The Effect of Website Security on E-Payment Usage: from Jordanian Customer Perspective

أثر أمن الموقع الالكتروني على استخدام الدفع الإلكتروني: من وجهة نظر العملاء الأردنيين

Prepared by:

Manar Khamis Alfarsi

Supervised By:

Dr. Sameer Al-Jabaly

A Thesis Submitted in Partial Fulfillment of the Requirements for Master Degree in E-Business

Faculty of Business

Middle East University

Amman - Jordan

April- 2016

Examination Committee's Decision

This thesis of the student Manar Khamis Alfarsi, wich studied "**The Effect of Website Security on E-Payment Usage: from Jordanian Customer Perspective**" has been defined, accepted and approved on 28/5/2016

Committee Members:

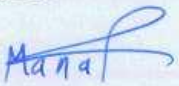
No.	Name	Title	Signature
1	Dr. Hanadi Salameh	Committee chairman & Internal Examiner	
2	Dr. Mahmoud Migdadi	External Examiner	
3	Dr. Sameer Al-Jabaly	Committee Member & Supervisor	

Authorization

I'm Manar Alfarsi do authorize Middle East University to provide hard or electronic copy of my thesis to any university ,library , and institutions or parties interested in scientific research as they request.

Name: Manar Khamis Alfarsi

Date: 28-5-2016

Signature: 

Acknowledgement

I would consider this research as an end result of a mutual effort that MEU and Business department help me to achieve. One academic year of research and hard work passed to create this research.

First I would like to express my gratitude to my supervisor Dr. Sameer Al-Jabaly, for his support, gaudiness, wisdom and help all the way. I truly appreciate his helpful comments and suggestions to improve my thesis research.

I also would like to thanks all the survey participants, who have willingly shared their valuable time.

Special gratitude to Marka VIP, Sheyakati, Karasi companies for the unlimited support.

I would also thank Dr. Adel al for his remarkable assistance and Encouragement.

Sincerely Yours,

Manar Alfarsi

Dedication

To beloved parents and husband, without any return or interest starting with my lovely supportive parents, to my small lovely family ending with friends. I would love to say ”thank you all, without you I wouldn’t be hear” maybe this is the first time that I can tell everyone that those are the real people who deserve to be thanked.

Yours truly,

Manar Alfarsi

Table of Content

List of Tables

List of Figures

The Effect of Website Security on E-Payment Usage: from Jordanian Customer Perspective.

Prepared by: Manar Khamis Alfarsi

Supervisor: Dr. Sameer Al-Jabaly

Abstract

This research aims to investigate the effect of Website Security on Electronic Payment usage in Jordanian shopping websites. That's where the population of the study includes Jordanian shopping websites customers, (620) questionnaires distributed as a sample of the study, only (469) questionnaires returned, where they respond rate (75.6 %) from the total distributed questionnaires.

The researcher used the descriptive study method; the data collected from the responses of the questionnaires were analyzed through Statistical Package for Social Sciences (SPSS).

The study explored a number of important and significant results summarizing as follows:

1-This study obtained the evaluation of website security in the Jordanian website shopping through four main dimensions (Privacy, Confidentiality, Data Integrity, and Authentication).

2-The study showed a high level of importance of all dimensions that evaluated in this study.

Based on study results and conclusions, the following recommendations are suggested: Jordanian website shopping recommended translating their vision into policies and procedures in order to enhance their effect on their operation competitive capabilities, and there should be a clear and shared understanding of website security.

Keywords: Website Security, Privacy, Confidentiality, Data Integrity, Authentication and e payment.

أثر أمن الموقع الالكتروني على استخدام الدفع الإلكتروني: من وجهة نظر العملاء الأردنيين

الطالبه: منار خميس الفارسي

المشرف: د.سمير الجبالي

الملخص

تهدف هذه الدراسة لبيان اثر أمن الموقع الالكتروني على استخدام الدفع الإلكتروني: من وجهة نظر العملاء الأردنيين ، حيث ان مجتمع الدراسة هو زبائن مواقع التسوق الالكتروني ، وقد تم توزيع 620 استبيان كعينة للدراسة وقد تم استعادة 469 فقط. بما نسبة 75.6٪ من مجموع الاستبيانات الموزعة.

قام الباحث باستخدام المنهج الوصفي، وقد تم معالجة المعلومات التي تم تحصيلها من الاستبيانات باستخدام برنامج SPSS للتحليل والنتائج.

وضحت الدراسة بعض النتائج الهامة ويمكن تلخيصها بما يلي:

عملت هذه الدراسة على تقيم الامن الموقع الالكتروني في مواقع التسوق الالكتروني من خلال اربع محاور رئيسة (الخصوصية والسرية وتكامل البيانات والمصداقية) حيث اظهرت الدراسة اثر مرتفع لأهمية أمن الموقع الالكتروني في مواقع التسوق الالكتروني في جميع العناصر المذكورة سابقاً، بناءً على نتائج الدراسة تم وضع بعض التوصيات: ترجمة الرؤية لسياسات واجرائات المواقع الالكترونية بهدف تحسين القدرة التنافسية للمواقع الالكترونية، ويجب أن يكون هنالك فهم واضح لسياسات امن الموقع الالكتروني لزبائن هذه المواقع.

الكلمات المفتاحية:امن الموقع الالكتروني، الخصوصية، السرية ،تكامل البيانات، المصداقية.

Chapter One

General Framework

(1-1) Introduction

(1-2) Study Problem

(1-3) Study Objectives

(1-4) Study Significance

(1-5) Study Questions

(1-6) Hypothesis

(1-7) Study Model

(1-8) Study Limitations

(1-9) Study Terminologies

Chapter 1

1.1 Introduction

Today's service industry is evolving rapidly because of advances such as the Internet and e-commerce, and the increasing demands of discerning customers (Chu and Kang, 2014).

Since using the internet have changed business path; applying it to commerce has been an emerging way of conducting business, so it affect our rapid lifestyle and wildly use of website in most felids. Recently, it has been related in most of the systems and our daily process; eliminate with it Traditional procedures. Living in a world where information can be easily exposed to others. Regardless of guarantee that company provides to current and predictable customer through online payment. The procedures and regulations company follows to convince customers to conduct online payment being able to spread the awareness of the importance of online process. The progressions of technology over the recent years have enabled the consumer a broader and much more enriched interactive experience (Yazdanifard, 2011).

Computers have had an enormous impact on communications and its potential for business growth has certainly been widely recognized (Mandić, 2009). Therefore, the main purpose of this research is to focus on the factors that affect the customer perspective of E- payment in specific and the whole idea of online shopping. Thus, to focus on security standards that motivate customer to conduct online buying process.

1.2 Study Problem

Some studies like **Sen al,** (2005) indicate that website security and e- commerce environment are critical issues which affect customer payment decision and the whole customer perspective, assuming that customer face a great challenge regarding E-payment and any online process, especially if it was their first experience of buying a new product or dealing with new company.

Based on the researcher Interview and the pilot study that been conducted with company's customers, the research notice that lack of security in website builds a barrier to customer and makes them hesitates about payment method.

Pilot study was coundcted on list of E-commerce Company's customer's such as:

- Marka VIP
- Sheyakati
- Karasi

1.3 Study Objectives

- Determine the effect of privacy on E-payment usage.
- Determine the effect of confidentiality on E-payment usage.
- Determine the effect of data Integrity on E-payment usage.
- Determine the effect of authentication on E-payment usage.
- Determine the effect of Website security on E-payment usage.

1.4 Study Significance

The objectives of this research is to show the effect of Website security on customer E-payment usage .This will aid and guide website customer to be aware of security dimensions and criteria that influence their E-payment usage, Also to understand the overview of customer perspective and make their online experience to be of much comfort, Trust an E-commerce site and the most appropriate E-payment methods for Jordanian customer especially.

Moreover, showing influence of website security towards customers as well as attitudes plays a key role in ecommerce implementation.

1.5 Study Questions

The issue mentioned in this research tries to focus on Website security (Privacy, Confidentiality, Data Integrity , Authentication.) , observe Jordanian customer perspective through customer overall experience of online shopping and website security criteria that affect their Electronic payment usage .In addition to the previous topics, this study will try to answer the below questions:

1. Is there a direct effect of privacy on E-payment usage?
2. Is there direct effect of confidentiality on E-payment usage?
3. Is there direct effect of data Integrity on e E-payment usage?
4. IS there direct effect of authentication on E-payment usage?

1.6 Study Hypothesis

H01: There is no direct effect of Website security on E-payment usage

H1.1 There is no direct effect of privacy on E-payment Usage.

H1.2 There is no direct effect of confidentiality on E-payment usage.

H1.3 There is no direct effect of data Integrity on e E-payment usage.

H1.4 There is no direct effect of authentication on E-payment usage.

1.7 Study Limitations

The followings are some limitation of present study:

- **Human limitations:** The scope of this study will deal with Jordanian online companies' customers.
- **Place limitations:** Jordanian online websites.
- **Time limitations:** There are many factors affecting on E-payment usage, but in this study because of time constraints, this research didn't examine all factors influencing on E-payment usage. The ability to achieve the study objective on time (Study time 2015-2016)
- **Scientific Limitations:** The ability to deploy the previous studies recommendations and solutions in this study.

1.8 Study Terminologies

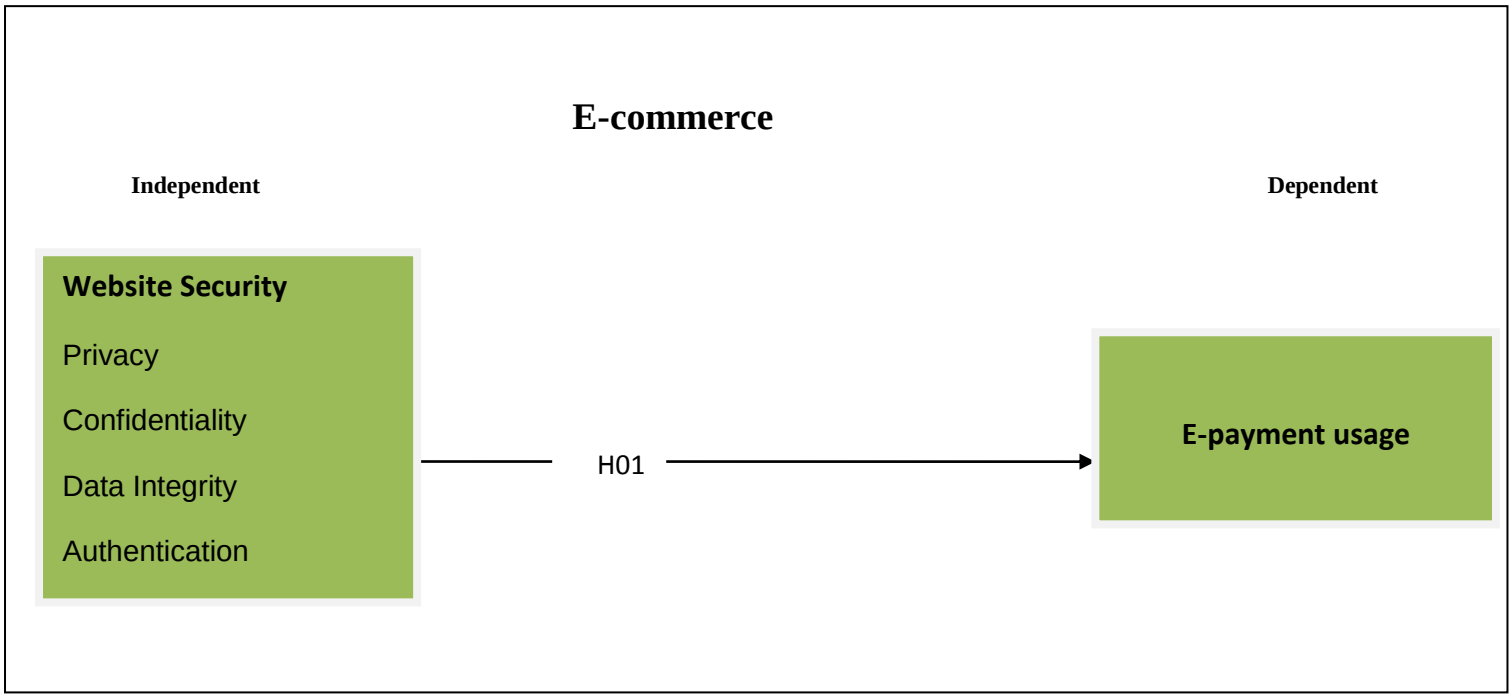
Website -Security "web security research problem is how to effectively enable a user who is running a client on an un trusted platform (i.e., a platform that may be under the control of an attacker) to securely communicate with a web application" (Szydlowski, et at, 2008)

E-payment" is the transfer of an electronic means of payment from the payer to the payee through the use of an electronic payment instrument, E-payment is defined here as the transfer of an electronic value of payment from a payer to a payer through an e-payment mechanism. "(Islam and Ahmed, 2015)

E-commerce "any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact"

(Zhang and Wang, 2014)

1.9 Study Model



Model 1.1

This model was built based on previous studies as sources that took the website security, E-payment and related factors as building criteria.

Previous studies:-

(Siddiqui, 2008); (Salem and Walsh, 2011)

Chapter Two

Theoretical Framework and Previous Studies

(1-1) Theoretical Framework

(1-2) Previous Studies

Chapter Two

The Theoretical Framework and Previous Studies

2.1 The Theoretical Framework:

This part reviews the available relevant literature to this study that will spot light on two dimensions, consists of:

- Reviews the E-commerce website security.
- Defining the concept of electronic payment usage.

E-commerce

This terminology was defined as "Electronic commerce is the buying and selling of products or services through electronic media, such as Internet and other computer networks. Originally, the term was applied to the execution of transactions through electronic transactions such as electronic data interchange. (Carmona et al, 2012)

Also it was defined as "E-Commerce is basically trading in product or services using computer network such as the internet, E-Commerce is a powerful tool for business transformation that allows companies to enhance their product-chain operation, reach market to market and improve service for customers as well as for providers".(Sen et al, 2015)

It's about elimination of the traditional experience of shopping and converts all of the phases from searching, selecting product and payment into electronic approach.

Website

"A company's website is becoming the most direct and interactive contact medium between retailers and consumers, Retailers' online presences not only enable consumers to gain product/services information, but further provide a venue for creating positive shopping experience that drives traffic to online and offline stores"(Zimmerman, 2012)

Website attributes: The dimensions of a website that create the whole shopping experience had by consumers, classified as website design, security/privacy, and shopping services. These website attributes established based on previous

Literature and were determined to be variables that capture the shopping experience of the website.

Website design: Representative of both aesthetic and functional aspects of the website. Website design describes the layout, navigation of the Retailers websites as well as product information and presentation of merchandises

Shopping services: Expanding on the traditional concept of customer service (e.g., sales help, easy and accurate transactions), shopping services cover a vast array of modern technological conveniences, from personal shopping advices, to social networking feeds, fashion blogs, and instant messenger sales help. The shopping service variable is categorized into two dimensions, personalized services, and interactive services. (Zimmerman, 2012)

Security

"The ability to handle online transactions and conduct ecommerce professionally" (Chen et al, 2010)

"The successful functioning of E-commerce security depends on a complex interrelationship between several applications development platforms, database management systems, and systems software and network infrastructure. Each phase of E-commerce transaction has a security measures. The key dimensions of E-commerce security are: Access Control – Privacy- Confidentiality- Authentication - Non Repudiation. - Integrity- Availability" (Yasin, et al, 2012)

Also it's been defined as "Security requirements can be studied by examining the overall process, beginning with the consumer and ending with the commerce server" (Islam, et al, 2015)

- **Confidentiality threats***:* Confidentiality is the prevention of unauthorized information disclosure. Breaching confidentiality on the internet is not difficult.
- **Integrity threats***:* An integrity threat exists when an unauthorized party can alter a message stream of information. Unprotected banking transactions are subject to integrity violations. Cyber vandalism is an example of an integrity violation. Cyber vandalism is the electronic defacing of an existing website page. Masquerading or spoofing – pretending to be someone you are not or representing a website as an original when it really is a fake –is one means of creating havoc on websites. Using a security hole in a domain name server (DNS), perpetrators can substitute the address of their website in place of the real one to spoof website visitors. Integrity threats can alter vital financial, medical, or military information.

- **Availability threats:** The purpose of availability threats, also known as delay or denial threats, is to disrupt normal computer processing or to deny processing entirely. (Islam, et al, 2015)

"Because e-commerce is operated on an open network, encryption technologies must be developed to deter hacker attacks. In particular, security failures reduce people's trust in e-payment systems and hinder the emergence of these systems" (Zhang and Wang, 2014)

Website-Security

Recent years, as the development of information technology and communication technology and the popularization of the Internet, E-commerce has been developed by leaps and bounds. However, security issues are emerging and have become the bottleneck of E-commerce development. Moreover, inherent complexity and uncertainty of E-commerce system security necessitate the participation of many experts in multi criteria decision making. Therefore, one of the key problems in assessing E-commerce system security is how to successfully combine experts' opinions in realistic decision making. (Liu, 2011)

"A security objective is the contribution to security that a system is intended to achieve. E-commerce is conducted on global network that is Internet which is untrusted. Therefore confidentiality is required during transaction and sending information should be kept secure against all type of threats. Security has emerged as an increasingly important issue in the development and success of an E-commerce organization" (Yasin et al, 2012)

"Websites also encounter a number of privacy threats, Due to the vulnerability of Internet; it is possible for hackers to attack these web sites. Some hackers prefer to change the entire server" (Jiang etc al, 2013)

Security for online payments

There are two main systems for transaction security, secure socket layer and secure electronic transaction.

1. **electronic transaction Secure Socket Layer (SSL)**

   SSL is the widely used secure service system and is an important measure to establish trust between online seller and buyer. Encryption and decryption allow secure transfer of information between an Internet browser and server. Data cannot be intercepted or changed during transmission. SSL also permits merchant identification through SSL server certificates.

   The SSL standard has been widely adopted because it is relatively simple and easy to use and does not place excessive demands on the average consumer's home PC, while at the same time reducing major concerns about the public nature of the communication infrastructure.

2. **Secure Electronic Transaction (SET).**

   SET is an alternative, more complex security system based on digital certificates and signatures. SET needs specific software and is more difficult for cardholders to obtain and use, and despite the high level of security offered it has not gained widespread use.

Suggested steps to protect personal information on website:

Some Suggested steps that have to be taken by organizations to protect personal information in the particular security risks within organizations. In determining appropriate security measures, organizations should:

- Identify the security risks to the personal information that is being held.
- Build up policies and procedures to reduce those identified risks.

- Apply suitable IT security settings governing system access.
- Monitor and measure performance against relevant international standards

(Tsiakis and Sthephanide, 2012) discussed the concept of security and trust in electronic payments. Although they discussed some of requirement and properties necessary to build successful electronic payment systems as listed below:

1. Integrity: confidence that information has not been changed after the data was signed.
2. Authentication: The process by which one person verifies that another entity is who they claim to be.
3. Fraud prevention and tolerance: prevention of parties from fraud and from economic losses in the case the system crashes or the network fails.
4. Privacy: information must not be revealed to not permit people.
5. Divisibility: option of numerous denominations.
6. Transferability: spending of token without the need to contact the issuer.

Privacy

Privacy was defined here as "The ability of an individual to control the terms under which their personal information is acquired and used." An individual's privacy, as such, is always in an inherent state of tension, since it must be defined in conjunction with capabilities of others to transact business and 40% of online shoppers were very concerned over the use of personal information, and 57% wanted some sort of laws regulating how personal information is collected and used. (Ackerman and Davis, 2003)

Also Privacy was defined as "Consumers trust about the performance of website during market transactions or consumption behavior." (Ling et al., 2010)

Data Integrity

“Data integrity assurance and protection from unauthorized modification In the process of their preservation or transfer” (Dzemydienė et al, 2010)

“About data integrity verification, because of data communication, transfer fees and time cost, the users cannot first download data to verify its correctness and then upload the data”(Chen, Hong Zhao,2012)

Data integrity “mean completeness or wholeness and it is basic requirement of information technology. Data integrity refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle. Data integrity ensures the data is the same as it was when it was originally recorded. Data integrity can be roughly divided into two overlapping categories Physical integrity and logical integrity Physical integrity deals with challenges related to storing and fetching of the data. Challenges for the physical integrity may include electromechanical faults, design flaws, material fatigue, corrosion, power outages, natural disasters, acts of war and terrorism. Physical integrity makes use of error detecting algorithms known as error correcting codes. Logical integrity is related with the correctness or rationality of a piece of data”. (Adilet and Ertem , 2013)

Integrity refers to the degree to which improper modifications to information are anticipated and prevented .Systems with superior integrity are better able to anticipate and prevent improper modification of information, such as faulty alteration, deletion, or addition. While some erroneous modifications of information are accidental, others may be made intentionally by unauthorized parties.

Common security measures to maintain integrity include digital signatures and anti-virus programs that prevent a virus from destroying data. (Hartono et al, 2014)

Data integrity refers to “maintaining and assuring the accuracy and consistency of data over its entire life cycle and it is a difficult aspect to the implementation, design and the usage of any system which stores the data, processes, or retrieves data. Data Integrity is given much more importance among the other cloud storage issues because only data integrity ensures that data is of high and good quality, correct, consistent and accessible.” (Daniel, 2015)

Confidentiality

Confidentiality defined as “data protection from unauthorized damage” (Dzemydienė, et al, 2010). “The brand is reputable and provides security measures.”(Zimmerman, 2012)

“Confidentiality refers to the degree to which improper disclosures of information are anticipated and prevented. Systems with superior confidentiality are better able to anticipate and prevent improper disclosure of information, such as leakage of information to an unauthorized party. A system's inability to anticipate and prevent improper disclosure of information may well indicate system insecurity.

Common security measures to maintain confidentiality include encryption and authentication such as password-based and token-based authentication” (Hartono, et al, 2014)

Authentication

Authentication **“**Refers to automatic identification of an Individual based on his distinguishing physiological and behavioral characteristics” (Zhang, 2002).

Authenticity is**”** Identification of the persons using the information system and protection against unauthorized access” (Dzemydienė et al, 2010)

Authentication “means by which both parties in an online transaction can be confident that they are who they say they are and non-repudiation is the idea that no party can dispute that an actual event online took place” (Raghallaigh, 2011)

As defined by (Business Dictionary) “Verification of the genuineness of a document or signature, to make it effective or valid. It usually takes the form of a sealed or stamped certificate that confirms the authority of a public official (such as judge or a notary public) or of a signatory”

About authentication “The key idea is to provide a encoded quantized data projection as authentication data. This can be correctly decoded with the help of an authentic data using as side information. Cryptography source coding provides the desired robustness against legitimate variations while detecting illegitimate modification. Additional adjustments might not change the meaning of the content, but could be misclassified as tampering. Users might also be interested in localizing tampered regions. Distinguishing legitimate encodings with possible adjustments from tampering and localizing tampering are the challenges addressed in this paper. We apply cryptography source coding and statistical methods to solve the data authentication problem” (Chouksey, et al., 2013)

Existing authentication methodologies involve three basic “factors”:

- Something the user knows (e.g., password, PIN);
- Something the user has(e.g., ATM card, smart card);
- Something the user is (e.g., biometric characteristic, such as a fingerprint).

Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed and

implemented multifactor authentication methods are more reliable and stronger fraud deterrents. For example, the use of a logon ID/password is single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses

(i.e., the card) combined with something the user knows (i.e., PIN). A multifactor authentication methodology may also include "out–of–band" controls for risk mitigation.

Mutual authentication

Mutual authentication is a process whereby customer identity is authenticated and the target Web site is authenticated to the customer. Currently, most financial institutions do not authenticate their Web sites to the customer before collecting sensitive information. One reason phishing attacks are successful is that unsuspecting customers cannot determine they are being directed to spoofed Web sites during the collection stage of an attack. The spoofed sites are so well constructed that casual users cannot tell they are not legitimate. Financial institutions can aid customers in differentiating legitimate sites from spoofed sites by authenticating their Web site to the customer.

Techniques for authenticating a Web site are varied. The use of digital certificates coupled with encrypted communications (e.g. Secure Socket Layer, or SSL) is one; the use of shared secrets such as digital images is another. Digital certificate authentication is generally considered one of the stronger authentication technologies, and mutual authentication provides a defense against phishing and similar attacks

Threats to User Identification and Authentication

The main goal of user identification and authentication is to validate the identity of the user. Computer systems typically require authentication. At the same time, attackers try to penetrate information systems and often their goal is to compromise the authentication mechanism protecting the system from unauthorized access. Attackers can take different approaches when they attempt to compromise the user identification and authentication mechanisms of a system, some of which are mention below:

1. Bypassing Authentication: If an attacker does not have a username and a password or other credentials, and is not able to authenticate to a system, he may try to bypass the authentication process. This can be accomplished in a number of ways, depending on the application, and the type of access that attackers have to the computer where the application is running.
2. Default Passwords: One of the major challenges of secure user authentication is represented by default passwords. Many software and hardware vendors assign default passwords for built-in users in their operating systems, software, and hardware.
3. Privilege Escalation: During the logon process, a user authenticates using a set of credentials. When a user tries to access resources, this request is actually performed by processes running on behalf of the user, that use the user access token to be authorized by resource servers.
4. Obtaining Physical Access: Security is not only a matter of strong authentication mechanisms, secure code, and cryptography. There are multiple other factors that affect the security of a system, and physical security is one of them.

Electronic Payment

“Electronic payment (e-payment) has become a popular means today for paying for online purchases made. The growth of internet has facilitated the popularity of this payment instrument as electronic commerce (e-commerce) has created new financial needs that in many cases cannot be effectively fulfilled by traditional payment systems”(Yen Teoh, etc al,2013)

- **The credit card**

  The credit card is the most popular payment method for online shopping today, despite its vulnerability to security breaches when used online. The credit card is a postpaid method.

- **The debit card**

The debit card (also known as a bank card or check card) is a plastic payment card that provides the cardholder electronic access to his or her bank account(s) at a financial institution. Some cards have a stored value with which a payment is made, while most relay a message to the cardholder's bank to withdraw funds from a payer's designated bank account. Online debit cards require electronic authorization of every transaction and the debits are reflected in the user’s account immediately. The transaction may be additionally secured with the personal identification number (PIN) authentication system; some online cards require such authentication for every transaction, essentially becoming enhanced automatic teller machine (ATM) cards. Stored-value card is often viewed as a prepaid method. Indeed, credit cards, stored-value cards, and smart cards all function like magnetic strip cards, but with different payment times. When the stored-value card is used in online commerce, customers must key-in certain identification numbers that match the information stored on the magnetic strip. The amount of the product or service is then deducted by the card reader and the reader rewrites information back to the card. ” (Zhang, Wang,2014)

E-payments have been reported to be the ultimate test of security and trust in e-business environment. In order to provide practical insight and guidelines for improving the trust and security of the e-payment, an investigative empirical study to evaluate these e-payment systems is needed, which is the primary motivation of this research. E-payment services exist as web-based user-interfaces that allow customers to remotely access and manage their bank accounts and transactions. The payment process involves a payer, a merchant and a bank. The entities transacting in a payment system are appointed by the specific commercial relationship which by itself may depend on series of conditions. E-payment systems that either currently available or have been previously put into practice for a period of time, including the credit card, the store-value card, the debit card and COD (cash on delivery).”(Zhang, Wang, 2014)

Characteristics of online payment systems

- Applicability: Availability (point of sale coverage), payment size (e.g. micropayments, large sums) and destination (e.g. merchants, private persons).
- Ease to obtain: Ease / complexity of registration.
- Reliability/ease of use: Simplicity, ease and transparency of use by customers and merchants.
- Cost: Distribution of costs between merchants and users; cost structure (e.g. fixed transaction charge or proportion of sales value).
- Security: Customer confidence and economic sustainability, information transmission mechanisms from buyer to seller, security of information stored on client and seller equipment.
- Liability: Legislative protection and provisions, coverage of potential losses.
- Anonymity: Protection of personal information; tradeoffs between anonymity and traceability for payment support

2.2 Previous Studies

(Alqatan et al., 2016)

Entitled "An Empirical Study on Success Factors to Enhance Customer Trust for Mobile Commerce in Small and Medium-sized Tourism enterprises in Jordan"

This research studies mobile technologies and wireless communications and explain the dramatic growing in M-commerce world and the great impact it has on the domain .As E-commerce and M-commerce, Trust has been an important factor in affecting consumers' behavior to accept and adopt a specific technology, especially when it comes to situation of uncertain environments. Also, it focuses on trust which that considers a main purpose of accepting M-commerce. The research focus specifically on Small and Medium-sized Tourism Enterprises (SMTEs) where Trust is an important aspect and the value created lifetime and invaluable. The study distributed the questionnaire to 361 respondents employed in Jordanian SMTEs. The study compares Familiarity with M-commerce, Calculative-based trust, Structural assurance, Propensity to trust, and Compatibility.

Results of the analysis showed that all factors, except for 'structural assurance' and 'calculative-based trust', affect the user's trust in such applications. The study provides a clear understanding of decision maker's perception about M-commerce acceptance in their businesses. This study is important in a global context, as SMTEs in Jordan are going for exporting their product in the global marketplace.

The reason of this study main focus is to examine the critical factors that influence customer trust for the acceptance of M-commerce by SMTEs in developing countries. Furthermore, actors influencing trust in M-commerce acceptance by SMTEs in developing countries. As results

indicate, Familiarity with M-commerce, compatibility, Propensities to trust and perceived security were found to be significant.

(Daştan and Gürler,2016)

Entitled "Factors Affecting the Adoption of Mobile Payment Systems: An Empirical Analysis "

The paper discussed and investigated the overview factors effecting adoption of mobile payment systems by the consumer in Turkey. Pointing out to widespread of mobile technology now a days and how smart mobiles revelation increase the usage of mobile transactions and facilitate business process. With this technology, companies took advantage of the technology progressive to develop business and reach customer. Because competition are button click away, motivate through it mobile technology progress and various payment system.

The major objective of this study has determine the direction of the effects of factors such as perceived trust, perceived usefulness, perceived ease of use and perceived mobility on adoption of MPS (Mobile Payment System). The structural model in the study was built based on previous factors .In addition, the research was applied on total of 225 online questionnaires, concluding the following results:

- The study did not detect any significant evidence for Perceived Usefulness and Perceived Ease of Use factors on the adoption of MPS.
- There is a positive effect of reputation and negative effect of environmental risk on Perceived Trust factor. The results of this study did not show any significant effect between the perceived ease of use and Adoption of MPS

(Punyani et al, 2015)

Entitled "Examining Factors Affecting Females' Perception towards the Usage of electronic Payments System: An Exclusive Study on E-Shopping"

The study highlighted the effective participation of female and factors that affect their payment decision, the wide usage of electronic shopping especially young female's customer. This study attempted to understand female consumer's online purchase behavior, and strategies that website apply to attract those targeted customer. Explaining facts how female customer decisions are influenced by perception, motivation, learning, attitudes and beliefs, and how it shape the permanent usage. Through analyzing factors influence the consumers' attitude to adopt online shopping: (a) Convenience (b) Security (c) Price & Selection (d) Information & Review. Also identify the various online shopping concerns involved.

Most online consumers are not utilizing online shopping facilities widely; because of security concerns, users being more comfortable with their current shopping and banking methods, and privacy concerns. Therefore, 196 questionnaires responds were analyze and study, concluding from it several facts and results:

- Females with a highly positive attitude towards purchasing online. Starting from demography, the findings indicated that maximum numbers of online female shoppers are young females and elderly women are not so eager online shopping.

- As a result of Frequency of buying, consumers usually buy once every 2-3 months on an average and average amount spent is between Rs. 1000-5000.

The second part of the analysis is studding factors influencing online consumers. From the results researcher concluded that the most influential and attractive factor among four factors is Information & Reviews with average percentile of 81, following security that is second most influencing factor with average score of 78 percentile, Price & Selection with average score 77 percentile and Convenience with average of 73 percentile is also important.

(Sen et al., 2015)

Entitled "A Study on E-Commerce Security Issues and Solutions"

Referred to the researchers, E-commerce recently considers an essential approach and a key role to expand business to reach worldwide. Provide methodology how to run a successful website. Also they point out to the advantages with features of E-commerce and how it facilitates the process to customer and companies.

Moreover, mention threats that E-commerce website exposed to. Since information on E-commerce website could be disclose through hacking, fraud and manipulation, applying security protocols will create successful E-commerce transaction. From different perspectives researchers conclude that website will face more attacks with less protection procedures and process.

The paper discussed the overview of E- Commerce, security issues in e-commerce, threats in e-commerce, key dimensions of e-commerce security, various security protocols. While the research study specifically about the Effect of Website Security on E-Payment from this perspective.

(Yee and Yazdanifard1, 2014)

Entitled "How Customer Perception Shape buying Online Decision"

The study highlighted on the role of customer in online shopping and the factors that affect customer buying decision. Also, focus in building up a long relation with the customer and then convert this customer into loyal customer generating customer loyalty. Researchers spotlight on the stages of perception process and generation the right decision during it.

Besides measuring customer satisfaction rate through shopping experience. The researcher reaches facts about how to motivate customer perception and ways to increase progression off E-commerce website as whole. The study focus on big companies that turned into E-world business. The researcher toke relevant variables such as consumers' perceptions, satisfaction and loyalty to activate online process but this research will take one variable customer perception and the effect of web security on it.The model that was created shows the differences between the interaction of stimuli, consumer characteristics, decision process and consumer response before they choose a product. The research was gather by using 50 respondents to test about how they response in different interaction.

(Hartono et al., 2014)

Entitled "Measuring perceived security in B2C electronic commerce website usage: A specification and validation"

This paper aims to clarify the concept of business-to-consumer electronic commerce (B2C ecommerce) which facilitate the process of buying and selling between customer and retailers, providing through it easier and cheaper methods that smooth business transactions.

As a result, these research focuses on dimensions of security which lead business retailers generate profit as well as customer fulfill their needs. Also, the research spot light on validation scope and its criteria that lead to achieve to security stage, while this research overview E-commerce and security concept form confidentiality, data Integrity and authentication perspective.

(Chu and Kang, 2014)

Entitled "The Effects of Customers' Perceived Relational Benefits on the Customer Perception of Service Innovation at Service Centers for IT Products: The Mediating Role of Customer Participation"

This research observes the relationships between customers' perceived functional benefits from service providers and customers' perception of service innovation.

The data in this research collected from 116 university students in South Korea.

The theory of service innovation is basically regarding product and process innovation. It's new or improved intangible benefit offered and provided by a company to the customers.

Furthermore, the research discuss the Relational benefits which is benefits arising from a long-term relationship between a company or a service provider and its customers.

The structural model in the study was built based on Perceived relational benefits; customers' participation and customers' perception of service innovation. The purpose is to conclude the relationship between those variables and their effect customer participation as the mediator.

In compare with my research paper which study the customer from one perspective and the effect of that on conducting payment and reach buying decision.

(Al rawabdeh et al.,2012)

Entitled "The Importance of Trust and Security Issues in E-Commerce Adoption in the Arab World"

The research indicates that adoption E-commerce in Arab world will change business path superiorly, generate profit and motivate companies to advance. Furthermore, the significant key role of this study is regarding web security in developing trust relation with customer and benefits from applying E-commerce.

The theoretical concepts mentioned in research the techniques that can be adopted by the companies in Arab world. These include data Encryption, Secure Socket Layer (SSL) Certificates and Certificates with Extended Authentication Validation (EV) and Trustmark.

The study draw conclusions about E-C adoption level in Arab world, user low participation and security, confidentiality issues as main measurement of adoption and conurbation in E-commerce website.

The aim of the paper to determine that security has dramatically impact on customer analysis and attitude toward E-commerce acceptance. As well as gaining customer trust to finalize the adoption process. In compare with this research that spotlight on Jordanian online website clearly.

Furthermore, study recommends focusing on factors such as level of satisfaction, trust and loyalty and their impact on improving opportunities of E-commerce business in Arab world, beside customer value and culture.

(Khalili et al., 2012)

Entitled "Evaluation of e-payment systems in Iran using analytic hierarchy process"

This research studies the Electronic payment system of companies in Iran. Pointing out to the facilitation that E-payment provide in E-world as of speed, digitization and global accessibility. Also, E- Payment provide economic, financial and monetary dimension in different sectors generating profit as well as providing competitive advantage to companies.

According to the writer there is 5 types of E-payment used in Iran which are electronic money, credit card, debit card, charging card and electronic check.

The study compares different payment methods and system, choosing the most appropriate method to the business in general.

The study tries to answer the following questions to conclude facts and result;

1. What are common e-payment methods in Iran?
2. Which criteria exist for evaluation of e-payment systems?
3. What is the ranking of e-payment systems?

The model here was built based on security criteria such as Authority, Privacy, and Integrity, Not be faked, Non-repudiation, Anonymity, and socioeconomic criteria such as Reliability, Degree of acceptability, User range, cost of transactions.

Through examine 5 types of electronic payment system the study concludes that each one has advantage, disadvantage and limitation to companies beside customers based on safety concern. The result shows that debit card is the best option followed by credit then E-check.

(Guo and Wong, 2012)

Entitled "A Dynamic Account Payment Method for Integrating Heterogeneous B2C Electronic Payment Systems"

This study explains and clarifies the difference between customer payment approach and a B2C e-payment system which lead to payment conflict among parties. This paper suggests a new dynamic account payment (DAP) method to resolve the conflict. This can be achieved by temporary e-payment account for the customer through a third party in feasible and efficient way; this technique guarantee successful transaction. Also, research represents two alternative implementations of DAP method manual approach and an automatic approach.

The research concludes results that Automatic Approach is more efficient than Manual Approach, by selecting the higher performance of E-payment system as indicator of adopting Automatic Approach. DAP method is a significant contribution to varied B2C e-payment integration.

(Yazdanifard et al., 2011)

Entitled "Security and Privacy Issues as a Potential Risk for Further Ecommerce Development"

The study focused on E-commerce website security and privacy as a main measurements and critical factors on website success or failed. In addition, writers mention the effect of those standers on B2B and B2C transactions. Include security issues such as privacy, confidentiality, integrity, authentication, non-repudiation, availability and effectiveness.

According to the research writers, the adoption of new and innovative technology systems will help to create secure environment for both customer and retailers. Also facilitate the E-commerce development process through following International regulations and procedures for website safety.

This research studies the E-commerce environment and focus on the importance of security and privacy for the customers as indicator to develop online relations and trust online website. As my research highlighted on the role of web security on and how it affect customer to reach buying decision and trust website.

(Dzemydienė et al., 2010)

Entitled "Evaluation of Security Disturbance Risks in Electronic Financial Payment Systems"

The aim of this paper is to analyze the development of information and communication technologies (ICT) which ensure the development of new security approaches in e-payment processes in Europe. The research tries to enhance safety support systems; this can be achieved through applying improved safety requirements and standards.

The paper highlighted on the financial vulnerability and potential risk factors in Electronic payment systems. The research mentions the risk factors in estimating safety procedures and measures for electronic payment. The writers examine several software and hardware systems that can use by hackers to retrieve personal data through misleading users.

The results represent major safety components in e-payment compensation. Through development of information and communication technologies (ICT) risk factors will be minimize, insure people and business data confidentiality and facilitate the implementation of advance ICT.

(Jing, 2009)

Entitled "On-line Payment and Security of E-commerce"

This paper discusses the creation of electronic commerce environment where online electronic payment is essential process and foundation of running business successfully.

The researcher assumed that electronic payment system is the basis for online payments, and online payments system development is an advance form of electronic payment. Considering electronic payment is the key role to ensure fast and convenient online shopping experience to customers. Also E-payment ensures safety and confidentiality to parties in transaction process.

The model here was built based on SET (security electronic transaction) it

's basically about providing data security, integrity and non-repudiation of transactions, to ensure that no leaking of information to the other account accounts in the business. Also the results indicate to maintain security in SET transactions such as E-cash and e-payment, system must have those characteristics Anonymity, Not shadowing; ,Savings on transaction costs; Savings on transmission costs; Poor risk; Pay flexibility; Prevent forgery and repeatability.

The writer recommends implanting safety standers via using secure network for the transaction between sender and recipient that ensure confidentiality of information exchanged.

(Kim et al, 2009)

Entitled "An empirical study of customers' perceptions of security and trust in e-payment systems"

Because of the rapid growth in Korea IT market, this paper examine different payment system in Korea , Focusing on Electronic payment system (EPS) as important role in executing wide-ranging activities and actively in E-commerce world. Moreover, it also present a theoretical foundation and practical guidelines for service providers in dealing with the security aspects of E-payment systems, Explaining different EPS brands such as Easycash, Easypaydirect, Inipay, iCash, eGate, eCredit, Smartpay,have been established recently . The structural model in this paper is employed to analyze data collected from 219 respondents in Korea.

The build Model here focus on the security issues influencing customers' participation in a mobile payment procedure and classify the security concept into two dimensions: objective security and subjective security. Also technical protections and security statements are significant factors for improving consumers' perceived security which show that consumers' perceived security is positively related to consumers' perceived trust and EPS use. To conclude, the findings confirm direct relationships between perceived security, perceived trust, and EPS use. The results clearly outline the role of consumers' perceived security in building the trust of consumers and the positive impact of both perceived security and perceived trust on EPS use.

Chapter Three

Methods and procedures

(3-1) Introduction

(3-2) Methodology of the Study

(3-3) Population and Sample of the Study

(3-4) Descriptive Analysis of the Demographic Variables

(3-5) Tools and Data Collection

(3-6) Statistical Treatment

(3-7) Validity and Reliability

(3-1) Introduction

In this chapter, the researcher will describe in detail the methodology used in this study, and the study population and its sample. Next, the researcher will design the study model and explain the study tools and the way of data collection. After that, the researcher will discuss the statistical treatment that used in the analysis of the collected data. In the final section, the validation of the questionnaire and the reliability analysis is applied.

(3-2) Methodology of the Study

It is important to choose the method that best reflects the objective of the paper. Method is the tool and technique used to obtain and analyze research data, including for example questionnaires, observation, interviews, and statistical and non-statistical techniques. The most common method to collect data is by using a questionnaire with an advance formulated alternatives to answer, in order to collect the necessary data to achieve the main purpose of the study. The researcher collected primary data through a questionnaire which was distributed to customers of Jordanian shopping websites, where they been chosen randomly. The descriptive research is basically describing characteristics of a population or a phenomenon. In addition, descriptive studies involve collecting data in order to test hypotheses and answer questions concerning the current status of the subject. Typical descriptive studies are concerned with the assessment of attitudes, opinions, demographic information, conditions, and procedures.

The researcher designed a special questionnaire to collect data from the study sample.

(3-3) Study Population and Sample

The population of the study includes customers of Jordanian shopping website. (620) questionnaires send via face book as a sample of the study, only (469) questionnaires returned, the responds rate was (75.6%) from the total questionnaires. Also (2) of the returned questionnaires were eliminated from the statistical analysis thus to the insufficient answers. Therefore, (467) questionnaires were analyzed, that mean approximately (75.3%) from the total distributed questionnaires.

3-4: Demographic Variables of Study Sample

Tables (3-1); (3-2); (3-3) and (3-4); show the demographic variables of the study sample

Table (3-1) Description the Gender of the study sample.

Table (3-1) shows that the (37.7 %) of the sample are male and (62.3) are female.

Table (3-1) Description the Gender of the study sample

Variables	Categorization	Frequency	Percent %
Gender	**Male**	**176**	**37.7**
	Female	**291**	**62.3**
Total		**467**	**100 %**

Table (3-2) Description the Age of the study sample

Table (3-2) show that (11.8%) of the sample age less than 25 Years, (50.7%) of the sample range Aged between 25-34 Years, (31.5%) of the sample range Aged between 35-44Years , (4.5%) of the sample range Aged between 45-54 and (1.5%) of the sample range Aged more than 55 Years.

Table (3-2) Description the Age of the study sample

Variables	Categorization	Frequency	Percent %
Age	Less than 25 Years	55	11.8
	From 25 -34 Years	237	50.7
	From 35-44 Years	147	31.5
	From 45-54 Years	21	4.5
	55 Years and more	7	1.5
Total		467	100%

Table (3-3) shows that the (32.9%) of the sample are Single, (63.2%) are married and (3.9%) divorced.

Table (3-3) Description the Marital status of the study sample

Variables	Categorization	Frequency	Percent
Marital status	Single	154	32.9
	Married	295	63.2
	Divorced	18	3.9
Total		467	100

The educational level as clarified in table (3-4) ; shows that all members of the study sample have a scientific qualification which is a good sign in adopting the high educational qualifications to accomplish their work.

Table (3-4) Description the Academic degree of the study sample

Variables	Categorization	Frequency	Percent
Educational Level	**Hi School**	**32**	**6.9**
	Diploma	**65**	**13.9**
	Bachelor degree	**314**	**67.2**
	Masters	**47**	**10.1**
	PHD	**9**	**1.9**
Total		**467**	**100**

3-5: Study tools and Data Collection

The current study is of two folds, theoretical and practical. In the theoretical aspect, the researcher relied on the scientific studies that related to the current study. Whereas in the practical aspect, the researcher relied on descriptive and analytical methods using the practical manner to collect, analyze data and test hypotheses.

The data collection, manner of analysis and programs used in the current study are based on two sources:

1. Secondary sources: books, journals, and theses to write the theoretical framework of the study.
2. Primary source: a questionnaire that was designed to reflect the study objectives and questions.

In this study, both primary and secondary data were used. The data collected for the model was through questionnaires. After conducting a thorough review of the literature pertaining to study variables, the researcher formulated the questionnaire instrument for this study.

The questionnaire instrumental sections are as follows:

Section One: Demographic variables. The demographic information was collected with closed-ended questions, through (4) factors (Gender; Age; Educational level; and Marital status).

Section Two: Independent variable: **Website Security (**Privacy, Confidentiality, Data Integrity and Authentication)

Privacy: The ability of an individual to control the terms under which their personal information is acquired and used. Were measured through (6) items on five Likert-type scales, from item (1-6).

Data Integrity: mean completeness or wholeness and it is basic requirement of information technology. Data integrity refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle. Were measured through (5) items on five Likert-type scales, from item (7-11).

Confidentiality "data protection from unauthorized damage" was measured through (5) items on five Likert-type scales, from item (12-16).

Authentication "Refers to automatic identification of an Individual based on his distinguishing physiological and behavioral characteristics" was measured through (5) items on five Likert-type scales, from item (17-21).

Section Three: Dependent variable: E- Payment usage: (e-payment) has become a popular means today for paying for online purchases made was measured through (5) items on five Likert-type scales, from item (22-26).

The scale is as follow:

Strongly Agree	Agree	Agree to an Extent	Disagree	Strongly Disagree
5	4	3	2	1

3-6: Statistic Treatment

The data collected from the responses of the study questionnaire was used through Statistical Package for Social Sciences (SPSS), the researcher used the following suitable statistical methods that consist of:

- _ *Percentage and Frequency*.
- *Cronbach Alpha reliability* (α) to measure strength of the correlation and coherence between questionnaire items.
- *Arithmetic* to identify the level of response of study sample individuals to the study variables.
- *Standard Deviation*: to measure the responses spacing degree about Arithmetic Mean.
- Variance Inflation Factor and Tolerance to make sure that there are no Multicollinearity between independent variables.
- *Multiple and Simple Regression analysis* to measure the impact of study variables on testing the direct effects.

$$\text{Class Interval} = \frac{\text{Maximum Class} - \text{Minimum Class}}{\text{Number of Level}}$$

$$\text{Class Interval} = \frac{5-1}{3} = \frac{4}{3} = 1.33$$

The Low degree from 1- less than 2.33

The Medium degree from 2.33 – 3.66

The High degree from 3.67 and above.

(3-7) Validity and Reliability Validation

Validation

To test the questionnaire for clarity and to provide a coherent research questionnaire, a macro review that covers all the research constructs was thoroughly performed by academic reviewers from Middle East University and other universities specialized in faculty and practitioners E-Business, Business administrative. Some items were added, while others were eliminated based on their valuable recommendations. Some others were reformulated to become more accurate to enhance the research instrument.

Reliability

Cronbach's alpha, was used to determine the internal consistency reliability of the elements comprising the four constructs as suggested by Gregory (2004). Reliability should be approximately (0.70) or higher to indicate adequate convergence or internal consistency (Hair et al., 2006). These results are the acceptable levels as suggested by (Hair, et. al., 2006). The results were shown in Table (3-5).

Table (3-5) Reliability of Questionnaire Dimensions

No.	Variable	Dimensions	No. of items	Alpha Value (α)
1	**Website Security**		21	0.773
(1-1) (1-2) (1-3) (1-4)		Privacy	6	0.753
		Confidentiality	5	0.685
		Data Integrity	5	0.718
		Authentication	5	0.783
2	**E-Payment**		5	0.856

Chapter Four

Analysis of the Results & Hypotheses Testing

(4-1) Introduction

(4-2) Descriptive Analysis of Study Variables

(4-3) Analysis Adequacy of the Data to Test the Study hypotheses

(4-4) Hypotheses Testing

(4-1) Introduction

According to the purpose of the research and the research framework presented in the previous chapter, this chapter describes the results of the statistical analysis for the data collection according to the research questions and hypotheses. The data analysis includes a description of the Means and Standard Deviations for the questions of the study; Multiple and Simple and Linear Regression analysis used.

(4-2) Description analysis of study variables

4-2-1 Website Security

The researcher used the arithmetic mean, standard deviation, one sample t-test, item importance and importance level as shown in Table (4-1).

Table (4-1)

Arithmetic mean, SD, item importance and importance level of

Website Security dimensions

No.	Website Security	Mean	St. D	Sig	Item importance	Importance level
1	**Privacy**	3.982	0.848	0.000	2	High
2	**Data Integrity**	4.145	0.748	0.000	1	High
3	**Confidentiality**	3.750	0.638	0.000	4	High
4	**Authentication**	3.852	0.655	0.000	3	High
Average Arithmetic mean and standard deviation		3.932	0.712			

t- Value Tabulate at level ($\alpha \leq 0.05$)

t- Value Tabulate was calculated based on Assumption mean to item that (3).

Table (4-1) clarifies the importance level of Website Security dimensions, where the arithmetic means for dimensions range between (3.750–4.145) compared with Average Arithmetic mean amount of (3.932). We observe that the High mean for the "**Data Integrity**" with arithmetic mean (4.145), standard deviation (0.748). The lowest arithmetic mean was for the "Confidentiality" with Average (3.750) and standard deviation (0.638). In general, it appears that the importance level of **Website Security** from Jordanian Customer Perspective under study from the study sample viewpoint was high

Table (4-2)

Arithmetic mean, SD, item importance and importance level of Privacy

No	Privacy	Mean	St. D	Sig	Item importance	Importance level
1	If I do not know how a websites handles my privacy, I do not continue shopping on that website.	**4.169**	**0.780**	**0.000**	**1**	**High**
2	If I am buying from a website for the first time, I look at their privacy policy.	**3.995**	**0.838**	**0.000**	**3**	**High**
3	The web site is not allowed to share information about what you purchased with other companies.	**3.625**	**0.956**	**0.000**	**5**	**Median**
4	The web site can change their privacy policy without telling me.	**4.115**	**0.755**	**0.000**	**2**	**High**
5	A web site must get their privacy policy reviewed by the government on an annual basis.	**3.449**	**0.962**	**0.000**	**6**	**Median**
6	Internet privacy policies are required by law.	**3.773**	**0.696**		**4**	**High**
Average Arithmetic mean and standard deviation **Privacy**		**3.982**	**0.848**			

t- Value Tabulate at level ($\alpha \leq 0.05$) t- Value Tabulate was calculated based on Assumption mean to item that (3)

Table (4-2) Clarifies the importance level of privacy, where the arithmetic means range between (3.449 - 4.161) compared with general arithmetic mean amount of (3.982). We observe that the highest mean for the item " ***If I do not know how a websites handles my privacy, I do not continue shopping on that website"*** with arithmetic mean (4.161), Standard deviation (0.780). The lowest arithmetic mean was for the item " ***A web site must get their privacy policy reviewed by the government on an annual basis***" with average (3.449) and Standard deviation (0.962). In general, it appears that the Importance level of Privacy in from the study sample viewpoint was high.

Table (4-3)

Arithmetic mean, SD, item importance and importance level of Data integrity

No	**Data integrity**	Mean	St. D	Sig	Item importance	Importance level
7	A website must ensure that my data are not subjected to modification.	**4.149**	**0.676**	**0.000**	**4**	**High**
8	Having personal profile is guaranty of I Integrity.	**4.269**	**0.648**	**0.000**	**1**	**High**
9	I think that website providing all the necessary information to customer.	**4.162**	**0.920**	**0.000**	**3**	**High**
10	I feel comfortable surfing this website.	**4.197**	**0.717**	**0.000**	**2**	**High**
11	This website makes it easy for me to build a relationship with this company	**4.014**	**0.827**	**0.000**	**5**	**High**
General Arithmetic mean and standard deviation **Data integrity**		**4.145**	**0.748**			

t- Value Tabulate at level ($\alpha \leq 0.05$)

t- Value Tabulate was calculated based on Assumption mean to item that (3).

Table (4-3) clarifies the importance level of brand elements, where the arithmetic means range between (4.014 – 4.269) compared with general arithmetic mean amount of (4.145). We observe that the highest mean for the item " ***Having personal profile is a guaranty of Data Integrity."*** with arithmetic mean (4.269), Standard deviation (0.648). The lowest arithmetic mean was for the item " ***This website makes it easy for me to build a relationship with this company***" with Average (4.014) and Standard deviation (0.827). In general, it appears that the Importance level of **Data integrity** from the study sample viewpoint was high.

Table (4-4)

Arithmetic mean, SD, item importance and importance level of Confidentiality

No	**Confidentiality**	Mean	St. D	Sig	Item importance	Importance level
12	I would totally trust website with my personal information.	**4.159**	**0.658**	**0.000**	**2**	**High**
13	I would allow website to access to my personal Data.	**3.259**	**0.633**	**0.000**	**4**	**Median**
14	It's all right if the website keeps my financial information and records.	**2.589**	**0.619**	**0.000**	**5**	**Low**
15	A website can access to my data while surfing it.	**4.258**	**0.657**	**0.000**	**1**	**High**
16	It's okay with me if website uses my information for other purposes	**3.589**	**0.671**	**0.000**	**3**	**Median**
General Arithmetic mean and standard deviation **Confidentiality**		**3.750**	**0.638**			

t- Value Tabulate at level ($\alpha \leq 0.05$)

t- Value Tabulate was calculated based on Assumption mean to item that (3).

The researcher used the arithmetic mean, standard deviation, item importance and importance level as shown in Table (4-4).

Table (4-4) clarifies the importance level of Branding strategy, More the arithmetic means range between (2.589- 4.258) compared with General Arithmetic mean amount of (3.719). We observe that the highest mean for the item " ***A website can access to my data while surfing it"*** with arithmetic mean (4.258), standard deviation (0.657). The lowest arithmetic mean was for the item " ***It's all right if the website keeps my financial information and records***" with Average (2.589) and Standard deviation (0.619). In general, it appears that the importance level of Branding strategy in companies under study from the study sample viewpoint was high.

Table (4-5)

Arithmetic mean, SD, item importance and importance level of Authentication

No	**Authentication**	Mean	St. D	Sig	Item importance	Importance level
17	It's acceptable if unauthorized employee can access to my personal and financial data.	**3.698**	**0.657**	**0.000**	**3**	**High**
18	I believe knowing employee information encourage me to relief my information.	**3.598**	**0.671**	**0.000**	**5**	**High**
19	I trust the website owner and employee with my information.	**4.158**	**0.678**	**0.000**	**1**	**High**
20	I think that website Authentication affects my e-payment decision.	**3.654**	**0.646**	**0.000**	**4**	**High**
21	In my opinion choosing website Authentication is a key of success.	**4.152**	**0.637**	**0.000**	**2**	**High**
General Arithmetic mean and standard deviation **Authentication**		**3.852**	**0.655**			

t- Value Tabulate at level ($\alpha \leq 0.05$) - t- Value Tabulate was calculated based on Assumption mean to item that (3).

The researcher used the arithmetic mean, standard deviation, item importance and importance level as shown in Table (4-5).

Table (4-5) clarifies the importance level of Authentication, where the arithmetic means range between (3.598 - 4.158) compared with General Arithmetic mean amount of (3.852). We observe that the highest mean for the item " ***I trust the website owner and employee with my information***.***"*** with arithmetic mean (4.158), standard deviation (0.678). The lowest arithmetic mean was for the item " ***I believe knowing employee information encourage me to relief my information***" with Average (3.598) and Standard deviation (0.671). In general, it appears that the importance level of Authentication from the study sample viewpoint was high.

4-2-2 E- Payment

Table (4-6)

Arithmetic mean, SD, item importance and importance level of *e Payment*

No	e Payment usage	Mean	St .D	Sig	Item importance	Importance level
22	I prefer website that offers offline payment option (cash).	**3.453**	**0.646**	**0.000**	**2**	**Median**
23	E- Payment option facilitates buying process.	**3.689**	**0.637**	**0.000**	**1**	**High**
24	It is matter if website offer several E-payment options (like visa- PayPal – credit card-diept card…etc).	**3.158**	**0.618**	**0.000**	**4**	**Median**
25	I think that paying in E-payment is much safer than cash.	**2.156**	**0.658**	**0.000**	**5**	**Low**
26	I think that paying in E-payment is much easy than cash.	**3.258**	**0.633**	**0.000**	**3**	**Median**
General Arithmetic mean and standard deviation **e payment**		3.142	0.632			

t- Value Tabulate at level ($\alpha \leq 0.05$)

t- Value Tabulate was calculated based on Assumption mean to item that (3).

The researcher used the arithmetic mean, standard deviation, item importance and importance level as shown in Table (4-6).

Table (4-6) clarifies the importance level of Marketing Strategy, where the arithmetic means range between (2.156 - 3.689) compared with General Arithmetic mean amount of (3.142). We observe that the highest mean for the item " ***E- Payment option facilitates buying process"*** with arithmetic mean (3.689), Standard deviation (0.637). The lowest arithmetic mean was for the item "***I think that paying in E-payment is much safer than cash.***" With Average (2.156) and Standard deviation (0.658). In general, it appears that the Importance level of ***e payment*** in firms under study from the study sample viewpoint was Median.

(4-3): Analysis adequacy of the data to test the study hypotheses

Before testing the study hypotheses, the researcher conducts some important tests to ensure the data adequacy for the regression assumption analysis as follows:

1. Variance Inflation Factor (VIF), this test used to measure how the multicollinearity can inflate the variance of regression, the coefficient should not exceed a value of (10).
2. Tolerance used to test the multicollinearity between independent variables, tolerance value should be greater than (0.05).
3. Skewness conducted in order to test that the data follow normal distribution, Skewness value is less than (1.0).

(4-3-1): Multicollinearity

Table (4-7)

Variance Inflation Factor, Tolerance tests

Website Security	Tolerance	VIF
Privacy	0.658	1.669
Data Integrity	0.565	1.145
Confidentiality	0.257	1.685
Authentication	0.477	1.936

According to the result shown in table (4-7), there is no multicollinearity between the independent variables, this is confirmed from the values of variance inflation factor (VIF) of the dimensions are (1.669 ; 1.145 ; 1.685 ; 1.936) , respectively, less than (10) . As can be seen, the values of Tolerance ranged between (0.257 - 0.658) which is greater than (0.05) this is an indication that there is no multicollinearity between the independent variables.

(4-3-2): Dependability of Dependent Variable:

Multiple regressions assume that variables have normal distributions. This means that errors are normally distributed, and that a plot of the values of the residuals will approximate a normal curve.

Table (4-8)

Pearson's Correlation research variables matrix

	Privacy	Data Integrity	Confidentiality	Authentication
Privacy	1.000			
Data Integrity	0.118	1.000		
Confidentiality	0.251	0.317	1.000	
Authentication	0.085	0.122	0.125	1.000

**. Correlation is significant at the 0.01 level (2-tailed).

The researcher use Pearson correlation analysis to find if there is multicollinearity between the independent variables. According to the result shown in table (4-9), the independent variables are un correlated, and there is no multicollinearity between the independent variables

(4-4) Hypotheses Testing

The researcher in this part tested the hypotheses, through Multiple and simple Linear Regression analyses with (F) test using ANOVA table analysis as follows:

(4-5): First Main Hypothesis

H01: There is no direct effect of Website security on E-payment usage *at the level ($\alpha \leq 0.05$).*

To test this hypothesis, the researcher uses the simple regression analysis to ensure the direct effect of Website Security on **E-payment usage** in Jordanian websit shopping industries at the level ($\alpha \leq 0.05$). As shown in Table (4-10).

Table (4-9)

Simple Linear regression model to test the effect of Website security on E-payment usage.

	R	(R^2)	F calculated	Sig*	Beta	T Calculated	Sig*
The effect of Website security on E-payment usage.	0.489	0.239	48.363	0.000	0.489	9.558	0.000

***The impact is significant at level ($\alpha \leq 0.05$) * (n-1 = 466) * (T tabulated = 1.96)**

From table (4-9) the researcher observes that there is a positive direct effect of Website security on E-payment usage among Jordanian website shopping. The (R) was (0.489) at level ($\alpha \leq 0.05$), whereas the (R^2) was (0.239). This means the (0.239) of E-payment usage among Jordanian website shopping industries changeability's results from the changeability in Website security. As (Beta) was (0.489) this means the increase of one unit in website security will increase E-payment usage of website shopping value (0.489). Confirms significant impact (F) Calculate was (48.363) and its significance at level ($\alpha \leq 0.05$), and accepted hypothesis:

Website security has a positive direct effect on E-payment usage Jordanian website shopping industries at the level ($\alpha \leq 0.05$).

(4-6) Sub Hypothesis test

H01.1: There is no direct effect of privacy on E-payment Usage in Jordanian shopping website at the level ($\alpha \leq 0.05$).

H01.2: There is no direct effect of confidentiality on E-payment Usage in Jordanian website shopping at the level ($\alpha \leq 0.05$).

H01.3 There is no direct effect of data Integrity on E-payment Usage in Jordanian shopping website at the level ($\alpha \leq 0.05$).

H01.4: There is no direct effect of on E-payment Usage in Jordanian website shopping at the level ($\alpha \leq 0.05$).

Table (4-10)

Multiple regression analysis to test Website Security (Privacy, Confidentiality, Data Integrity, Authentication) effect on e payment Jordanian website shopping

Dependent variable	R	(R^2)	F Calculate	DF	Sig*	Independent variable	T Calculated	Sig*
E-payment usage	0.418	0.174	22.854	466	0.000	Privacy	9.185	0.000
				466		Confidentiality	3.658	0.028
				466		Data Integrity	6.354	0.016
				466		Authentication	8.365	0.000

***The impact is significant at level ($\alpha \leq 0.05$) * (n-1 = 466) * (T tabulated = 1.96)**

Privacy and Authentication have more effect on E-payment usage and that's because of the low significance rate and the high proportion of T.

To test this hypothecs the researcher use the multiple regression analysis to ensure the direct effect of website security (Privacy, Confidentiality, Data Integrity, Authentication) on e-payment usage in Jordanian shopping website, As shown in table (4-10).

The regression model achieves a high degree of fit, as reflected by (R) (0.418) and (R^2) (0.174), which asserted that (0.174) of the explained variation in e payment usage can be accounted for website security. As well as table, (4-11) shows, the analysis of variance of the fitted regression equation is significant with (F) value of (22.854). This is an indication that the model is a

good one. Since the p-value is less than (0.05), it shows a statistically significant effect of website security on E-payment usage.

(4-7)Sub Hypothesis analysis

H01$_1$: Privacy has a positive direct effect on e-payment in Jordanian shopping websites at the level ($\alpha \leq 0.05$).

From table (4-11) the researcher observes that there is a positive direct effect of Privacy on e- payment usage in Jordanian shopping websites. As shown in the above table the (T) calculated is greater than the (T) tabulated where the calculated is (9.185), while the (t) tabulated is (1.96). According to the result reached, we reject the null hypothesis and accept alternative hypothesis, on the other hand the p-value confirmed this result it was less than (0.05). That means:

Privacy has a positive direct effect on e-payment usage in Jordanian shopping websites at the level ($\alpha \leq 0.05$).

H01$_2$: Confidentiality has a positive direct effect on e- payment usage in Jordanian shopping websites at the level ($\alpha \leq 0.05$).

According to the result shown in table (4-11), the (t) calculated is greater than the (t) tabulated. The (t) calculated was equal (3.658) while the (t) tabulated is (1.96). In addition, the p-value was (0.028) it is less than significance, (0.05) or less, so we reject the null hypothesis and accept alternative hypothesis, that means:

Confidentiality has positive direct effect on e-payment usage Jordanian shopping websites at the level ($\alpha \leq 0.05$).

H01$_3$: Data Integrity has a positive direct effect on e- payment usage in Jordanian shopping websites at the level ($\alpha \leq 0.05$).

According to the result shown in table (4-11), the (t) calculated is greater than the (t) tabulated. The (t) calculated was equal (6.354) while the (t) tabulated is (1.96). In addition, the p-value was (0.016) it is less than significance, (0.05) or less, so we reject the null hypothesis and accept alternative hypothesis, that means:

Data Integrity has positive direct effect on e-payment usage in Jordanian shopping websites at the level ($\alpha \leq 0.05$).

H01$_4$: Authentication has a positive direct effect on e- payment usage in Jordanian shopping websites at the level ($\alpha \leq 0.05$).

According to the result shown in table (4-11), the (t) calculated is greater than the (t) tabulated. The (t) calculated was equal (8.365) while the (t) tabulated is (1.96). In addition, the p-value was (0.000) it is less than significance, (0.05) or less, so we reject the null hypothesis and accept alternative hypothesis, that means:

Authentication has positive direct effect on e-payment usage in Jordanian shopping websites at the level ($\alpha \leq 0.05$).

CHAPTER FIVE

5.1 The Main Result of Study

5.2 Study Conclusion

5.3 Study Recommendations

(5-1) The main results of the study

The study explored a number of important and significant results that the researcher hopes that they would lead to novel contributions to theory and relevant literature. The researcher also hopes that such results would trigger a number of critical decisions by website shopping organizations. Also hope that such decisions would be reflected positively on their business' benefits. Based on the data analysis and hypotheses testing in chapter 4, the research results generated from this piece of work can be summarizing as follows:

1. This study obtained the evaluation of website security of the Jordanian shopping websites through four main dimensions (Privacy, Confidentiality, Date Integrity and Authentication). The study showed high level of importance of website security in Jordan with all dimensions discussed earlier in this study. That agrees long with the study of (Sen, et al, 2015) and (Jing, 2009)
2. The importance level of Privacy in Jordanian shopping websites was high (3.982), which corresponds with (Alqatan et, al., 2016) finding the influence of privacy in Small and Medium-sized Tourism enterprises in Jordan.
3. The importance level of Data integrity in the Jordanian shopping websites was high (4.145), with standard deviation equal to (0.748) and the highest statement got approved from the viewpoint of sample study was " Having personal profile is guaranty of Data Integrity.
4. The importance level of Confidentiality in the Jordanian shopping websites was high (3.750). Which indicate that Jordanian shopping websites support (Hartono, et al., 2014), that indicate Jordanian shopping websites owners should develop a Confidentiality policy.

5. The importance level of Authentication in Jordanian shopping websites was high (3.852). Where the arithmetic means range for this independent variable was between (3.598 – 4.158) compared with General Arithmetic mean amount of (3.852). We observe that the highest mean for the item, " I trust the website owner and employee with my information.
6. The importance level of e payment usage in the Jordanian shopping websites was high support (Khalili, et al., 2012), study entitled "Evaluation of e-payment systems in Iran using analytic hierarchy process".
7. Website security has a positive direct effect on E-payment usage in Jordanian shopping websites industries at the level ($\alpha \leq 0.05$). The (R) was (0.489) at level ($\alpha \leq 0.05$), whereas the (R^2) was (0.239). This means the (0.239) of E-payment usage among Jordanian website shopping industries changeability's results from the changeability in Website security. As (Beta) was (0.489) this means the increase of one unit in website security will increase E-payment usage of website shopping value (0.489).
8. Privacy has a positive direct effect on e payment usage in Jordanian shopping websites at the level ($\alpha \leq 0.05$), the researcher observes that there is a positive direct effect of Privacy on e- payment usage Jordanian website shopping. As shown in the above table the (T) calculated is greater than the (T) tabulated where the calculated is (9.185), while the (t) tabulated is (1.96).
9. Confidentiality has positive direct effect on e- payment usage in Jordanian shopping websites at the level ($\alpha \leq 0.05$), the (t) calculated was equal (3.658) while the (t) tabulated is (1.96). In addition, the p-value was (0.028) it is less than significance, (0.05) or less.

10. Data Integrity has positive direct effect on e- payment usage in Jordanian shopping websites at the level ($\alpha \leq 0.05$), the (t) calculated is greater than the (t) tabulated. The (t) calculated was equal (6.354) while the (t) tabulated is (1.96). In addition, the p-value was (0.016) it is less than significance
11. Authentication has positive direct effect on e- payment usage in Jordanian shopping websites at the level ($\alpha \leq 0.05$), the (t) calculated is greater than the (t) tabulated. The (t) calculated was equal (8.365) while the (t) tabulated is (1.96). In addition, the p-value was (0.000) it is less than significance.

That means that there is positive direct effect of the independent variables on dependent variable.

(5.2) Conclusions

This research aimed to study the effect of website security on e- payment usage. The research tried to determine the key of website security that affects e-payment such as: (privacy, Confidentiality, Data Integrity, and Authentication). This study classified privacy, Confidentiality, Data Integrity, and Authentication. Certainly, in this new digital world of business, the website security seems to be the right solution to get e payment usage. This is because in the current e-commerce environment and e-payment can provide shopping websites with various benefits such as optimizing and integrating business processes, maximizing operational and managerial profits, and improving strategic and organizational benefits.

To achieve the objectives of this study, the researcher developed a novel model to measure the effect of website security on e-payment usage. An extensive literature review has been prepared and considered as essential element for developing research model. The model has two main variables: website security and e-payment usage. The construct of website security includes the following sub-dimensions: privacy, Confidentiality, Data Integrity, and Authentication.

The developed model applied and tested in the context of Jordanian shopping websites, the sample was determined to include the usage e- payment of Jordanian website. For hypotheses testing, a questionnaire instrument was designed on the basis of the constructed model. Prior to data collection, the questionnaire instrument was validated by a number of professors and experts in the domain of this study and working at Middle East University and other universities in Jordan. Moreover, questionnaire instrument was validated in terms of clearance, meaning, format, and its ability to measure the constructs included within the research model. Questionnaire instrument revised to reflect the comments and suggestions of those received by the referees. Thereafter, (620) questionnaire distributed to the sample of this study and (469) responses considered valid for data analysis. The analysis conducted using Statistical Package for Social Sciences (SPSS) Version (20). Following data analysis, results were obtained and reported in chapter four.

(5-3): Recommendations

Based on study results and conclusions, the following recommendations are suggested:

1. Jordanian shopping websites recommended translating vision into policies and procedures in order to enhance the effect on operation, competitive capabilities.
2. Jordanian shopping websites should be a clear about website security policy.
3. Jordanian shopping websites recommended building a relationship with their customers.
4. Jordanian shopping websites must train employee how to encourage customers to relief information.
5. Jordanian shopping websites must facilitate E-payment process and methods.

References

1. Adilet.K &Ertem. E. (2013) Flex DPDP: FlexList-based Optimized Dynamic Provable Data Possession",In proceedings of International journal of Engineering Research and technology .
2. Al-ma'aitah Mohammad Atwah (2013) Security Concerns in E-payment and the Law in Jordan: (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.7, 2013
3. Alqatan, S, maizura, n ,noor, n, man, m ,mohemad ,r (2016). An empirical study on success factors to enhance customer trust for mobile commerce in small and medium-sized tourism enterprises (smtes) in Jordan Journal of Theoretical and Applied Information Technology31st January 2016. Vol.83. No.3
4. Carmona ,C. Ramírez ,S. Torres, F. Bernal ,E. del Jesus, J & García,S. (2012).Web usage mining to improve the design of an e-commerce website, Elsevier journal .
5. Chen, D. Zhao. H(2012).Data Security and Privacy Protection Issues in Cloud Computing, International Conference on Computer Science and Electronics Engineering.
6. Chen, Y.H., Hsu, I.C., & Lin, C.C. (2010). Website attributes that increase consumer purchase intention: A conjoint analysis, Journal of Business Research, 63, 1007-1014.
7. Chouksey,S. Agrawal, R. Verma, D & Metta, T .(2013). Data Authentication Using Cryptography, Inernational Journal of Advanced Computer Research.(Volume-3 Number-2 Issue-10), June-2013.
8. Daştan,I ,Gürler, C (2016).Factors Affecting the Adoption of Mobile Payment Systems: An Empirical Analysis .Volume 6 No 1 (2016) | ISSN 2158-8708 (online) | DOI 10.5195/emaj.2016.95
9. DZEMYDIENĖ, D. NAUJIKIENĖ, R. KALINAUSKAS, M. & JASIŪNAS, E. (2010). Evaluation of Security Disturbance Risks in Electronic Financial Payment Systems

ISSN 1822-8038 (online) INTELLECTUAL ECONOMICS, No. 2(8), p. 21–29

10. Guo, J & Wong,C .(2012).A Dynamic Account Payment Method for Integrating Heterogeneous B2C Electronic Payment Systems,: Infrastructures and Tools for Multiagent Systems
11. Hartono,H .Clyde ,W. Holsapple ,b. Kimc, K. Sik Na,K& Simpson ,T. (2014). Measuring perceived security in B2C electronic commerce website usage: A respecification and validation, Elsevier journal, Decision Support Systems.
12. Havighurst ,Robert (2007) by Taylor & Francis Group, LLC User Identification and Authentication Concepts.
13. http://www.ffiec.gov: Federal Financial Institutions Examination Council Authentication in an Internet Banking Environment
14. Jaques,E. (2007). Measurement of responsibility; a study of work, payment and Individual capacity.
15. Jiang,W.Fan ,X. Duanmu, D&Deng, Y.(2013).A New Security Risk Assessment Method of Website Based on Generalized Fuzzy Numbers, Journal of computers, VOL. 8, NO. 1, JANUARY 2013.
16. Jing, Y. (2009). On-line Payment and Security of E-commerce, ,Proceedings of the International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, May 22-24, 2009.
17. Khalil,H , Ebrahimi,S & Nalchigar, S.(2012). Evaluation of e-payment systems in Iran using analytic hierarchy process. African Journal of Business Management Vol. 6(19), pp. 5950-5956, 16 May, 2012.
18. Kim,C, Tao ,W ,Shin,N , Kim ,K (2009). An empirical study of customers' perceptions of security and trust in e-payment systems
19. Ling, K.C., Chai, L.T., & Piew, T.H. (2010). The effects of shopping orientations, online trust and prior online purchase experience toward customers' online purchase intention. International Business Research, 3(3), 63-76,

20. Liu ,D.(2011)/E-commerce System Security Assessment Based on Grey Relational Analysis Comprehensive Evaluation, , school of Economics and Management, Shenyang Ligong University, Shenyang.
21. Majava, J.Nuottila,J & Haapasalo,H.(2013). Exploring Customer Definition and Representation in Market-Driven NPD in ICT Industry. International Journal of Business Development and Research, ISSN: 2286-6213, Volume 1, Number 2.
22. Mandić, M. (2009). "Privacy and security in E-commerce", M. A. Art Design and Internet technologies.(Vol. XXI)
23. Mark ,S. Ackerman , Donald T. Davis**,** Jr,(2003).Privacy and Security Issues in E-Commerce Review chapter for the New Economy Handbook (Jones, ed.).
24. Ming, W. Teoh, Y.Chong, S. Lin,B&Chua ,J(2013).Factors affecting consumers' perception of electronic payment: an empirical analysis, Internet Research , Emerald Group Publishing Limited .(Vol. 23) No. 4, pp. 465-485
25. OECD (2000), OECD Information Technology Outlook 2000, Chapter 4, ìOverview of issues in electronic settlement of paymentsî, Paris.
26. OECD (2006), "Online Payment Systems for E-commerce", OECD Digital Economy Papers, No. 117, OECDPublishing. http://dx.doi.org/10.1787/231454241135
27. Priya.G.A &E. Daniel. (2015). A Literature Survey on Integrity Verification Techniques,International Journal of Engineering Research & Technology , Vol. 4 Issue 05, May-2015
28. Punyani,G, Sharma,S, Dash, G (2015) . EXAMINING FACTORS AFFECTING FEMALES' PERCEPTION TOWARDS THE USAGE OF ELECTRONIC PAYMENT SYSTEM: AN EXCLUSIVE STUDY ON E-SHOPPING: J of Advances in Business Management /eISSN-2395-7441/pISSN-2395-7328/ Vol. 1/ Issue 3/ July-Sept. 2015 Page 27
29. Raghallaigh, E. (2011). Major Security Issues in E-Commerce BSc(Hons), DipHPsych .

30. Salem,A &Walsh,W.(2011) .Making security information usable Guidelines for creating an effective Air Domain website.
31. Sen,P . Islam,R&Ahmed,R. (2015). A Study on E-Commerce Security Issues and Solution. International Journal of Computer and Communication System Engineering .Vol. 2 (3).
32. Siddiqui,H.(July,2008). Investigation of Intention to use e-commerce in arab countries :A comparison of Self-Efficiency ,Usefulness ,Culture ,Gander and Socioeconomic statue in Saudi Arabia and UAE.
33. Szydlowski,M . Kruegel,C&Kirda ,E. (2012). Secure Input for Web Applications**,,**Systems Lab ,Technical University Vienna , Austria.
34. Tsiakis, T., and Sthephanides, G. "The concept of security and trust in electronic payments", Computers & Security, Vol.24, pp: 10-15.
35. Yasin,S. Haseeb, K & Qureshi,R .(2012) .Cryptography Based E-Commerce Security: IJCSI International Journal of Computer Science Issues, (Vol. 9, Issue 2, No 1). March 2012
36. Yazdanifard ,R .Al-Huda Edres ,N& Seyedi ,A .(2011).Security and Privacy Issues as a Potential Risk for Further Ecommerce Development, International Conference on Information Communication and (vol.16) Management IPCSIT , IACSIT Press, Singapore.
37. Yee,C & Yazdanifard,R.(2014). How Customer Perception Shape buying Online Decision,. Global Journal of Management and Business Research: E Marketing Volume 14 Issue 2 Versions 1.0.
38. Zhang ,Y& Wang ,R. (2014).Comparison of E-payment of the B2C E-commerce in China from the Security and Trust Perspective , International Journal of Security and Its Applications ,Vol.8, No.3
39. Zhang, D. (2002). Biometric Solution for authentication in an E-world

40. Zimmerman,J. (2012).Using the S-O-R MODEL to understand the impact of website attributes on the online shopping experience, university of north Texas.

Appendixes

1. Appendix 1: Questioner

Middle East University

Business faculty

E-Business department

Dear Responder,

The researcher is in the process of conducting a field study regarding the Effect of Website Security on E-Payment Usage: from Jordanian Customer Perspective, which will be applied on the Jordanian website shopping.

Being a part of the requirement to acquire a master's degree in e Business.

This questionnaire is intended only for the purposes of scientific research.

Please note that basis of the questionnaire measurement would be a five point Lekart scale, employed accordingly:

Strongly disagree	Disagree	Natural	Agree	Strongly agree
1	2	3	4	5

Researcher: Manar Khamis Alfarsi

Supervisor: Dr. Sameer Aljabaly

Part1: Demographics:

Gender: ☐ Male ☐ Female

Age: ☐ Less than 25 ☐ 25-34 ☐ 35-44 ☐ 45-54 ☐ more than 55

Marital status: ☐ Single ☐ Married ☐ Divorced

Academic degree: ☐ Diploma ☐ Bachelor degree ☐ Masters ☐ Philosophy ☐ Doctorate

#	Item	Strongly agree (5)	Agree (4)	Natural (3)	Disagree (2)	Strongly disagree (1)
Privacy defined here as "The ability of an individual to control the terms under which their personal information is acquired and used.						
1	**If I do not know how a websites handles my privacy, I do not continue shopping on that website.**					
2	**If I am buying from a website for the first time, I look at their privacy policy.**					
3	**The web site is not allowed to share information about what you purchased with other companies.**					
4	**The web site can change their privacy policy without telling me.**					
5	**A web site must get their privacy policy reviewed by the government on an annual basis.**					
6	**Internet privacy policies are required by law.**					
Data integrity assurance and protection from unauthorized modification In the process of their preservation or transfer						
7	**A website must ensure that my data are not subjected to modification.**					
8	**Having personal profile is guaranty Integrity.**					
9	**I think that website providing all the necessary information to customer.**					
10	**I feel comfortable surfing this website.**					
11	**This website makes it easy for me to build a relationship with this**					

	company					
Confidentiality "data protection from unauthorized damage"						
12	**I think that launching a new product from my favorite brand should be relevant to the product that I know.**					
13	**I don't like to see my favorite brand supporting other political parties.**					
14	**I think that advertising campaigns guides me to the right product.**					
15	**In my opinion choosing brand location is a key of success.**					
16	**I think that product pricing for a brand is important.**					
Authentication "Refers to automatic identification of an Individual based on his distinguishing physiological and behavioral characteristics"						
17	**It's acceptable if unauthorized employee can access to my personal and financial data.**					
18	**I believe knowing employee information encourage me to relief my information.**					
19	**I trust the website owner and employee with my information.**					
20	**I think that website Authentication affects my e-payment decision.**					
21	**In my opinion choosing website Authentication is a key of success.**					

Electronic payment (e-payment) has become a popular means today for paying for online purchases made						
22	**I prefer website that offers offline payment option (cash).**					
23	**E- Payment option facilitates buying process.**					
24	**It is matter if website offer several E-payment options(like visa-PayPal – credit card-diept card…etc).**					
25	**I think that paying in E-payment is much safer than cash.**					
26	**I think that paying in E-payment is much easy than cash.**					

2. Appendix 2: Names of arbitrators.

No.	Name	Specialization	Work Place
1	Prof. Laith Al-Robaei	Marketing	MEU
2	Prof. Abdelhafez Salameh	اساليب تدريس	MEU
2	Dr. Morad Al-Atiani	Business Administration	Al- IsraaUni
3	Dr. Ahamed Ali Saleh	Business Administration	MEU
4	Dr. HanadiSalameh	E-Business	MEU
5	Dr. Abdaziz Sharabati	Business Administration	MEU