemented e-commerce systems used by farmers in Africa, form of digital currency being tested, the process of international movement of information, e-government regulations regarding technology, monitoring systems to calculate enterprise vulnerability, and safe and low cost micropayment schemes.

Introduction

Securing electronic commerce has become an increasing issue as new applications and internet based infrastructures are manufactured. As new technologies are on the rise so are security exploits in relation. A simple violation could be just a mailing address being discovered or larger than the breaching of a network with thousands of clients’ sensitive information. All electronic data you send, read, and receive involve a risk. When the dependency on technology raises so does the volume of risk. Causing the strain for all-inclusive security programs and network security jobs more difficult.

New Internet security exposures revealed almost daily. These findings can be credited to failings in software or the result of software configuration errors. These weaknesses can be exploited by hackers and malicious persons to gain entree to the system.

The confidentiality, integrity, and availability of information on the Internet are three basic security concepts [8]. Information that is read or copied by someone not authorized to do so is known as loss of confidentiality. Information that has been classified as confidential is usually private or sensitive and should not be disclosed. Examples of this type of information include credit card applications, medical records, bank records, and corporate business plans. If information is available on an insecure network it can be corrupted. The result is a loss of integrity because the information has been modified in an unexpected way. Unauthorized changes have been made to the information, sometimes by human error or intentional tampering. Integrity of information is important for activities such as electronic funds transfers and air traffic control. The loss of availability is when information is erased or becomes inaccessible. This means that people who are authorized to get information cannot get what they need. Availability is important to service-oriented businesses that depend on information. Availability of the network itself is important to anyone whose business or education relies on a network connection (Gehling and Stankard 32).

Research on securing electronic commerce is extensive. Electronic data interchange and secure online transactions are key perceptions to focus on to improve security. Through Computing/Technology Policy, commerce policy and computer crime are major components to understand. Lastly, security services and Software and Application Security are vital areas maintain when securing electronic commerce.

Chapter 1 LITERATURE REVIEW

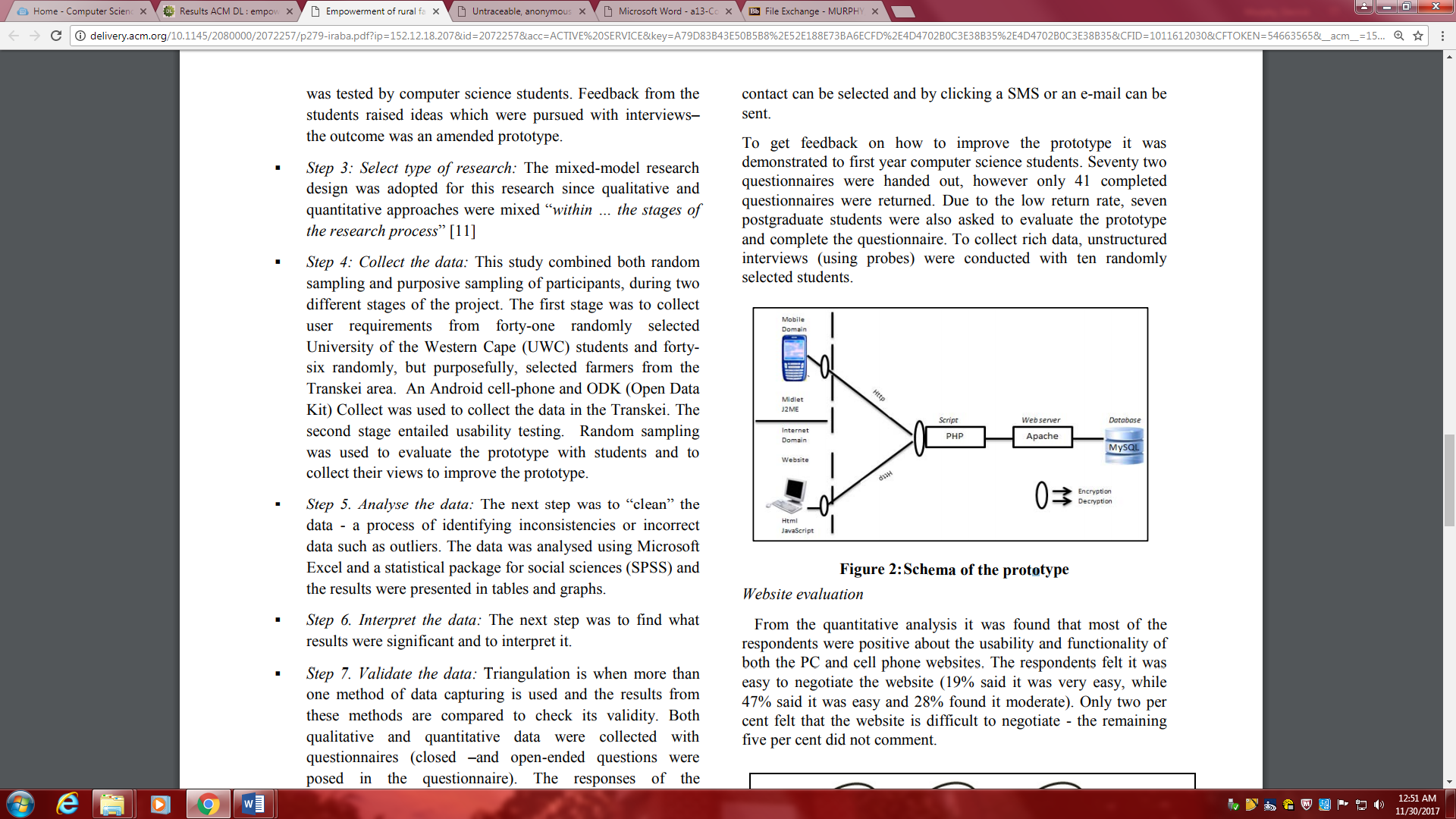
1.1 Electric Commerce

1.1.1 E-Commerce Infrastructure

Researchers developed advanced e-commerce infrastructure through a project to empower rural farmers to do business by means of inexpensive mobile technologies. In particular, the aim is to take advantage of the inexpensive features of low-end mobile phones to access market related information and to allow farmers to promote their commodities competitively (Louise and Venter 279). Farmers from rural areas of the Eastern Cape were administered questionnaires and some interviews with the intentions of acquire data about farming, cell phone usage and internet accessibility additionally the cost of these services. A prototype of a mobile marketing system was designed using the information. The prototype was designed and evaluated in terms of its usability and functionality. The researcher used different mobile devices and web browsers to test the application’s compatibility.

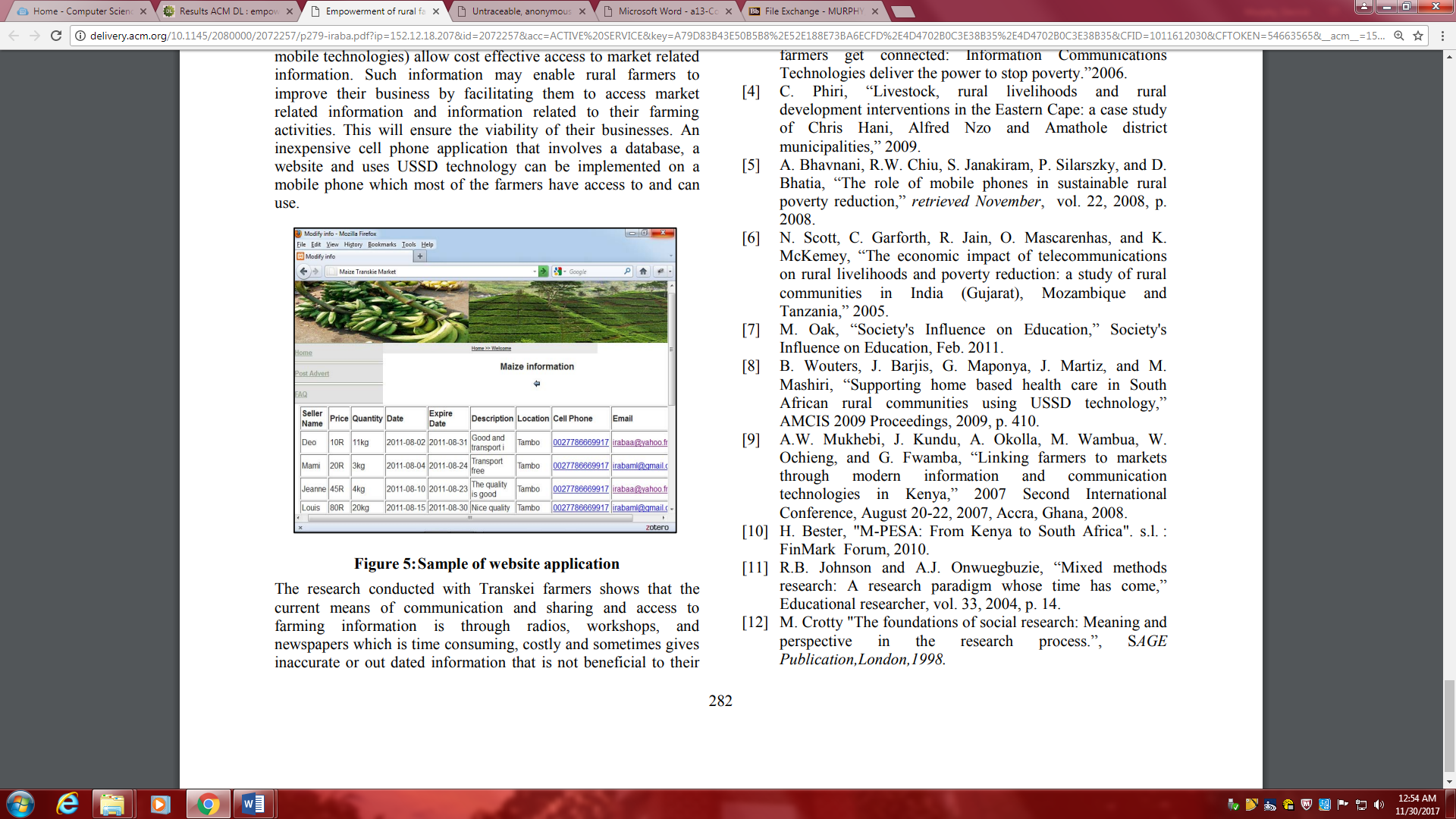
The data concluded that farmers have mobile phones and access to the internet but these tools are not utilized for accessing business information. As an alternative farmers used radio reports and contacting shop/store owners to source market information of whom they want to sell or plan to buy merchandise. Overall respondents were familiar with using cell phone services such as airtime top-up, checking balances, sending a please call me and they were also able to send and read SMS’s. The prototype designed comprised two portions: the web-based interface, reachable by cell phone or personal computer (PC), that allow users to post commodities, contact sellers or buyers by SMS or e-mail; and a USSD(Unstructured Supplementary Services Data)-based application (on a cell phone) which could be used by sellers to post their commodities, buyers to check prices, and sellers’ contact details. The completed prototype evaluation shows that users found it easy and convenient to use.

Business and information technology (ICT) were used to help the researchers, learn more about the people in the area. An integrated approach was followed in order to obtain the desired information.

The research was done as two distinct cycles: Initially user requirements were collected, and modelled to provide a system that met the requirements. Unified modelling language (UML) was used to illustrate interactions between the system and the users and also describe the system's classes, attributes, and the relationships between the classes. During the second cycle a prototype was developed with both a website and cell phone application. The website was designed using Hypertext Preprocessor (PHP) and JavaScript as programming languages, Apache as web server, and HTTP was used as protocol for retrieving inter-linked resources. The cell phone application was designed using Java 2 Platform, Micro Edition (J2ME) and My Structured Query Language (MySQL). Both parts of the prototype access a MySQL database (Louise and Venter 280).

The project followed an eight-step mixed method research model. First *clarifying the question*, Second *Determining whether a mixed design is appropriate*, next *Select type of research*, fourth *Collect the data,* step 5 *Analyze the data*, next *Interpret the data*, sixth *validate the data*, lastly *Draw conclusions and write a report.*

With the proposed mobile application farmers will be able to easily access or post information on a common database. Easy access to information, using a mobile phone (which most of the farmers own), makes it possible to get accurate and timely information. If farmers are able to advertise their produce and if they can be put into contact with potential clients, they will be able to choose the best offers and thus be empowered (Louise and Venter 282).



1.1.2 Digital Cash

Recent technology that sparks evolution in digital cash is the Private and secure payment with Radio Frequency Identification (RFID). RFID systems that were initially directing simple object identification are used more often for sophisticated applications such as access control and payment. Parallel to normal electronic cash, users can pay using so called coins or virtual currency. Using PSP, tags do not need to store valid currency, but produce it as necessary. RFID can be used for a variety of applications, however attaining security and privacy of payment is challenging due to resource restrictions of RFID tags.

The Oyster Card [29] is a prominent example of a large scale deployment of contactless smartcards, i.e., powerful RFID tags, enabling convenient payment for public transportation services. In such a scenario, people entering a metro just quickly hold their tags close to a reader device in front of a gate to issue the payment for the transport fee. Similar payment and access control schemes are in widespread use for other kinds of public transportation such as buses, tramways, or trains (Blass 51).

Unfortunately, such payment setups rise challenging security and privacy issues. First, an impostor or a malevolent user, issuing false payments or mimicking genuine users, should be prohibited from having admittance to public transportation. Next, privacy that is often highlighted both as a user condition and a governing matter. Privacy requires that neither an external contender nor the public transportation system is able to recognize users by misusing the payment system. Additionally, readers with in a metro bus are often embedded devices that are not permanently connected to a backend system such as a server. Thus readers are obligated to authenticate offline and within a small amount of time, whether a transaction is valid or not.

Ensuing the concepts of digital or electronic cash, the tag serves as a rechargeable electronic wallet. It is responsible for recurring loading of pre-paid coins of a virtual currency, and manages all communication with the reader. The focal point of PSP is that the tag does not actually store coins, but it obtains some data to produce a restricted amount of binding coins any moment. Using Bloom filters, readers can authenticate the legitimacy of coins received from tags.

PSP meets the security and privacy requirements raised by RFID based payment as follows:

An adversary cannot arbitrarily invent new coins, i.e., introduce coins into the system for which he did not legitimately pay for through the bank.

Overspending coins is impossible: an adversary cannot replay coins from his own payments or stolen coins from other people’s payments he eavesdropped.

Readers are offline and only synchronize, e.g., once a day, with the bank. Yet, an adversary still cannot doublespend coins: he cannot pay with the same coin twice at different readers. If he does, his identity will be revealed at the bank. Revealing the identity of adversaries trying to doublespend money has O(1) complexity for the bank, but is impossible for readers.

Users of RFID tags remain anonymous and are untraceable: the true identity of a user is hidden to the public transport system and the adversary. Also, neither the public transportation system nor an adversary can trace users/tags on subsequent payments, i.e., link different payments to the same tag.

PSP is lightweight: besides being able to execute a hash function, tags feature only a few bytes of nonvolatile memory.

PSP can cope with resource-limited readers. Readers are often embedded devices, so their storage and computational resources are, although orders of magnitude higher compared to tags, still restricted. With respect to the number of tags and coins, complexity for verifying a coin is in O(1) (Blass 52).

Using tiny RFID tags all the while being Secure, privacy-preserving, maintaining offline electronic payments only is a new and challenging problem. The PSP remains a solution minimizing computational necessities for the tag, but still presents fortification against overspending and privacy against payees. Pretenders cannot invent new coins, replay, or steal coins from genuine users of the scheme. Payees, e.g., a metro system, cannot trace or associate succeeding transactions of users to the same tag. Privacy is assured, because tags only evaluate a hash function and store 84 byte in non-volatile memory.

1.2 Computing / Technology Policy

1.2.1 Transborder Data flow

Sharing of knowledge, information, and practices across cultural and national boundaries are the problems and opportunity globalization brings. As a result, governments around the world are progressively engaging in Transnational Public Sector Knowledge Networks (TPSKNs) as appropriate mechanisms for dealing with a host of global problems that no one nation or single government is capable of solving alone. Environmental quality, public health, international trade, and responses to disasters are just a few of the areas where information and knowledge need to cross national and cultural boundaries through channels and mechanisms that are more agile and less controlled than the formal interactions among sovereign states (Dawes 362). This type of network is becoming a key feature of a twenty-first century in which government representatives and establishments exchange information and organize actions to address issues on an international scale. TPSKNs are viewed as an emerging area within the domain of digital government.

While the number of TPSKNs continues to surge, limited studies have been directed to explore empirically the complex and dynamic phenomenon of knowledge and information sharing that they embody. The lack of empirical studies in this area signifies a space in the DG literature and a space in the knowledge accessible to government practitioners who are expected to participate in these affiliations. According to a study conducted by the Center for Technology in Government (CTG) to assess the pertinent literature of international digital government research from 1994 to 2008, out of 276 articles representing the total number of international DG studies, only 20 articles (7%) fall into the transnational category which refers to studies that focus on issues or problems that involve either planned or unexpected interaction among two or more countries (Dawes 362). Those articles fixated on technical and organizational aspects primarily and not as much on political, legal, institutional, and cultural aspects.

Through the transnational cases, specific research questions have a particular interest in being addressed:

How do participants in different countries perceive the dimensions, stakeholders, benefits, and risks of engaging in intergovernmental systems for information and knowledge sharing?

What are the similarities and differences in these perceptions? What cultural, political, economic, and social factors account for them?

How do the participants attempt to create shared understanding of technologies, context, terms, processes, and contingencies that generate capabilities for effective action?

Which strategies, tools, and behaviors are more likely to lead to successful international knowledge networks that benefit individuals, organizations, and communities?

What preparation, methods, and tools are best suited for research on these questions (Dawes 362)?

TPSKN panels have multiple goals. Initially, it strives to increase interest in research on transnational topics in general. This goal will be achieved by demonstrating the roles these networks play or could play in addressing serious worldwide issues. Next, the panelists will discuss existing methods to research in this area that is both theoretically sound and relevant. This includes approaches they used and the problems they came across while working with international research partners, networking and gathering information from international participants. Third, the panel is intended to exchange ideas and approaches with the audience regarding the central value and the everyday considerations of exploring this developing area of digital government research and practice.

1.2.2 Government Technology Policy

From Instagram to Snapchat to Twitter, social media technologies have become pillars of the internet world. Technically titled technology-mediated social participation systems, commonly known as social media, offers a wide range of chances for interaction, engagement, participation, and collective problem solving. Although associated with entertainment and interpersonal relationships, these social media technologies also open advanced methods for instantaneous and constant communication among citizens and governments.

These technology uses occur within established guidelines for access, management, and preservation of data. Government agencies, however, have generally begun using social media without sufficient consideration of this larger policy environment. Though the Office of Management and Budget (OMB) and the General Services Administration (GSA) offer federal agencies guidance regarding the use of social media, inconsistent goals and practices among related policies, combined with conflicting design values applied to implementations, have created long-term policy conflicts, particularly in approaches to defining and implementing access (Jaeger 216).

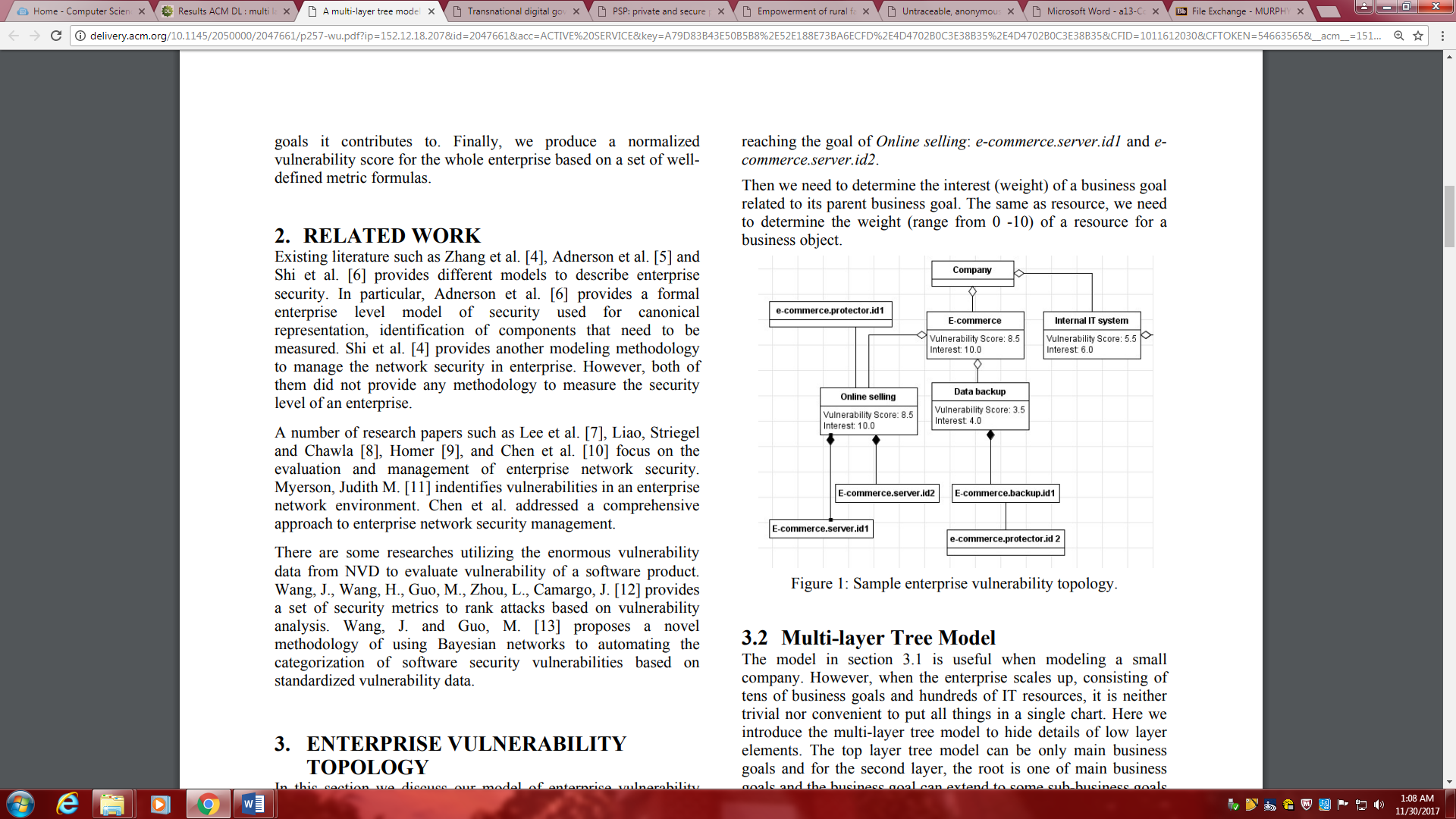
Though the current policy environment addresses many issues of privacy, security, accuracy, and archiving in some detail, much of the policy related to the use of social media predates the creation of social media technologies. As a result, many of the existing policies do not adequately address the technological capacities, operations, or functions of social media. Further, as social media provide new ways to combine previously unavailable and/or separately maintained data, there are now cross-dataset concerns that impact multiple policy issues. Finally, it is important to consider that social media services are private ventures with their own acceptable use, data use, accessibility, and privacy policies that often do not conform to federal requirements (Jaegar 217).

Some of these polices are very broad. The Telecommunications Act of 1996 and the E-government Act of 2002 both contain statements that access to information and communication technologies being used online and to e-government content should be accessible to all members of the public. Undoubtedly, government-to-citizen social media communications fall under these orders.

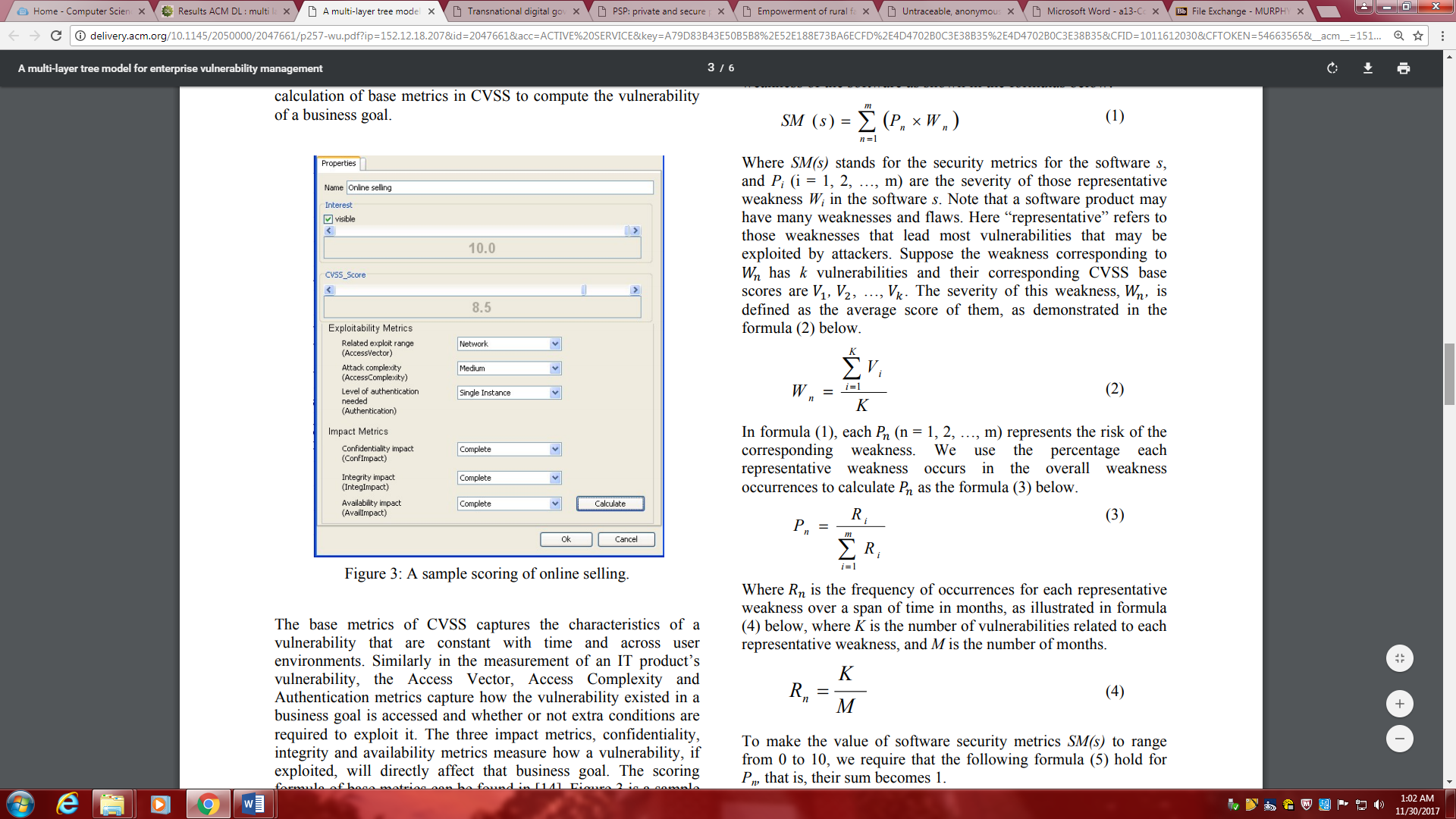
1.3 Security and Privacy

1.3.1 Security Services

In order to assess an enterprise’s information security status properly enterprise-wide vulnerability assessment should be conducted on a regular basis. Complexity of information systems and the quick arrival of new weaknesses make it a time-consuming duty for security experts. A moderate enterprise would normally to have hundreds of diverse IT resources such as computer hardware and software, distributed in different zones of enterprise. As the IT resources scale up, it is gradually more difficult for a single manager to compare the vulnerability information with each IT. Security professionals are seeking an automated tool to help screen and manage the complex IT resources. A newly presented multi-layer tree model-based approach supports the single management of enterprise vulnerability, which is vital for enterprise risk management.

The methodology firstly offers an well-organized model to define an enterprise vulnerability topology. Here we abstract an enterprise as a collection of business goals, such as E-commerce, customer services, and financial accounting, etc. These business goals are established by the senior managers of an enterprise. Only by meeting these business goals, can a company maintain its competitiveness in the business and market. In an enterprise, there are a large number of IT resources contributing to business goals. For instance, an HTTP server and database play the core roles of E-commerce business goal. In general, we assume that we have a formal description of an enterprise IT resources with respect to the device, weight, and their functioning roles to the business goals (WU 257). To back the modeling of an enterprise vulnerability topology, EVMAT is implemented, this proposes a user-friendly GUI help construct the model using the above three elements.

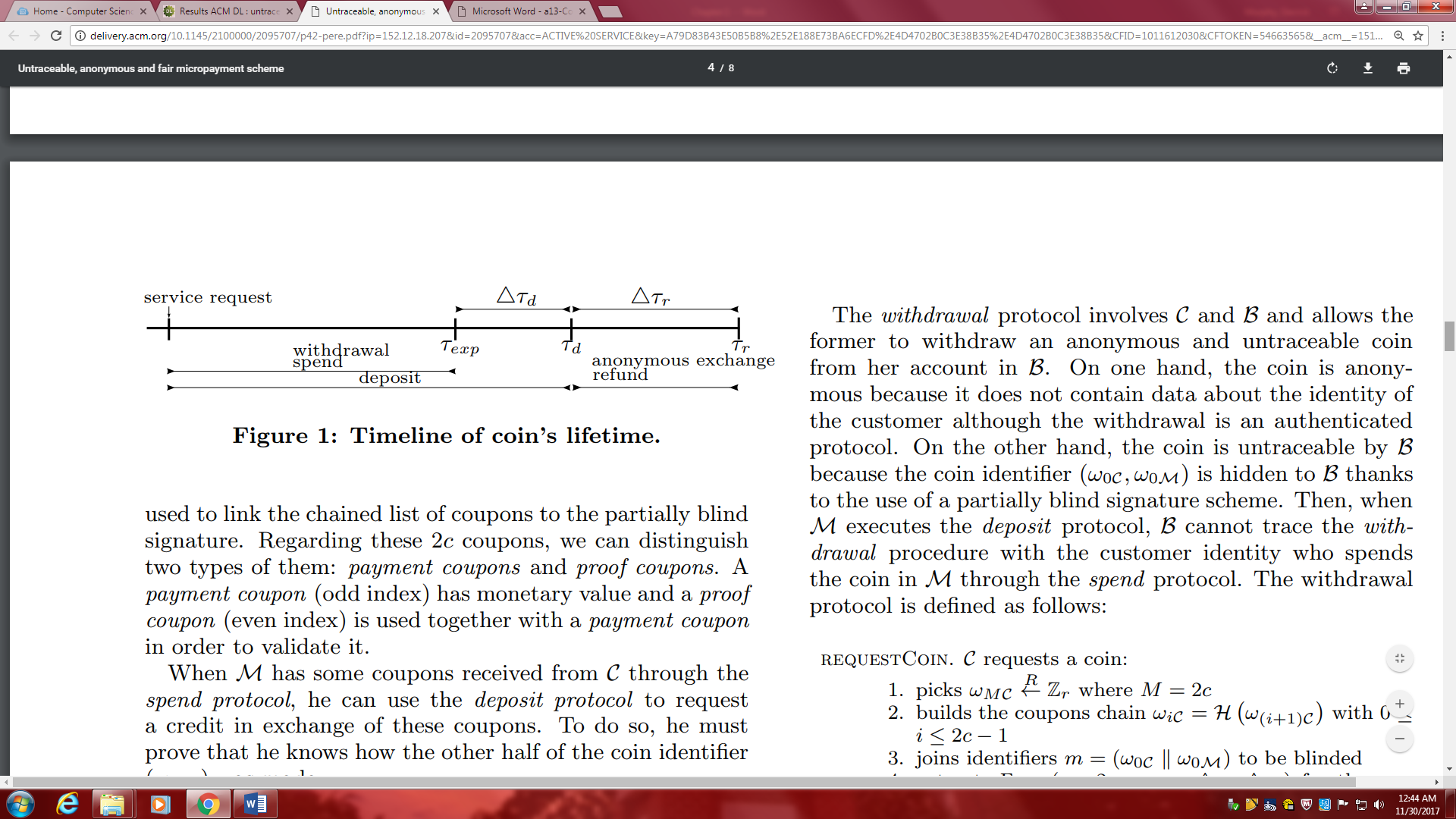
Different weights and interest are assigned to a businesses goals and resources.Next, the Common Vulnerability Scoring System is used to calculate the vulnerability scores for all leaf business goals. After, a multi-layer C/S structure tool to gather and extract system characteristics from all resources in the enterprise network based on the Open Vulnerability and Assessment Language standards and further retrieves vulnerability data from National Vulnerability Database in order to evaluate software vulnerability scores corresponding to those resources. Then we rank the weaknesses of each product installed in a resource to support decision making of security professionals. Fifthly we calculate the overall vulnerability score of a resource and the corresponding impact score to the business goals it contributes to. Finally, we produce a normalized vulnerability score for the whole enterprise based on a set of well defined metric formulas (WU 258).



1.3.2 Software and Application Security

Everyday new applications and services develop in the field of electric commerce. Minor payments of currency for small services is one of the applications. These kind of payments are called micropayments and they have unique functional and security requirements inside the field of electronic payments. Micropayments offer a advantage because they utilize small paymenys in contrast to normal payments that are typically large amounts of money.Thus, micropayments can be applied to the intangible selling of properties such as information, virtual gifts or electronic data. All of these examples involves low-value transactions, so the operational cost needs to be as low as possible in order to be profitable for merchants and customers.

On one hand, security properties are a primary concern for the development of micropayment systems to avoid financial risks for merchants and also to ensure privacy for customers. On the other hand, efficiency and the cost for individual transactions are critical factors for the development of these systems. However, efficiency and security are usually opposed, so micropayments must provide a trade-off between these requirements (Isern-Deyà 42).

Within a micropaymeny scheme the involved parties are commonly the Customer, Merchant , and either a Broker or Bank. Hence, in the common model the customer withdraws a coin from their monetary account to purchase a electronic product presented by a merchant. Lastly, merchant can deposit their received coins from customer into their broker account. The security requirement are privacy and fair or atomic exchange. Privacy must take into account anonymity, unlinkability, and untraceability. Fair Exchanges intel a reliable transfer of services through a network. Functional features of micropayment schemes include low transaction costs, lower limit, and financial risk control. Permitting low transaction costs requires alterations in interaction scheme from on-line payments mediated by banks to off-line payments, volume of information, computational cost, minimum storage, and use of built in service specific coins. Lower limits must permit exchange of small pieces of information. While financial risk control aims to minimize cost from the assumed risks of micropayments.

To improve efficiency used coins in merchant payments are specifc to a single merchant. Accompanying being anonymous and untraceable according to the presented scheme.

1.4 Statistical Analysis Methods

1.4.1 Descriptive Statistics

1.4.2 Hypothesis Test Statistics

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Basic | SSL | TLS |
| Mean |  | 89.50556126 | 29.55052102 | 5.956146434 |
| Standard Deviation |  | 41.07645655 | 12.85431791 | 3.618271231 |
| Variance |  | 1687.275283 | 165.2334889 | 13.0918867 |
| N |  | 30 | 30 | 30 |
| T-Value |  | 0.193699203 |  |  |
| P-Value(Basic and SSL) | | 6.42837E-09 |  |  |
| P-Value(TLS and SSL) | | 3.06421E-11 |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| P-Value is lower than 0.05 | |  |  |  |
| Probability the observed results are random are due to chance are low | | | | |
| Conculsion : Null hypothesis is denied | | |  |  |

Chapter 2 RESEARCH DESIGN

2.1 Research Objectives

The objective of the proposed research is to:

* Review the current models involved in e-commerce
* Gain insight on the various scopes that determine a secure e-commerce environment

Proper analysis of e-commerce environments acknowledges meaning of electronic commerce, computing or technology policies in place, and security and privacy methods present.

* + 1. Research Problem

The research aimed to understand the appropriate scheme to solve security flaws in e-commerce. With the exponential growth of electronic commerce systems, creating a safe system has been the preceding race. Many variables come with calculating the trustworthiness in e-commerce.

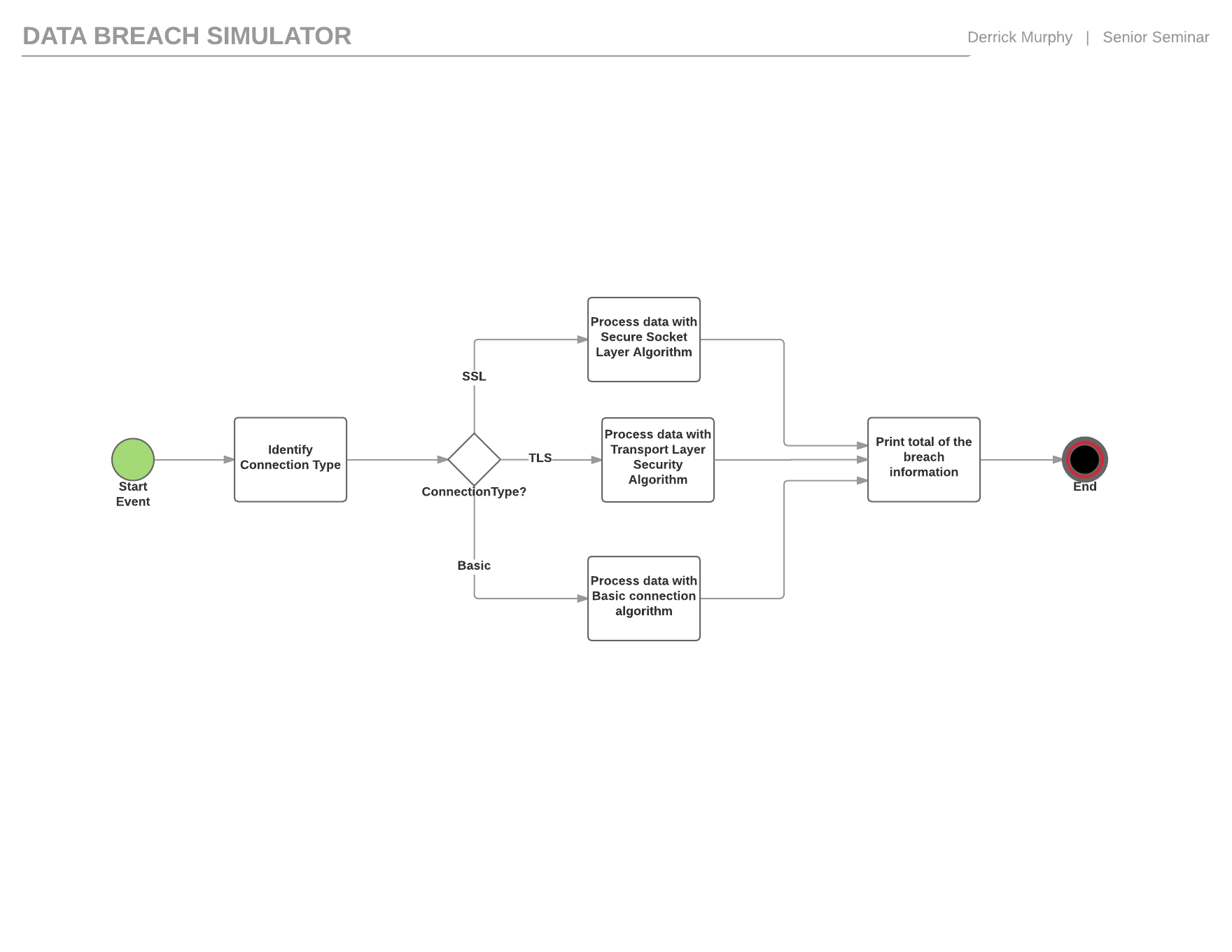
* + 1. Variables and Hypotheses

In the projected experiment there are two independent variables and a single dependent variable. First dependent variable includes the type of connection used during connectivity. Second dependent variable takes account the sample data size. Leading to resultant values for the dependent variable, size of the data breached during interconnectivity. Concluding these variables, the corresponding null hypothesis of the states, there is no significant difference in the size of the data breached between using a secure data connection or a basic data connection.

* + 1. Related Work

Following the research of the topic there were many respectable sources encompassing electronic commerce. There are a wide range of resources relating to security and privacy, these include the security services and software and application security. Unfortunately, there lack studies involving policies of e-commerce, but minimal yet sound information was available. As a result, related work of interest to the incredible electronic commerce include discovering more of the unknown policies of the e-commerce medium. As the legal knowledge and the know how to take advantage of these policies come to the forefront, we can assume the potential of e-commerce could finally begin to strive towards its peak.

2.2 Experiment Design



2.2.1 Experiment Description

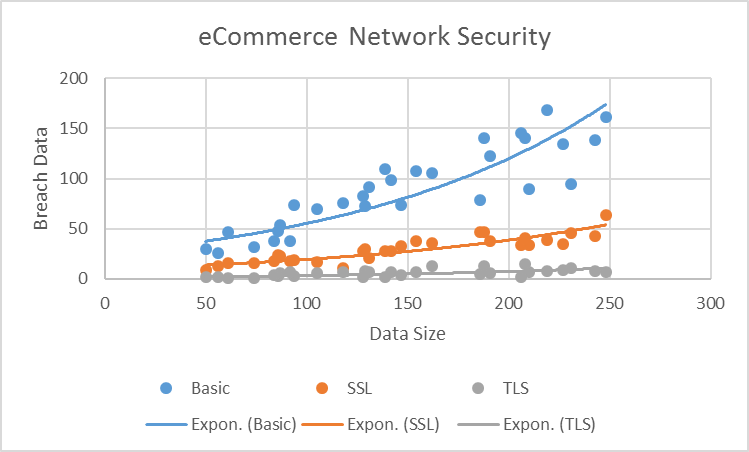
In the experiment, the independent variable connection type is initially declared by the user. The program generates random results for the second dependent variable, sample size. If the connection is processed on a secure socket layer then the breach algorithm becomes void and the breach results return zero. If the connection is basic this means information is visible by hackers spying on the processes to intercept data. Therefore, the program continues to produce the necessary values to process the breach algorithm. A random number generator establishes a sample size between fifty and one hundred and fifty; along with randomization of the unit of the sample. In the yield of the output a value that is a portion of the original sample size is returned. This is done by dividing the data size with random number between two and six, the return value is the declared breach size.

2.2.2 Data Collection Design

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Observation | Data Size (MB) | Basic | SSL | TLS |  | | 1 | 87 | 53.49921865 | 22.48057273 | 5.92795818 |  | | 2 | 142 | 98.09918299 | 27.61714738 | 7 |  | | 3 | 118 | 75.28833422 | 10.67705601 | 6.815497543 |  | | 4 | 50 | 29.65590201 | 9.289195418 | 1.593053618 |  | | 5 | 86 | 48.07312299 | 23.5560268 | 2.963380696 |  | | 6 | 94 | 73.29652267 | 18.42611344 | 2.447044089 |  | | 7 | 61 | 47.08759269 | 16.2348205 | 1.064368089 |  | | 8 | 188 | 140.5428537 | 46.66495026 | 12.53381835 |  | | 9 | 105 | 69.21536938 | 17.02656172 | 5.550068949 |  | | 10 | 162 | 105.8014323 | 35.39407623 | 12.50253361 |  | | 11 | 206 | 145.2535231 | 33.6391708 | 2.313798255 |  | | 12 | 129 | 72.7387185 | 30.15153836 | 7.48943409 |  | | 13 | 210 | 89.25599946 | 34.03065549 | 6.902834892 |  | | 14 | 154 | 107.7378107 | 37.57199363 | 7.275868233 |  | | 15 | 84 | 38.10901487 | 17.90715548 | 3.695037604 |  | | 16 | 191 | 122.5292737 | 37.25863912 | 6.303860943 |  | | 17 | 231 | 94.14495595 | 46.15059038 | 11.19645781 |  | | 18 | 56 | 25.9579225 | 12.8198242 | 1.949781493 |  | | 19 | 139 | 109.8801427 | 27.67547063 | 1.820197447 |  | | 20 | 243 | 138.1001134 | 42.72038321 | 7.889532255 |  | | 21 | 128 | 82.60684294 | 27.62834744 | 1.804104997 |  | | 22 | 219 | 167.9681805 | 38.54490308 | 7.661449827 |  | | 23 | 92 | 38.21687478 | 17.60617695 | 6.669640491 |  | | 24 | 208 | 140.5798671 | 41.0723871 | 14.57548242 |  | | 25 | 74 | 31.38636261 | 15.92425605 | 0.793994977 |  | | 26 | 131 | 92.08374946 | 20.3076982 | 7.253330339 |  | | 27 | 227 | 134.3799126 | 35.23742256 | 8.930988927 |  | | 28 | 147 | 73.27680219 | 32.51115421 | 3.527773408 |  | | 29 | 248 | 161.6543734 | 63.37906563 | 6.95031021 |  | | 30 | 186 | 78.74686561 | 47.01227765 | 5.282791274 |  | | Mean |  | 89.50556126 | 29.55052102 | 5.956146434 |  | |  |  |  |  |  |

2.3 Data Analysis Design

2.3.1 Descriptive Statistics Design



2.3.2 Hypothesis Test Statistics Design

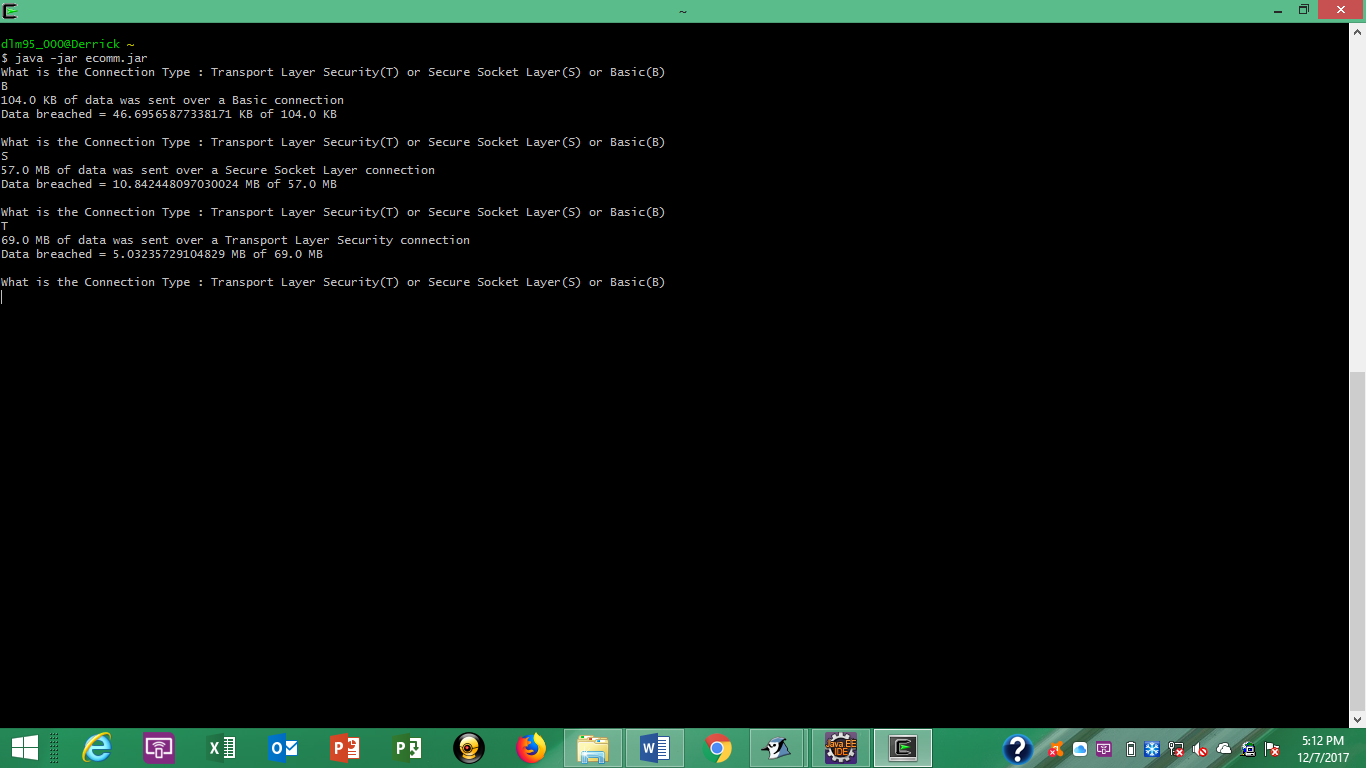
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Basic | SSL | TLS |
| Mean |  | 89.50556126 | 29.55052102 | 5.956146434 |
| Standard Deviation |  | 41.07645655 | 12.85431791 | 3.618271231 |
| Variance |  | 1687.275283 | 165.2334889 | 13.0918867 |
| N |  | 30 | 30 | 30 |
| T-Value |  | 0.193699203 |  |  |
| P-Value(Basic and SSL) | | 6.42837E-09 |  |  |
| P-Value(TLS and SSL) | | 3.06421E-11 |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| P-Value is lower than 0.05 | |  |  |  |
| Probability the observed results are random are due to chance are low | | | | |
| Conculsion : Null hypothesis is denied | | |  |  |

Chapter 3 RESEARCH FINDINGS

3.1 Experiment Results

30 observations were monitored during the experiment about data breaches on Basic, Secure Socket Layer, and Transport Layer Security connections. The algorithms for each connection produce different results. I can conclude that connections would produce more breaches if the encryptions complexities are simpler.

* + 1. Materials and Procedures

In order to perform the experiment a Java installation must be installed on your system and you must obtain the java code that contains the e-commerce breach simulation. Once you have initiated the installation follow the directions of the prompts and ensure the everything meets your system requirements. Next, the Java code that makes the program has to be entered into a Java programming platform. Then, the code must be compiled and executed. Once running you will be prompted to type the first letter of the connection being used during transport. Lastly, the program output the results.

* + 1. Comparison to Related Work

In my research I came across other simulator that calculated data loss as well. The algorithms used in the compared work were not visible to create an exact match. Thus, my project contained algorithms that would produce common results. In my work I developed a simulation of data loss using the varying connection types used by e-commerce platforms. As a result of the simulation users should have a respectable understanding of the protection of information delivered through e-commerce connections.

3.2 Data Analysis Results

Graphs were used to provide a visual of the calculations returned from the experiment. With the growth of e-commerce marketplaces, it is valuable to understand the risks of engaging with these forms of market. This experiment was developed to measure the breach information regarding to the security of connecting the network in an e-commerce infrastructure.

3.2.1 Descriptive Data Analysis

The descriptive data analyzes the breach total for various data sizes. Analysis for Basic, Secure Socket Layer, and Transport Socket Layer connections were observed. The information is depicted on a scatter plot from the lowest data size of 50 MB to 250MB. Each connection type has a corresponding color that represents its’ value. The results are described using exponential lines to understand the trend of the different possible outcomes.

3.2.2 Hypothesis Test Data Analysis

The hypothesis test data was analyzed using a T-test. The values calculated are the mean, standard deviation, variance, count of observations(N), T-Value (Basic-SSL), and P-values (for Basic-SSL and TLS-SSL). The test found the P-value was lower than 0.05. This correlates to the probability of the observed results are random due to chance are low. Concluding the Null hypothesis is denied following the results.

3.3 Discussion Findings

As a result of the research conducted I came across much interesting information. There were products that could be purchased by people who wanted to start an e-commerce marketplace. The products contained the necessary tools to run a proper e-commerce platform. These also included the security features that would protect everyone accessing and using the platform. I learned the different characteristics that should be incorporated in a comprehensive e-commerce system.

Chapter 4 CONCLUSIONS

* 1. Conclusions

Understanding the security measures in an e-commerce system is important. Data breaches are a common security threat in the digital environment. Online markets allow hackers to know where they could gain sensitive information and a lot of it. These are highly visited places that hackers know are being used constantly and increasingly popular. As a conclusion of the finding in this research one should observe the means of protection used when processing any information crossing through an e-commerce network.

* 1. Implications for Future Research

Following the research of the topic there were many respectable sources encompassing electronic commerce. Unfortunately, there were lack studies involving policies of e-commerce, but minimal yet sound information was available. As a result, related work of interest to the incredible electronic commerce include discovering more of the unknown policies of the e-commerce medium.

Bibliography

1. Bob Gehling and David Stankard. 2005. eCommerce security. In Proceedings of the 2nd annual conference on Information security curriculum development (InfoSecCD '05). ACM, New York, NY, USA, 32-37. DOI=http://dx.doi.org.courseinfo.wssu.edu:2048/10.1145/1107622.1107631
2. Iraba, M. Louise, and I. M. Venter. “Empowerment of rural farmers through information sharing using inexpensive technologies.” Proceedings of the South African Institute of Computer Scientists and Information Technologists Conference on Knowledge, Innovation and Leadership in a Diverse, Multidisciplinary Environment - SAICSIT 11, 2011, doi:10.1145/2072221.2072257.
3. Blass, Erik-Oliver, et al. “PSP: Private and Secure Payment with RFID.” Computer Communications, Elsevier, 10 Nov. 2012, [www.sciencedirect.com/science/article/pii/S0140366412003830](http://www.sciencedirect.com/science/article/pii/S0140366412003830).
4. Dawes, Sharon S. “Purpose, value, challenges.” Transnational digital government research collaborations, ACM, dl.acm.org/citation.cfm?doid=2037556.2037626.
5. Jaeger , Paul T. “Access Perspectives and Design Values in Government Social Media Usage.” ACM Digital Library, ACM, dl.acm.org/citation.cfm?doid=2307729.2307764.
6. WU, Bin, and Andy JU An Wang. “A Multi-Layer Tree Model for Enterprise Vulnerability Management.” ACM Digital Library, ACM, dl.acm.org/citation.cfm?doid=2047594.2047661.
7. Benjamin Edelman. 2009. Adverse selection in online "trust" certifications. In Proceedings of the 11th International Conference on Electronic Commerce (ICEC '09). ACM, New York, NY, USA, 205-212. DOI=http://dx.doi.org.courseinfo.wssu.edu:2048/10.1145/1593254.1593286
8. A. J. Davies and A. J. Garcia-Sierra. 1999. Implementing Electronic Commerce in SMEs — Three Case Studies. BT Technology Journal 17, 3 (July 1999), 97-111. DOI=http://dx.doi.org/10.1023/A:1009684605872
9. B. A. Cross. 1999. BT Trustwise — Enabling eCommerce Through Trust. BT Technology Journal 17, 3 (July 1999), 44-49. DOI=http://dx.doi.org/10.1023/A:1009620202237
10. Fusheng Jin, Zhendong Niu, and Haiyang Lang. 2010. A Pattern Based Anti-Fraud Method in C2C Ecommerce Environment. In Proceedings of the 2010 International *Conference on E-Business and E-Government* (ICEE '10). IEEE Computer Society, Washington, DC, USA, 242-244. DOI=10.1109/ICEE.2010.68 http://dx.doi.org/10.1109/ICEE.2010.68
11. Andreu Pere Isern-Deyà, M. Magdalena Payeras-Capellà, Macià Mut-Puigserver, and Josep L. Ferrer-Gomila. 2011. Untraceable, anonymous and fair micropayment scheme. In *Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia* (MoMM '11). ACM, New York, NY, USA, 42-49. DOI=http://dx.doi.org/10.1145/2095697.2095707
12. Kyle Meadors. Secure Electronic Data Interchange over the Internet. In *Internet Computing, IEEE*. IEEE, 82–89.

Appendices

Page

CHAPTER

1. LITERATURE REVIEW
   1. Electronic Commerce 2
      1. E-commerce Infrastructure 2
      2. Digital Cash 4
   2. Computing / Technology Policy 6
      1. Transborder data flow 6
      2. Government technology policy 7
   3. Security and Privacy 8
      1. Security Services 8
      2. Software and Application Security 10
   4. Statistical Analysis Methods 12
      1. Descriptive Statistics 12
      2. Hypothesis Test Statistics 13
2. RESEARCH DESIGN
   1. Research Objectives 13
      1. Research Problem 14
      2. Variables and Hypotheses 14
      3. Related Work 14
   2. Experiment Design 15
      1. Experiment Description 15
      2. Data Collection Design 16
   3. Data Analysis Design 17
      1. Descriptive Statistics Design 17
      2. Hypothesis Test Statistics Design 18
3. RESEARCH FINDINGS
   1. Experiment Results 19
      1. Materials and Procedures 19
      2. Comparison to Related Work 19
   2. Data Analysis Results 20
      1. Descriptive Data Analysis 20
      2. Hypothesis Test Data Analysis 20
   3. Discussion Findings 20
4. CONCLUSIONS
   1. Conclusions 21
   2. Implications for Future Research 21

Acknowledgements

Dr. Elva Jones, Bob Gehling, David Stankard, M. Louise Iraba, I.M. Venter, Erik-Oliver Blass, Refik Molva, Thorsten Strufe, Sharon S. Dawes, Paul T. Jaeger, Bin WU, Andy Ju An Wang, Benjamin Edelman, A. J. Davies, A. J. Garcia-Sierra, B. A. Cross, Fusheng Jin, Zhendong Niu, Haiyang Lang, Andreu Pere Isern-Deyà, M. Magdalena Payeras-Capellà, Macià Mut-Puigserver, Josep L. Ferrer-Gomila, Kyle Meadors