T.C.
ISTANBUL GEDİK UNIVERSITY
INSTITUTE OF GRADUATE STUDIES

DATA SECURITY AND PROTECTION IN ELECTRONIC COMMERCE MANAGEMENT

MASTER'S THESIS

Abdul Munam ALHAMEED

Engineering Management Master in English Program

JULY 2021

T.C.
ISTANBUL GEDİK UNIVERSITY
INSTITUTE OF GRADUATE STUDIES

DATA SECURITY AND PROTECTION IN ELECTRONIC COMMERCE MANAGEMENT

MASTER'S THESIS

Abdul Munam ALHAMEED
(191281026)

Engineering Management Master in English Program

Thesis Advisor: Prof. Dr. GÖZDE ULUTAGAY

JULY 2021

T.C.
İSTANBUL GEDİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜ

Yüksek Lisans Tez Onay Belgesi

Enstitümüz, Engineering Management Department İngilizce Tezli Yüksek Lisans Programı (191281026) numaralı öğrencisi Abdul Munam ALHAMEED'in "Data Security and Protection In Electronic Commerce Management" adlı tez çalışması Enstitümüz Yönetim Kurulunun 07.07.2021 tarihinde oluşturulan jüri tarafından *Oy Birliği* ile Yüksek Lisans tezi olarak *Kabul* edilmiştir.

Öğretim Üyesi Adı Soyadı

Tez Savunma Tarihi: 07/07/2021

1) Tez Danışmanı: Prof. Dr. Gözde ULUTUGAY

2) Jüri Üyesi:. Dr. Öğr. Üyesi Redvan GHASEMLOUNIA

3) Jüri Üyesi: Doç. Dr. Sevcan DEMİR ATALAY

DECLARATION

I, Abdul Munam ALHAMEED, do hereby declare that this thesis titled as “Artificial Intelligence Utilization in Production Quality Management: Piping Fabrication” is original work done by me for the award of the masters degree in the faculty of Engineering Management. I also declare that this thesis or any part of it has not been submitted and presented for any other degree or research paper in any other university or institution. (07/07/2021)

Abdul Munam ALHAMEED

DEDICATION

It is my pleasure to dedicate my thesis work to the soul of my beloved parents (Father and Mother). They taught me many lessons that become the guide of my life. I also dedicate my thesis work to my dear and lovely wife and kids. They always stand for me and gives support. I dedicate my thesis work to my amazing brothers and sisters. I feel so greatly privileged to have them in my life.

PREFACE

First, I would thank my supervisor Prof. Dr. Gözde Ulutagay for all support and guidance throughout my research work.

It was all fruitful advice during my academic career.

It is my pleasure to thank my family and friends for their help and support. It is my pleasure to thank my father, mother, brothers, and sisters who stood by me during my study and always offered their love, care, and support.

Finally, I would like to thank all participants who took part in the study and enabled this research to be possible.

July 2021 Abdul Munam ALHAMEED

TABLE OF CONTENT

Page

ABBREVIATIONS

ACH : Automated Clearing House
AOL : American Online
APP : Appendix
B2B : Business To Business
B2B2C : Business To Business To Customer
B2C : Business To Customer
B2E : Business To Employee
C2B : Customer To Business
C2C : Customer To Customer
CORBA : Common Object Request Broker Architecture
DES : Data Encryption Standard
DSA : Digital Signature Algorithm
EDI : Electronic Data Interchange System
EFT : Electronic Fund Transaction System
FTP : File Transfer Protocol
HTML : Hypertext Markup Language
HTTP : Hypertext Transfer Protocol
ICMP : Internet Control Message Protocol
ID : International Data
IIS : Internet Information Server
IMAP : Interactive Mail Access Protocol
IP : Internet Protocol
ITEF : Internet Task Engineering Force
KEA : Key Exchange Algorithm
MAC : Message Authentication Code
MD5 : Message Digest Algorithm
NSF : Non-Sufficient Fund
PI : payment information
POP3 : Post Office Protocol
RAS : Remote Access Server
RC2 & RC4 : Symmetric encryption algorithm used by the US government
RSA : Rivest & Shamir & Adleman
SET : The Secure Electronic Transactions Protocol
SH-1 : Secure Hash Algorithm
SKIPJACK : Conventional Symmetric Key algorithm used by the US government
SMTP : Simple Mail Transfer Protocol
SNMP : Simple Network Management Protocol
SSL : The Secure Sockets Layer Protocol
TCP : Transmission Control Protocol
TCP/IP : Transmission Control Protocol/ Internet Protocol
TELNE : Teletype Network
TLS : Transport Layer Security

UDP **:** User Datagram Protocol
URL **:** Universal Resource Locator
VAN **:** Value Added Network
X.509 **:** Standard certificates used by the SSL and SET ordinances

LIST OF TABLES

Page

LIST OF FIGURES

Page

DATA SECURITY AND PROTECTION IN ELECTRONIC COMMERCE MANAGEMENT

ABSTRACT

The rapid growth in e-commerce has put more pressure on website programmers. That is because internet security issues need to be further studied and seriously discussed. This study has discussed and analyzed the issues of information security. This study was applied to one of the Iraqi E-commerce websites. The website is (The Elryan online shopping market) https://www.elryan.com/ar/. The goal of the study is to prepare the site to be ready and secure for online financial transactions. Four steps were done to check the site for any possible security problems and to fix these problems if found. The first step was reviewing the site operation system and components. The second step was the security check to identify any possible security weakness. The third step was applying security tools to fix the security problems. The final step was testing the system to ensure that the security tools are working and the website security weaknesses are removed. Three security problems were found on the site. The first problem was the confidentiality problem. The second problem was the authentication problem. The third problem was the encryption algorithms agreement problem. The first two security problems were fixed, and the site was tested. The results showed that the security weaknesses were removed and the site is secure for online transactions. The encryption algorithms agreement problem was not solved directly, but there were two suggested solutions. The first solution is to update the site so it can accept most of the encryption algorithms. The second solution is to deal only with the parties that use encryption algorithms supported by SSL.

Keywords: *E-commerce, Security, Protection, financial transactions, Secure Sockets Layer(SSL).*

ELEKTRONİK TİCARET YÖNETİMİNDE VERİ GÜVENLİĞİ VE KORUNMA

ÖZET

E-ticaretteki hızlı büyüme, web sitesi programcıları üzerinde daha fazla baskı oluşturdu. Bunun nedeni, internet güvenliği sorunlarının daha fazla incelemesi ve ciddi şekilde tartışılması gerektiğidir. Bu çalışma, bilgi güvenliği konularını tartışmış ve analiz etmiştir. Bu çalışma Irak E-ticaret sitelerinden birine uygulandı. Web sitesi (The Elryan çevrimiçi alışveriş pazarı) https://www.elryan.com/ar/. Çalışmanın amacı, siteyi çevrimiçi finansal işlemler için hazır ve güvenli olacak şekilde hazırlamaktır. Sitede güvenlik sorunları olup olmadığını kontrol etmek ve bulunursa bu sorunları düzeltmek için dört adım gerçekleştirildi. İlk adım, site işletim sistemini ve bileşenlerini incelemek. İkinci adım, olası herhangi bir güvenlik zayıflığını tespit etmek için güvenlik kontrolü. Üçüncü adım, güvenlik sorunlarını çözmek için güvenlik araçları uygulamak. Son adım, güvenlik araçlarının çalıştığından ve web sitesi güvenlik zayıflıklarının giderildiğinden emin olmak için sistemi test etmekti. Sitede üç güvenlik sorunu bulundu. İlk sorun gizlilik sorunuydu. İkinci sorun, kimlik doğrulama sorunuydu. Üçüncü sorun, şifreleme algoritmaları anlaşması sorunuydu. İlk iki güvenlik sorunu giderildi ve site test edildi. Sonuçlar, güvenlik zayıflıklarının kaldırıldığını ve sitenin çevrimiçi işlemler için güvenli olduğunu gösterdi. Şifreleme algoritmaları anlaşması sorunu doğrudan çözülmedi, ancak önerilen iki çözüm vardı. İlk çözüm, siteyi şifreleme algoritmalarının çoğunu kabul edebilecek şekilde güncellemektir. İkinci çözüm, yalnızca SSL tarafından desteklenen şifreleme algoritmalarını kullanan taraflarla ilgilenmektir.

Anahtar Kelimeler: *E-ticaret, Güvenlik, Koruma, finansal işlemler, secure sockets layer (SSL).*

1. INTRODUCTION

1.1 Overview

The term electronic commerce (e-commerce) is used for any type of commercial transaction, and it is the transfer of information over the Internet as it covers a different set of commercial activities that are used on the Internet as a platform through which information can be transferred as well as the exchange of monetary currencies or both, so dependence on commerce has become Online buying, selling and getting cash has been one of the most popular things recently, (Bajaj,2005)

E-commerce means that the Internet is used in commercial transactions, which depend on the exchange of value, whether through organizational or individual borders, in exchange for the products and services that are provided, and in general, e-business that takes place over the Internet and an exchange of value in it is called e-commerce.

The history of e-commerce has started since the invention of the phone in the last century when data is exchanged on a large scale, and large institutions have been keen to develop electronic data exchange beginning in the sixties and although at the beginning it did not gain acceptance from everyone, it continued and developed And the lack of acceptance of it continued until the eighties, and during the past thirty years, a lot of development in e-commerce has occurred clearly and significantly.

In the beginning, it was known that electronic commercial transactions would be facilitated through the electronic exchange of data as well as the electronic transfer of funds, and this was a motivation for many companies to send commercial documents to them electronically and this facilitated the matter, and among the forms of e-commerce in the eighties are purchase orders or Invoices, as well as the growth or acceptance of credit cards and automated teller machines, and other telephone banking services, and among the forms of electronic commerce are reservations for airlines and railways via the Internet, and this system has been relied upon in the

United States of America in the auto trade and other developments It updated it to become one of the most important fundamentals of commerce today.

Beginning in the nineties, other developments in e-commerce took place, which is that data and consultations are stored through the Internet, and it became more widespread in 1994 and at that time the beginning of marketing through the Internet, and it took many developments to be a means through which this is developed, (Wigand,1997).

At the end of the year 2000, many American and European companies offered a lot of services through the World Wide Web, and this was the beginning of the word e-commerce being linked with the ability to purchase various goods via the Internet, relying on secure protocols as well as electronic payment services.

The Internet has been designed beginning in 1969, and the matter has developed gradually and rapidly, and always increases the number of users to the web, and among the services that spread besides buying and selling are the services that take place between two or more companies, and these factors were the reason for the use of the Internet It has a purpose that is more than just browsing or entertainment, obtaining information and socializing, but at the same time, it is considered a good and modern way of doing business.

Many websites are used to promote products, in addition to the applications that have spread widely, including phone or computer applications, which are clear evidence of the prosperity of e-commerce on a large scale.

The advent of a new economic system is one of the characteristics of informatics since it can be seen that the global economy has largely transformed into a new system that relies mainly on human knowledge, so the information society increases the value of a thing with knowledge rather than effort and if the theory in the past was that work is the basis of value, then we are now facing the need to formulate a theory in knowledge as a basis for value. An American economist named Edward Dennison concluded that two-thirds of the American economic growth resulted from the progress of the knowledge of the workforce and the upgrading of its capabilities from manufacturing to the thinking industry. The information society is an economic fact and not an intellectual abstraction, not only is it self-renewable, Knowledge has become an economic weapon in the battles of profit and production, so the old

elements have disappeared to replace new elements that depend on intelligence, and the amount of their production and profit depends on the qualitative and quantitative level of their information i.e. specialized workers and smart machine.

The Internet in our present age and e-commerce with its current technologies do not pose a danger except to distributors and workers in intermediate channels between the consumer and the producer due to the so-called phenomenon of killing middlemen (Disinter-Mediation), but who knows what the future holds and which (progressive and revolutionary technical push) will come Then turn the entire business administration thought and practice upside down. In the technical fray, there may be other victims, (Choi,Stahl & Whinston,1997).

E-commerce applications started in the early 1970s and the most popular one is Electronic Funds Transfer (EFT), but the extent of this application did not exceed the giant commercial establishments and some small companies. Then came the electronic data exchange (EDI), which expanded the application of electronic commerce from just financial transactions to other transactions and caused an increase in companies contributing to this technology from financial institutions to factories, retailers, service institutions, and others, (Barr,1991).

Other applications have also appeared, such as buying and selling stocks, tickets, on the Internet, and on private networks. Such systems were called telecommunications applications and their strategic values were well known and apparent. With making the Internet a financial and profitable material in the nineties of the last century and its spread and growth to millions of people, the term "e-commerce" came to light, and then e-commerce applications were developed greatly. One of the reasons that led to the huge growth in the number of e-commerce applications is the development of networks, ordinances, and software. Another reason for this increase is the result of increased competition between companies.

1.2 Research Problem

The security threats to networks in all their divisions have become a permanent problem that worries producers, managers, and users alike, despite the research and studies on this topic, and the rapid progress in security equipment and applications, but all of this has been accompanied by progress in the methods of illegal attacks. The knowledge of these methods and exposure to them through theoretical, practical,

and analytical research and knowledge of developments in the solutions presented, all of these problems that this research may contribute to addressing, (McCrohan,2003).

E-commerce is not without problems that threaten it, whether practical, technical, or even legal, and we will present in this requirement a brief presentation of the most important problems of e-commerce:

1. The problem of the volume of e-commerce and its exorbitant expenses.

By looking at a study in this regard, we found that the problem of the volume of e-commerce and its high expenditures is enormous. If the amount of electronic shopping in Arab countries, for example, is compared with what is spent on advertisements on international sites, we find a very meager number, and this is due to the inaction of many banks and commercial institutions. The big Arab business, businessmen and those interested in trade should not enter strongly to trade remotely or e-commerce, and this does not serve it, so it must keep pace with the development in commercial dealings and make e-commerce a basic base in its local, global and future commercial strategy as well. Because although the Arab countries stand suspicious, hesitant, and cautious about e-commerce, other countries such as China are advancing strongly towards it to achieve giant steps towards economic growth. Besides the size of e-commerce is affected by the size of the number of exchanges that take place in it, it is also affected by fees or the taxes it imposes on companies operating in the e-commerce sector, for fear of the negative impact of e-commerce activities. Some governments are calling for the imposition of these taxes to achieve equality between companies that do not operate in the field of e-commerce.

2. Technology and its transfer between countries of the world.

One of the most important features of the end of the twentieth century is the occurrence of tremendous progress in technology, especially the computer and the sciences associated with it, which resulted in a change in the administrative and production systems, and all this was reflected in e-marketing or e-commerce. But now it involves vending machines in many activities. It has also become possible for the buyer to browse the catalog and choose what suits him from the commodities without the hassle of moving from one seller to another to inquire about his commodity.

According to the rapid technological advancement, traditional commerce will disappear, and electronic shopping will replace the stores, which reduces the need and costs for stores and salesmen.

In addition to all of the above, technological progress and its disparity from one country to another will divide the countries of the world into a group of technology exporters and importers, and this will be reflected in e-commerce, as developed countries market their advanced production of industry, consumer goods, services, and information systems. Another hand the role of the third world countries is the consumer in this trade, as he receives technology, goods, and services from the developed world, and this makes us conclude that the general concept of the economy is one, where there are supply and demand, whether in an economy based on traditional trade or e-commerce where the dispute is the essential between the two systems is only the quality of the commodity and the mechanisms for handling the transaction,(Gunasekaran,Marri,

McGaughey & Nebhwani,2002).

3. The problems of the fulfillment instrument - credit cards (electronic money).

The emergence of the idea of electronic money and its use ensures the speed and ease of settling payments and reducing the need to keep cash, which expands the process of trade exchange, and therefore invoices are paid and funds transferred to other accounts outside the bank through electronic money exchange, (Vlasov,2017).

As it has the facilities it provides, it also has problems that arise from it, briefly, as follows:

- Misuse of electronic payment cards by the cardholder, such as using the card after the end of its validity period or using it despite the bank canceling it.
- Misuse of the card by third parties such as stealing the card and using it or stealing the password of the cardholder and using it.
- Manipulation by the employees of the card-issuing bank in agreement with the cardholder or the merchant or with others, such as allowing the card limit to be exceeded in the drawing or the validity period.
- Manipulating credit cards via the Internet by hacking international communication lines or creating fake sites as original sites

4. Consumer and his protection in e-commerce.

In a free economy and the control of the market mechanisms in it, the consumer has become vulnerable to manipulating his interests and trying to deceive him. The risk to which the consumer is exposed in the context of e-commerce is greater than the risk in traditional commerce because the scope of e-commerce is wider and more comprehensive. That is why the media must be taken into consideration, to enable the consumer to know the quality of the product, its true advantages, and even its disadvantages or some of its defects.

It is also important to present sites that can be marketed through and to provide advice and insight to the consumer in order not to be bothered by his dealings on the net and to feel difficult and unimportant to him, (Kim,Ferrin & Rao,2008).

5. Piracy and destruction of e-commerce sites.

One of the most important features that should be characterized by e-commerce is to protect trade through the confidentiality of information, and this is because most of the information dealt with daily can be protected by many protection systems. But the real danger is that any business, if its information is stolen or disclosed, will pose a risk that may affect negatively, and this is why one of the biggest threats surrounding e-commerce is the disclosure or confidentiality of information.

1.3 Research Assumptions

Since the threats cannot be terminated, but rather to reduce them, or in other words, to make them as difficult as possible, so I put for this research two hypotheses.

- Knowledge of the security protocol architecture, including the Secure Sockets Layer (SSL) ordinance, helps you to understand building hard to penetrate systems.
- To strengthen the confidentiality of the content of messages sent over the network, we use Arabic letters instead of English because the Arabic language has good informational and encoding properties.

1.4 Research Aims

The research aims to provide an integrated package of security services that an e-commerce user can use to secure his resources and wealth on the internet, and the

research aims, in general, to enrich simple libraries in the field of confidentiality of information, especially concerning financial transactions and is particularly exposed to a detailed study of the Secure Sockets Layer (SSL), and the Secure Electronic Transactions (SET) ordinance. There are many goals for electronic commerce, which have increased with the technological development, and among these goals are the following:

- To have benefits for companies as well as for the consumer and work to increase commercial relations and increase market space.
- That the customer gets good help, as all alternatives can be seen and choose the best, and since every company seeks to be the best, this will increase the efficiency of products, prices, and the consumer is the beneficiary.
- All companies seek to multiply customers, and this is what drives them to develop high-quality services and services provided by the companies to grow in the market in a good and profitable way.
- It is an upgrade to traditional commerce, which creates a lot of profit and multiplier results.
- It is a way for both buyers and sellers to come together in cyberspace from a physical location, expanding the scope.
- You can reach anywhere in the world and get the products you want at any time, which is one of the most important advantages.
- Information is delivered very quickly and at the same time, the cost is lower than anywhere else.
- It is a way for people of equal interest to share the same things.
- They cause the world to move from mass production to mass customization, that is, the customization of the quality of goods, products, and designs.

1.5 Research Importance

The risks that threaten commercial information systems over the past few years have expanded and developed rapidly beyond all expectations. A company MI2G indicated It is one of the market companies specializing in security and network solutions in the United Kingdom. Indicated that the (Klees) virus has inflicted losses

on the global economy that exceeds 9.9 billion US dollars, as for the (Love Bug) virus, its losses reached 9.6 billion dollars according to consultants working with a research house. and the total pirate attacks inflicted losses on the global economy in the year 2000 of about 1.6 trillion US dollars.

All this makes security studies a priority in universities and scientific research institutions, and international conferences are held for them. This research derives its importance from the importance of the topic it researches.

The importance of electronic commerce varied, which increased with the development of this field, which is represented as follows:

- Seeking to obtain a lower cost than anywhere else, and because of competition, discounts and offers are made between companies.
- Eliminate travel, which costs a lot of effort and time until you buy anything, but it can be simply requested.
- It is considered the best way to shop which saves a lot of time and money.
- You are provided with all the information on anything before you buy it, as most websites make additional information available.
- They are available throughout the day, making it easy for you to get what you want at any time, (Kim& Solomon,2013).
- It depends on many websites and applications, which guarantee the diversity of the offers that are presented.

1.6 Research Methodology

To surround the research topic from many angles, the following methods were used:

1. The theoretical aspect: The theoretical backgrounds of the topic, previous studies, and research were presented by reference to scientific references, periodicals, Internet libraries, and related sites.
2. The practical aspect: The practical aspects of the security decrees were studied after designing a commercial website, performing some tests on it, and recording the results.

3. Analytical aspect: The results obtained were analyzed and compared with the results of previous studies and research, and new findings and recommendations that enrich this topic were produced.

2. INTERNET SECURITY

2.1 Overview

In early 1996, about 13 million computers from 195 countries including Antarctica were connected to the Internet. The Internet is not a single network, but it can be presented as global groups of networks. These groups are connected in a free and easily accessible way by computers (clients) to host computers, (Leiner, Cerf, Clark, Kahn, Kleinrock,

Lynch, Postel, Roberts,Wolff, 2009).

The connection can be through multiple methods including gateways, routers, phone calls, and Internet service providers. The internet is easily accessible to anyone with a computer and a network. Individuals and organizations can reach any point on the network without taking into account national or geographic borders between countries.

With this state of comfort and easy access to information, new risks emerge. The risks could be losing this valuable information. The information can be stolen or misused, which would result in great harm. When the information became recorded electronically and available on the network computers, it became more risk of theft, and loss, (Hawkins,Yen and Chou,2000).

If the information can be printed on paper or saved on files, then thieves do not need to enter offices or homes or travel to another country. Because they can steal all the information they need using their personal computer.

Therefore, the security method called (blindness) was addressed as one of the best ways to ensure the security of information. The method was built with some basic concepts in the modern science of cryptography. In particular, more focus was placed on the informational and cryptographic properties of the Arabic language.

Some important criteria about the Arabic language were defined and calculated. For example, the information rate, frequency, roughness scale, and chance coefficient in clear and blind texts. In addition, calculating the limit for breaking blinding in some

traditional encryption methods. Tables for the actual distribution of single and double letters (duals) in the Arabic language were also presented. Based on statistics of letters occurring in the Holy Qur'an obtained using a computer, (Khan, Alghathbar, Khan, AlKelabi and AlAjaji, 2010).

Many studies in the literature have investigated the behavior of hackers and their motivations. In addition, these studies have tested the size of the damage that they may cause, and how they act illegally.

Most of the security weaknesses are in the internet gates such as (TCP / IP, ICMP, UDP, SMTP, HTTP, FTP) and others. The important illegal actions that can be done on the internet can be reading, copying, modifying, and deleting information. Most types of information that can be stolen are confidential information such as account numbers and credit card numbers, (Atkins, Buis, Hare, Kelly, Nachenberg, Nelson, Phillips, Ritchey and Stean,1997).

The security problem in the internet network needs multiple software solutions. For example, in the connection layer, attention has been paid to the wire and wireless connection. For the Internet protocols layer (IP), (IPsec), and (TCP / IP) the Secure Protocol Layer (SSL) is activated. For the application layer, the solution is by using the well-known Protocols of web services (HTTP- LDAP-IMAP).

The software solutions could not be enough, so engineering solutions can also be applied. The engineering solutions can be designing circuits, processors, and even all computer hardware. Some specialized companies have moved from standard design to custom design. They have designed flexible circuits that have some secure hardware, (Householder, Houle and Dougherty, 2002).

It is important to indicate that the design of any computer system must take into account some considerations. The most important consideration is that every part of the system should be saved from hackers. That is, the system should be efficient for use with a minimum probability of attack.

2.2 Basic Security Concepts

There are some basic security concepts that are important to understand when sharing information on websites. As internet users, individuals usually ask many questions before sending their data to any website. For example, who is the issuer of

the certificates? Do you trust them? Is the degree of encryption and privacy acceptable? Individuals ask these questions because many sites attract them using free or low prices strategy. However, the low prices usually have a high risk when using internet websites, (Grossman, 2012).

2.2.1 Basic security concepts that are related to the website's security

1. Confidentiality

The information is said to be confidential when no one can copy or use them without authorization. When the information is read or copied by someone who is not authorized, this is known as (loss of confidentiality), (Grossman, 2012).

Some types of information have very important and private confidentiality while others not. For example, the research information, medical information, insurance records, new product specifications, and investment company strategies. In some cases, there may be a legal obligation to protect the individual's personal information. These cases are in financial institutions, banks, and hospitals, doctors' offices, medical laboratories, tax offices, and others.

2. Integrity

The information is said to have Integrity when no one can modify them without authorization. If the information can be easily modified, this process is known as (loss of integrity). That includes both unauthorized modifications, human error, and deliberate tampering.

All of these cases make the information lose its integrity, especially when dealing with critical information such as financial data, electronic fund transactions, and military data.

3. Availability

The availability, in this case, refers to the ability to access editing the information.

If the Information can be edited and easy to access, that resulting in (loss of data availability). That means that authorized users cannot always do what they want.

Availability of information is often the most important characteristic of a business that relies on information. For example, airline schedules, online reservations, and

inventory systems. When the user tries to access or edit the information, the accessing request will be denied.

2.2.2 Basic security concepts of individuals who are using that information

1. Authentication

It is the process of identifying the individuals. This process can be done by using certain procedures such as names, addresses, mobile phones, PINs, and passwords. In some cases, the authentication can be done using vital criteria, such as a signature or physical tools such as a fingerprint, (Kaufman, 2009).

2- Authorization

It is the right to do a specific activity by a specific user such as reading a file, running a specific program, or accessing a service.

3- Nonrepudiation

It includes verification and authorization when they go together and complement each other. An individual must verify that he/she is authorized to do a specific activity before doing it. When the verification and authorization are accepted, the required activity can be done, otherwise, it will be denied.

It is important to indicate that all of the above basic internet securities can be applied individually or together. That depends on the type of website and the services provided.

2.3 Internet Security Incident

The internet security incident is defined as any network-related activity that leads to negative security consequences, (Howard, 1997).

This usually means that the activity explicitly or implicitly violates information confidentiality and privacy.

Security incidents can happen in different shapes, sizes, and results in different consequences. For example, it could come from any website; it could come from specific systems or networks. In addition, it could happen when the attacker has access to the subscribers' accounts. Unauthorized entry may be a relatively simple event that affects one site or a major event that affects tens or thousands of sites.

The worse cases can happen when the attackers can reach the users' accounts and using the victim's system to attacks other websites. Table (2.1) show statistics about the number of internet incidents over time. Table (2.1) clearly show the huge growth in the number of internet incidents over time. That reflects the need for more internet securities.

There are many types of an internet security incident that can be classified into as follow:

1- Probe

The probe incidents are the unusual repeated attempts that ultimately enable the attacker to enter a system or to discover information about the system. For example, when the attacker tries to access an account that is not in use.

2- Scan

The scan is simply surveying a large number of investigation attempts using an automated method. The result of the scan can sometimes be an incorrect configuration or has another error. However, more often it can lead to a more accurate attack on vulnerable systems.

3- Account compromise

It is the unauthorized use of an account by someone other than the original owner of that account. That can happen when the account has no level of security and privileges such as privileges of the system administrator or network administrator. This type of incident can lead the victim to lose important data and information.

Failure to reach the root level (which is the administrator level) means that the damage can be under control. In addition, it also means that the user level can reach deep into the system, (Lee and Lee, 2012)..

4- Root compromise detection

The root statement is similar to the user's account statement except that the account has special privileges in the system.

The term "root" is derived from UNIX system accounts that give the user unlimited privileges. It is also called "Super fuser" privileges, (Grossman, 2012).

Table 2.1: The Growth of the Number of Internet Incidents Over Time

Year	Number of internet incidents
1988	6
1989	132
1990	252
1991	406
1992	773
1993	1334
1994	2340
1995	2412
1996	2573
1997	2134
1998	3734
1999	9859
2000	21756
2001	53658
2002	82094
2003	76404

Source: Lee (2012).

Intruders who can access the root detection can learn anything about the victim's system. In addition, they can run the victims' programs, and changing how their system works.

5- Packet Sniffer traceability

It is a program that monitors the movement of data packets sent over the network. That data may include usernames, passwords, and other private information is sent in the form of unencrypted plain text.

By possessing perhaps hundreds or thousands of passwords, attackers can launch widespread attacks on many systems. Installing such software does not necessarily aim at privileged access. However, it can work as root detection.

6- Denial of service

The goal of the blocking operation is not to gain unauthorized access by the attacker, but to prevent legitimate users from using a service. Denial of service can come in

many forms. For example, attackers may flood the network with a large torrent of data to slow or paralyze traffic. Attackers can be carrying control commands or suspending network connections. They may block physical components of the network or manipulating the destination of the data.

7- Exploitation of trust

It is expected that computers on a network are trusting each other. For example, before executing some commands, a group of computers were examined to determine which ones on the network are permitted to use those commands. If the attackers could form an identity that enables them to use the trusted computer, they will be able to gain unauthorized access to other computers.

8- Malicious code

Malicious code is a general term for software that causes unwanted results in the system when executed. Systems' users usually do not aware of the danger of this software until they discover the damage. The malicious code may contain Trojan horse programs, viruses, or worms.

Trojans and viruses usually hide in your programs or files and then attackers manage them remotely to corrupt more than you expect. Worms are self-replicating programs that spread without manual intervention after they start working. Viruses are also self-replicating programs, but they usually require some work to be spread unintentionally to other programs or systems. These types of programs can lead to serious data corruption, significant loss of time, denial of service, and other types of incidents, (Anderson, 2014).

9- Internet infrastructure attacks

These attacks are rare but serious, and they target major components of the internet infrastructure rather than specific systems on the internet.

For example, the attack network servers, internet service providers, and the large archive sites that are used by many users. In addition, widespread automated attacks can also threaten the internet infrastructure and can seriously disrupt the daily operation in many locations,(Chakrabarti and Manimaran, 2002).

2.4 Internet Risks in Electronic Commerce

Traders around the world practice their electronic activities in the open field on the internet without security restrictions. Traders can be individuals, private companies, and public institutions. Traders usually have their own websites to display their information and products on the network. That can make their websites open to multiple types of internet risks. The internet risk in this case depends on the size and importance of the trader's activities on the internet. The most common types of risks related to this case are,(Vysotska, Rishnyak and Chyryn, 2007).

1- Modifying the site’s content:

Modifying the site’s content is one of the simple risks that all traders can face regardless of the size of the information. The content here can be modified by attackers who may be amateurs or professionals. Attackers may change some content that affects the appearance of the site and makes it ridicule.

Attackers may be changing important data that can negatively affect the relationship between the companies and their customers. It is important to indicate that no party, whatever was its technical capabilities and advanced equipment can be saved from these risks. For example, the White House website and the US Air Force, which was supposed to have high security, were attacked.

2- Disrupting the functionality of the site

Some attackers occupy the server computers with a torrent of messages, attachments, and inquiries. That can cause the sites to become unable to deal with any inquiries coming from actual users. In addition, it can cause the inability of any user to access the site information.

One of the most famous incidents happened to AOL (American Online), which is the largest internet service provider in the world. What happened is that the e-mail system has stopped for 19 hours. There is another incident that happened to the Amazon website. This website was completely stopped working for a few hours. That forced the company to adopt a policy of having a full backup of the email system for each user.

3- Misuse of the site

The medium and small business are exposed to this type of attacks, which are practiced by hackers and cyber fraud. Attackers use the workplace site as a starting point to do attacks on another website. It is also possible that attackers use corporate information systems, which do not have adequate levels of protection to hide some files. That is more likely in cases of economic spying or banks and e-marketing sectors. For example, an attacker can hide a file that is not allowed to enter the bank's branch site, then the attacker enters the bank's headquarter website from outside and get what he/she wants.

4- Controlling internal information systems

This level is considered as one of the highest levels of risk. It is limited to institutions that have electronic linking systems between headquarters and their internal systems. This type of risk is the most influential type of e-commerce. Entering into the internal systems represents a real threat to the organization.

That may negatively affect the company's business or performance. It sometimes leads the company to completely suspend its operation. For example. the attackers may erase some of the internal information. That may lead to the loss of some important information that causes the operation to stop, until solving this issue.

2.5 Future Directions of Internet Security

The future directions of internet security are going towards developing an advanced safer environment in more than one field as follow, (Bellovin, 1998).

1- Network protocols

Most of the networks currently in use have changed in response to the increasing internet attacks. Some changes have done to strengthen the website's encryption. Other changes work on the diversity of encrypted verification to distinguish the source of the information. Almost all new networking under development uses modern cryptography to verify the source of the data and protect its integrity and confidentiality.

2- Intrusion detection

The detection of strange activity is based on the specific patterns of the normal behavior of networks, servers, and users. In the normal mode of work, it is possible to discover the mismatched or anomalous behavior. In normal behavior, the developers examine the data set over a sufficient period to obtain a good sample of the ideal behavior. However, the main difficulty facing the developers is that normal behavior is so variable. That is because it is a mix of different types of normal activities. Many of the activities are difficult to distinguish from the normal business of authorized users.

3- Software engineering

Current methods of software engineering are only successful in managing the mental complexity of designing and implementing software. As for the security aspects, the design of systems and programs was an afterthought rather than being an essential and complementary element to the general design of systems. That means the systems and programs are not likely to have exploitable security weaknesses.

4- Web software and scripting language

Downloading useful or entertaining material from websites to a local computer is the most common activity when using the internet.

For example, normal web browsing is a very simple issue for the users but it is a serious issue for internet security experts. That is because the information on websites may harm the personal computer just by downloading them. To solve this problem, the content can be done using both web and script languages. That is because they are specifically designed to implement such content. These languages may be (Java and ActiveX, or Java and Script) or maybe others.

5- Intelligent agents

The future of the internet environment is more likely going to rely on a proxy-based model to ensure safe and more reliable online transactions. More specifically, the task of agents is to implement programs that are not related to any specific host server.

Agents perform any processing or communication specified by the user, but in reality, the place of execution and processing is outside administrative control. The

conceptual model for the agent process is that there is a smart agent, at the request of a user. That agent can go to one or more servers to perform calculations or collect information, and then return the result to the user. The agent's business model may range from partial to fully autonomous, and the degree of independence of the agent may vary in his lifetime.

2.6 The Cryptography in the Internet Network

2.6.1 The concept of cryptography

The term cryptology is derived from the Greek word (Kryptos), which is a word that describes anything secret, mysterious, hidden. In the world of data messaging, cryptology can be defined as the method that can be used to create a more safe internet environment. Cryptology means that the data is encoded or encrypted to prevent its contents from being revealed by unauthorized users. More specifically, it uses text cipher and other methods, so that no one can reach them except the authorized users, (Zimmermann, 1998).

Cryptography has also many other definitions. For example, it is the study of mathematical methods related to the subject of information security. Cryptanalysis is the study of mathematical methods that attempts to uncover cryptographic techniques. Cryptology is the study of the two previous topics together. A cryptosystem is a general term referring to the set of cryptographic foundations used to support information security such as public and symmetric key technology, electronic signature, and others, (Piper, 1996).

2.6.2 The principles of cryptography

Cryptography often requires that the data must be kept safe from unauthorized access. The best protection solution is natural protection.

That is to place equipment in safe buildings. However, this is not always the right choice because of high financially expensive and lacks of efficiency. To solve this problem, six considerations must be taken, as follows, (Goyal, 2012).

1. Confidentiality.
2. Authentication.
3. Authorization.
4. Data Integrity.

5. Non-repudiation.
6. Availability of data

2.6.3 Applying cryptology

Cryptography is used for security considerations, and to encrypt data that is settled in storage media, or transmitted over communication channels. The goal is to prevent any illegal access to the data. Cryptography is also used to secure verifications between the various parties when trying to perform any function within the system. Since each party desires to hold the powers on the system, it must present something to prove what it says, (Shankar, Lakshmanaprabu, Gupta, Khanna, and de Albuquerque, 2020).

That is known as Credentials. There are criteria to ensure the validity of these credentials and the identity of the true owner. The obvious and classic example of this identity is the password. These passwords are used to protect user accounts from illegal use.

2.6.4 The key-based encryption

Nowadays, the most common encryption process in the practical field depends on the key. The key is defined as a group of bytes, which are used to encode plain text into mysterious text. There are two types of key encryption, depending on the availability of the key, (Al-Haidari, Gutub, Al-Kahsah and Hamodi, 2009).

1- Private key encryption

In private key encryption, both the sender and the receiver use the same key. That key must pass the secret communication channel. To communicate, the two parties exchange the key, this process is known as Key Distribution. The process must be complex and difficult to guess.

2- Encryption with the public key

In this case, each party owns two keys, one of them is known to all and called the public key, while the other is kept secret and the owner knows it. This key is called the private key. When one party wants to communicate secretly with another party, he/she encrypts the data to be sent with the public key. On the other hand, the recipient can decode the data with his private key.

2.6.5 Electronic signature

The emergence of public-key encryption systems gave rise to the concept of electronic signature. The electronic signature scenario can be summarized as follows:

Assume that there are two parties (party 1 and party 2) who want to communicate safely through the internet. They use the private key (A) and public key (B).

1. Party 1 encrypts the data with its private key (A), and this is like a signature.
2. Party 1 encodes what was produced from step (1) with the public key (B), and sends the result to party 2.
3. Party 2 decodes the incoming data with its private key (A), and then decodes the result with the public key (B).
4. 4-If the first batch of data is known to the recipient, this will document the rest of the data, as well as the sender.

2.7 Receptive Properties of the Arabic Language

The natural languages of the human being are characterized by having a very complex statistical structure. The statistical distribution and the number of letters may differ from one language to another. However, all languages are characterized by an irregular distribution and a relatively high frequency. That allows their speakers to know the intended meaning even if part of the message was lost or slightly changed, (Nemat, 2011).

In the Arabic language, for example, the relative repetition varies from one letter to another. In the Arabic alphabet, some letters (such as the letter Alif) appear much more than other letters (like the letter Dhaa), indeed the probability of a specific letter appearing in a written text depends directly on the letter or letters preceding it.

Many studies were conducted to know the statistical distribution and the information rate of the Arabic language. One important reference of these studies is the Holy Quran. The Holy Quran represents a long text that has 77888 words and 402871 letters, including spaces between words at a rate of 5.17 letters per word.

The information rate of a language is defined as the amount of doubt (or uncertainty) about the message that the source can produce. For the Arabic language, it equals 2.4 binary units, while for the English language is 1.5 binary units. The characteristics

that distinguish the Arabic language from others make it useful in writing encrypted texts, (Hawkins,Yen and Chou,2000). Table (2.2) shows the informational characteristics of Arabic and English.

Some terms in table (2.2) are defined as follow:

- Redundancy: The difference between the greatest possible rate of information and the actual rate of information.
- Relative repeatability: It is the repeatability ratio of the actual information rate.
- Index of Coincidence: The probability that any two letters are chosen randomly from a text is the same.
- Roughness Factor: It is the statistical variance of the character distribution of any text clear or blind.
- Unicity Distance Limit: The lowest possible length of the captured text, which, in theory at least, enables the attackers to find the secret key used.

2.8 Types of E-Commerce

E-commerce has made a significant contribution by cutting out paper documents to replace them with electronic files. Eliminating the use of traditional paper documents can save paper, and save time by reducing the slow movement of paper documents. E-Commerce can eliminate the probability of risk that comes from corruption and damages. It can also save spaces by reducing the possibility of inflating the archive of paper documents.

E-commerce can be viewed as a multi-dimensional concept that can occur through nine forms. The most important e-commerce form is the one between a business unit and a commercial activity.

The forms of e-commerce vary and differ according to the type of activities and their targets. Below is the list of different Types of e-commerce, where (B) represents the business, (C) represents Customers, and 2 is (to). For example, (B2B) means trade between business to business, and so on, (Strader and Shaw, 1997).

Table 2.2: The Informational Characteristics of Arabic and English

Property	The English language		The Arabic language		Code
	Without space	**With space**	**Without space**	**With space**	
Number of letters	26	27	29	30	M
Information rate	1.5	1.23	2.4	2.0	H
Redundancy	3.2	3.52	2.37	2.91	R
Redundancy Relativity	%68	%74	%49	%59	r
Index of Coincidence For clear text	0.066	0.077	0.0697	0.083	ICmax
Index of Coincidence for random text	0.038	0.037	0.0345	0.033	ICmin
Roughness Factor	0.025	0.040	0.0352	0.05	MR
Unicity Distance	28	27	44	38	U

Source: Al-Haidari, et al (2009).

1. B2B e-commerce

This is a type of trading that targets commercial exchanges between companies. Usually, these deals are big, and they are mostly wholesale. This type of electronic commerce occupies most of the transactions that fall within the scope of electronic commerce.

Transactions in this type take place between the two parties through the internet. These transactions could be for the purpose of selling and buying goods, the flow of information, or the implementation of some services. An example of this type: Dell Company sells its products to companies through its online order. Figure (2.1) illustrates this type of e-commerce.

2. B2C e-commerce

In this type, companies offer their products or services to customers who are distinguished by their different social levels and the heterogeneity of their personal preferences.

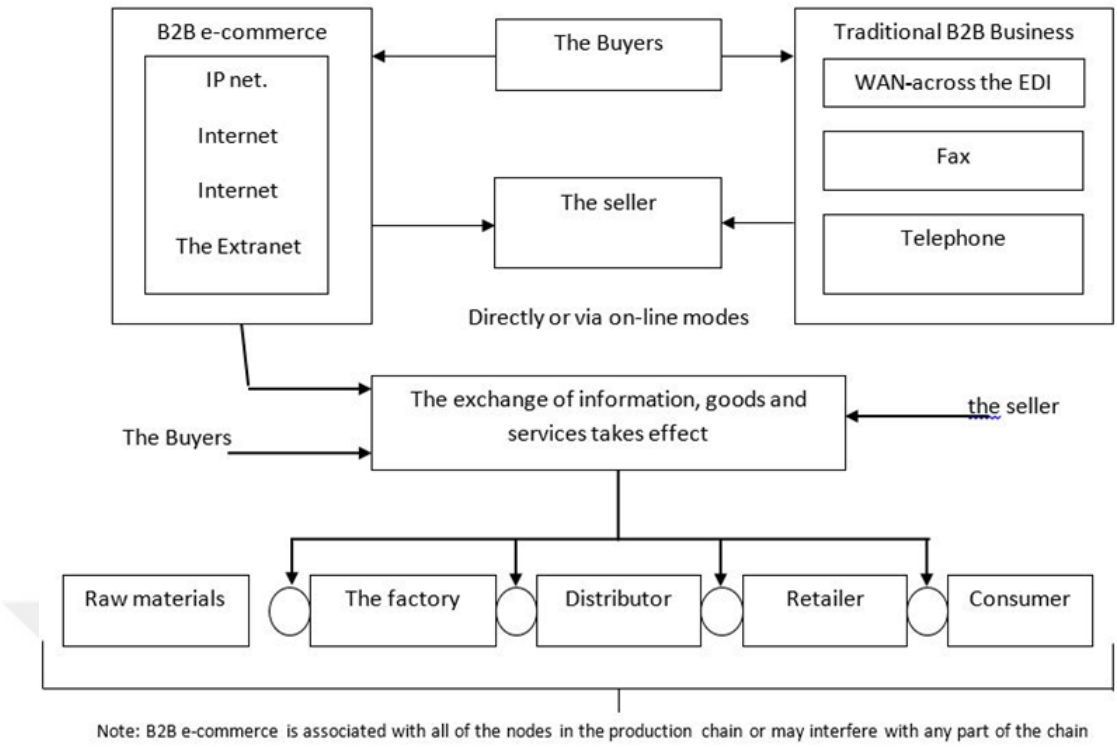

Figure 2.1: The Process of B2B E-commerce

Source: Nemat, (2011).

3. C2B e-commerce

In this type, individuals sell their services or products to companies. For example, someone offers to provide a website design service for companies, or someone offers to design uniforms for the company's employees.

4. B2B2C e-commerce

Electronic transactions take place through two steps in this type. The first step is from the company (factory) to another company (wholesale). The second step is from the company (wholesale) to the consumer. For example, a major company manufacturing electrical appliances supplies to stores that sell these appliances, and the stores sell them to consumers.

5. Intra Business

In this type, electronic transactions take place between the different units of the same company. That is each section benefits from what the other section produces. For example, a company owns a unit for manufacturing tires and another unit for assembling cars. The assembling unit buys tires from the other unite.

6- B2E e-commerce:

In this case, the company provides its products to its employees at low prices and special offers.

7. C2C e-commerce

An individual trades with other individuals. Someone posts his/her products on the internet, and consumers buy them. Two implementations of C2C markets, the first one is the auctions, and the other is the advertisements. C2C marketing has become more common now. Examples of this type are companies such as eBay, and Craigslist.

8. E-Government

The governments provide their services to the citizens through electronic platforms.

2.9 Electronic Markets

The electronic market is a website that provides electronic trades and financial transactions. In these types of markets the exchange of products, services, information, and money can be done. The electronic market is not a building, but it is a network that provides electronic commercial transactions, (Yu, and Kuo, 2002).

The participants in the electronic markets, including sellers, buyers, and brokers, are usually from different places, and they rarely know each other.

The methods of communication between individuals in the electronic marketplace differ from one individual to another and from one case to another.

2.9.1 Electronic payment methods and systems

There are many methods of electronic payment, and below are some examples, (Boss,

2000).

2.9.1.1 Credit cards

Credit cards are defined as plastic cards made of a material that is difficult to tamper with. They are often issued by banks or financial institutes. Usually, these cards have the name of the owner and his/her account number.

The cardholder has to present the card to the store when paying for his purchases. Special electronic machines can read the card and make the transaction. The money will automatically transfer from the cardholder account to the store account. The use of credit cards can be safe and fast.

It is important to indicate some common institutions that are related to credit card transactions:

1. The International Card Center: It is a global institution that sponsorships the cards and approves the membership of banks around the world.
2. Card issuer: They are banks and other financial institutions.
3. Merchant: It is a term used to refer to the companies and institutions in which the card issuer agrees to accept the transaction with the cardholder.
4. Cardholder: any individual who owns the card and uses it to buy goods and services from merchants or withdraw cash from cash withdrawal machines or banks.

2.9.1.2 Digital or electronic money (Digi-Cash / E-Cash)

- Electronic money is intangible money, but it takes the form of electronic units. The transaction using the electronic money is done by a safe client's "electronic wallet". The customer can use this wallet to sell, purchase, and transfer money.
- There are two types of electronic money.
- The first type is nominal electronic money. In this type, the electronic cash unit contains information related to the identity of all people who traded., which is similar to credit cards where the bank can trace the monetary unit during its circulation.
- The second type is the non-nominal electronic money where the unit of cash is traded without disclosing its holder unless someone tries to spend it more than once. The advantages of the electronic month are that it is easy to use, it has confidentiality and privacy, it is safe, and it has low-cost transaction

2.9.1.3 Electronic checks

These checks are used to do electronic payments between two parties through an intermediary. The electronic check does not differ from the paper check except that electronic checks are processed through the internet. The electronic check is an electronic document that has the check number, the payer's name, and the payer's account number. In addition, it has the name of the bank, the name of the beneficiary, the amount of money to be paid, the unit of currency used, the date of validity, the electronic signature of the payer.

2.9.1.4 Smart cards

It is a plastic card that has an electronic chip. The cars has also data storage that can save the payer's data such as name, address, issuing bank, and others. It is possible to link this card to a computer, to download data and information. This card is also called the electronic check book because it can provide a complete record of the transactions made by the cardholder.

This type of card is characterized by several elements to protect against theft. These safety elements are the type of plastics, the magnetic tape, the customer's photograph, the password, and the inability to open the outer cover.

One advantage of this type of card is that it can substitute for cash in all transactions. In addition, it has easy account management, high safety, and it allows money transactions between holders of this type of card without visiting

2.9.2 E-commerce solutions

The first question facing online traders is how to determine who is responsible for creating and managing the electronic transactions, (Bingi and Khamalah, 2006).

In other words, do they make a deal with another company that handles this process, or do that themselves? The answer to this question depends on several things as listed below:

1. Company size.
2. Previous experience of the company in e-commerce.
3. The costs including employee training and the costs of electronic devices and services.

For Small companies that have few technicians and have a small financial budget, it is better to make deal with another company.

The big companies that have experience in e-commerce and good IT technicians have two options. Either making deal with another company or do it. The

2.9.2.1 The electronic transactions providers

There are three types of companies, which provide and manage electronic transactions, (Boss, 2000).

1- Internet complexes

There are around three thousand internet complexes. The complex consists of a single front end for a group of electronic front interfaces. Any complex with successful management allows buying and selling transactions between stores. It also provides payment methods so that the buyer can pay only once for the purchase from different stores. The owner of the complex is sharing the net profits of the stores.

2- Internet service providers

Internet service providers provide internet connection services to many companies and individuals. In addition, they also provide host services to e-commerce. They provide a safe environment for financial transactions and do not give much importance to the content of the shop. That means the traders who use their services have to request web design from another specialist company.

3- Telecommunication companies

The telecommunications companies provide e-commerce solutions services. The main customers of these companies are other large companies. Many companies have started building and managing their electronic services on their own. However, the difficulties in technical and marketing complexities affect this trend.

The development and construction of any electronic services must be done in light of the technical standards and habits of the company itself. For example, a company that has a lot of UNIX equipment should use Linux hardware, software, and tools in the process of creating and managing its website.

2.9.2.2 E-commerce challenges

Information security is currently the cornerstone of the rise of information and communication technology. It is known that internet privacy is inversely proportional to the technological advancement of information and communication. Therefore, it is important to innovate new information and communication technology that satisfy the safety and the privacy of users. The most common challenges in this issue are, (Thekkath, Nguyen, Moy and Lazowska, 1993).

1- Technical challenges of e-commerce: There is a lack of reliability and safety. There is not enough bandwidth. Software tools are still changing rapidly. It is difficult to connect the Internet and e-commerce software with some applications and databases currently in use. Providers may need special web servers and other infrastructure. Some e-commerce software is not compatible with some hardware components or with operating systems.

2- Non-technical challenges of e-commerce: The cost of developing e-commerce could be very high. It is hard to select a provider company to do an e-commerce system because it is not easy to know which company is right.

3- Security and privacy: Some customers do not trust sellers who do not see them or trust paperless transactions or electronic cash.

3. THE SECURE ELECTRONIC PROTOCOLS

3.1 The Secure Electronic Transactions Protocol, (SET)

Before starting the study of the Secure Electronic Transactions protocol (SET), a general idea about the network's protocol must be given. It is important to know about its setup, uses, limitations, and relationship with the other protocols.

The network protocol is a set of laws, regulations, and formulas that govern and control the connective process between any party and its counterpart. In other words, the protocol permits both parties to agree on a set of messages that could benefit the connective process itself. These messages are not the messages that require a transfer or the actual data, (Kessler, 2004). Below is a brief review of the most famous network protocols.

1. The (TCP/IP) protocols

This group of protocols enables users to achieve a connection through networks that have different environments and different properties. For example, windows environment and Apple Mack environment. Therefore, they gain a global standard in internet working, (Khare, 1998). This group of protocols has four layers:

- Application layer
- Transport layer
- Internet layer
- Host-to-Network layer

2. The (Telnet) protocols

This protocol allows the users to access another computer's sources called the server (Telnet Server).

After requesting some files for security purposes, such as a password it starts the (Telnet) session. Then, users can use whatever app they want after putting in the right password, (Shiquan, 2008).

3. The (FTP) protocol

This type of protocol Help users to receive the files they want from other computers whatever their hardware or software features are. Users can complete multiple tasks that are in relation to the files and indexes, (Pawlowski, Noveck, Robinson and Thurlow,

2000).

It is important to indicate that both (FTP) and (TELNET) protocols can work together to ensure the connection to the other computer. In addition, they work together to ensure that the users receive the files they want with specific connectivity and security. Neither one of those protocols is a server. However, the users' computer uses the programs in (FTP) and the server computer uses the server programs in (FTP).

4. The (NFS) protocol

This protocol is very important to networking especially for sharing existing files on the network's computers, which may differ in software. Suppose the NFS's server is implemented with the NetWare operating system. Suppose that NFS's client software is implemented with the UNIX operating system, (Riabov, 2005).

Then, this protocol will specify part of the storage memory for the NetWare server to store some of the UNIX files that the users need. It does that even though the file system in NetWare is different from the file system in UNIX. Therefore, the users of both systems can receive the same file according to their individual file system without feeling any difference.

5. The (SMTP) protocol

This protocol is used to send and receive (E-mail). This protocol consists of a user client, which is a program for reading or preparing incoming or sending mail. In addition, it also has client message transfer, which is another program for sending or receiving incoming or sending mail, (Hare, 2011).

This protocol is used for communicating mainly between messaging clients. Some clients may use the protocol (POP3) for e-mail. Mail is exchanged between message transfer clients after the connection is established, as the transport client that wants to

send a message to another transport client establishes a connection that is supervised by (SMTP).

6. The protocol (SNMP)

One of the most important and prominent factors that help the success of the network continuity in operation is to closely monitor the network. The network manager can achieve this by using the protocol (SNMP). This protocol collects and processes valuable and important information related to the network's performance, (Jestratjew and Kwiecien, 2012).

This protocol can help the network's stations to monitor, collect information within fixed time frames, and send reports to the management station. In addition, it also plays a role in informing the network administrator about any sudden events or errors in the network. This protocol also has a degree of sensitivity that can be controlled. The only person who is able to control it is the network administrator.

7. The protocol (HTTP)

It is the protocol of moving web pages. It consists of many messages and responses that the client (which is the browser) and the server exchange. The exchange can be before, during, and after the transfer of the requested web pages. This protocol provides the owner a simple transmission technique that ignores or avoids the contents of what is transmitted. Requests for this protocol generated by the browser are text files based on ASCII code, (Kravets, 2013).

This protocol represents the goal of the request or the work required from the server, and there are three functions in the protocol:

- The (GET) function is often used when a user uses the browser to request a web page or to display an item from a specific page.
- 2. The (HEAD) function is used to request header information only, as a part of the request letter in the protocol. The sender places additional information in special fields called header fields, and this information benefits the recipient, such as the required file size and the type of data.
- The POST function is used to send information from the client to the server process. Such a function is very important, especially when filling out forms That is because it enables the designer to retrieve information from the user.

For example, a password that sends out where it will be processed and analyzed and will perform some work depending on the result.

This protocol has also some other elements. The first element is the page address (URL). The page address can be requested by users to search for information. The second element is the version ID (HTTP). The version ID is used to determine the version of the HTTP that is being used. The third element is the Header information. That can be used to send information to the server, or the response messages that the server responds to.

The response status in which the server informs the client of its initial response to the request, and this response consists of three numbers that have a specific meaning as shown in table (3.1).

The size of the response message including the data that will return to the client, and the response message do not contain data that belongs to the client. Therefore, the existence of this field depends on other factors.

Table 3.1: The Response Status of the Server to the Browser.

Numbers	General Meaning
200, 201, 202, 204	• Completely positive response. The request has been received, understood, and will be delivered.
301, 302, 304	• The request has been received, but there is some additional information necessary to fulfill the request completely.
400, 401, 403, 404	• The request will not be fulfilled because there is something wrong with it that the customer is responsible for (such as if the order has incomplete parts or fields)
500, 501, 502, 503	• The request will not be fulfilled due to an error in the server.

Source: Jestratjew and Kwiecien, (2012).

8. The protocol (TCP)

It is a protocol that not only greatly important for the internet, but for everything related to networking. This protocol is highly reliable, which guarantees accurate data transmission. That is because it has been equipped to perform error checks and re-broadcast when it is necessary. In addition, it can help to provide reports to the higher classifications of errors that cannot correct themselves, (Partridge and Pink,1993).

This protocol can break down the data into several parts called packages. It can number them, arranges them, sends them, and waits for utile receiving notification of arrival. If a package does not receive a notification, it is resent until receiving a notification, and then it will be installed in the target again to obtain the original data.

9. The protocol (UDP)

When network reliability is not a primary issue, this protocol is a successful alternative to the previous one. This protocol receives the data from the higher classes, breaks it down, and numbers it. Then, it sends it directly to the target without establishing contact with them or waiting for a notification, (Borella, Grabelsky and Taniguchi, 2001).

10. The protocol (IP)

This protocol supervises the transportation of packages that need an address for a target station and a sending station. This address must be understood and work properly to be used in the routing process. That what makes this protocol places the address itself, (Gupta and Sharma, 2011).

Therefore, every local or abroad network must label all its stations with a distinguishable address called (IP Address). The IP address is often done automatically. This address consists of 32 bits, which are four bytes separated by three points. Each byte of the four bytes represents a decimal number. For example, the address maybe 172.16.122.204.

There are three different classes of addresses, which are A, B, and C. Although the address appears to be a single value, in reality, they are two different addresses. One of them represents the address of the network in which the station is located. The other represents the address of the station within the network. Therefore, the network address is the street address and the station address is the home number within a large city, which is the internet. Table (3.2) shows different types of IP addresses.

Table 3.2: The Different Types of IP Addresses.

Type	Form	The network address field	Number of Stations
A	N.H.H.H	126 -1	16777214
B	N.N.H.H	128191 -	65543
C	N.N.N.H	192233 -	245

Source: Borella, et al (2001).

3.2 The Concepts of the Secure Electronic Transactions (SET)

The secure electronic transactions SET is an open encryption and security system. The SET is used to protect the confidentiality of online electronic money transfers, (Lee, 2015).

The purpose of SET is to ensure the preservation of data, security, privacy, and integrity. In addition, it is used to verify that it reaches the required party while conducting financial transactions over an open network such as the internet.

The SET protocol is not a payment system, but rather is a set of protocols and procedures that help users safely entering their credit card numbers over an open network such as the Internet. More specifically, it does the below three things:

- It provides a secure communication channel between all parties involved in the transfer process.
- Provides identity verification by adopting digital certificates.
- Secures the privacy of the parties involved by sending them information when and where necessary.

The SET uses software called Electronic Wallet Software. This Wallet is used to maintain the privacy and integrity of the information transmitted over the internet between cardholders and merchants. The electronic wallet contains the cardholder's number and the digital certificate belonging to her/him. The merchant has a digital certificate issued by one of the accredited banks. Both the cardholder and the merchant use their digital certificate, which allows each of them to verify the identity of the other when making financial transactions over the internet.

The merchant cannot see the credit card number during the session of the Secure Financial Movements protocol. That is because the encrypted version of this number is sent to the issuer of this card to approve the financial transaction with the merchant. This method ensures that the number is not displayed, as well as prevents any unauthorized modification during the transmission of data.

3.3 The Electronic Financial Transaction between Parties Based on SET

The electronic financial transaction has five parties according to the SET, and these parties are, (El Ismaili, Houmani, and Madroumi, 2014).

1. The cardholder
2. The electronic wallet providers
3. The merchant
4. The payment processor
5. The payment gateway

A Cardholder is a person who has a credit card account (with Visa, MasterCard, or others). This person uses an electronic wallet that contains digital certificates for the secure electronic transfer (SET) protocol. The cardholder is the customer in this process, (Lee, 2015).

The Electronic Wallet Provider is the financial institution. The provider provides customers with tools that enable the secure purchase of goods and services over the internet. Examples of these tools are digital certificates, or certified SET.

Merchants are companies and individuals who offer goods and services over the internet. For these merchants to be able to respond to the financial transactions of customers, they must have a close relationship with payment processors or other accredited financial institutions, [46].

Among the parties of this process is the Acquirer or Payment Processor, which is the financial institution that provides merchants with accounts (accounts). In addition, these institutions undertake the verification to dealing with and processing payments made by customers.

As for the payment gateway, it is the device operated by the payment processor (Acquirer). This device handles the payment messages they receive from merchants, and the payment orders they receive from cardholders.

3.3.1 The steps of electronic financial transactions under SET

The customer first opens a credit card account in a bank. Then the bank issues to the card owner a specific program for the Secure Electric Transfer protocol (SET) called the electronic wallet program. This wallet is used in purchasing and making financial transactions over the internet, (Waters, 2009).

The electronic wallet is installed on the user's computer, where the user can access it at any time to make an online payment. This wallet contains information such as the credit card number, the SET Certificate, the expiration date of the card. In addition to

other information, the wallet program can be downloaded from the internet, and this program is password-secured.

On the other hand, the SET Certificate is considered proof that the bank has verified the identity of the cardholder. To obtain this certificate, the customer is referred to an agency authorized to issue certificates and approved by the bank.

The merchant opens an account with the Payment Processor of his choice such as a bank. The bank provides the merchant the necessary software to use the safe electronic transfer protocol. This software includes the SET Certificate granted to the merchant and the public key of the chosen payment processor. This software is used to process financial transactions on the internet.

On the internet, the customer can ask for a certificate of the merchant's secure electronic transfer protocol. That is to verify the merchant's status and make use of his/her public key. When a specific purchase order is made, the customer uses the electronic wallet to retrieve the credit card number and the certificate of the safe electronic transfer protocol.

The customer uses the merchant's public key to sign the purchase order information. In addition, the bank's public key is also used to sign the payment information that will later be directed to the merchant.

After that, the merchant returns with his secure electronic transfer protocol certificate to the bank or payment processor. That is to verify the customer's identity and obtain payment authorization. That depends on the customer's secure electronic transfer certificate (or payment confirmation letters).

The bank (or payment processor) verifies the merchant and customer's identities and processes the purchase order and payment information. After verification, the bank (or payment processor) digitally signs an authorization letter that it sends to the merchant. Then, the merchant sends a confirmation message to the customer and performs the services requested. Finally, the merchant generates the receipt, and ships the goods.

3.3.2 The dual digital signatures

It should be noted that the SET contains a new concept in digital signatures called a dual signature. This dual signature is intended to link two messages of different

destinations with each other in one message, (Panurach, 1996). The dual signature process is shown in figure (3.1).

In figure (3.1), the payment information (PI) goes to the bank, and at the same time, the merchant does not have to know the method of payment and the account number. In addition, the bank does not have to know the details of the purchase order. Merging the two letters into one message indicates that the amount paid is to purchase the same goods or service that is in the purchase order.

In some cases, the merchant can also receive payments from customers without a certificate of the secure electronic transfer protocol. In this case, the merchant only has to use his own financial transfer protocol certificate to document financial transactions with the bank or the financial transactions processor. After confirming the validity and acceptance of the financial movement, this merchant generates the bond, and ships the goods to the customer.

3.4 The Electronic Fund Transaction System (EFT)

The Electronic Fund Transaction system (EFT) is a critical part of the online banking infrastructure.

This system enables the movement of money transfers or payments from one bank account to another bank account. In addition, it can also transfer information related to these transactions using secure electronic technology, (Brandel and Geary, 1981).

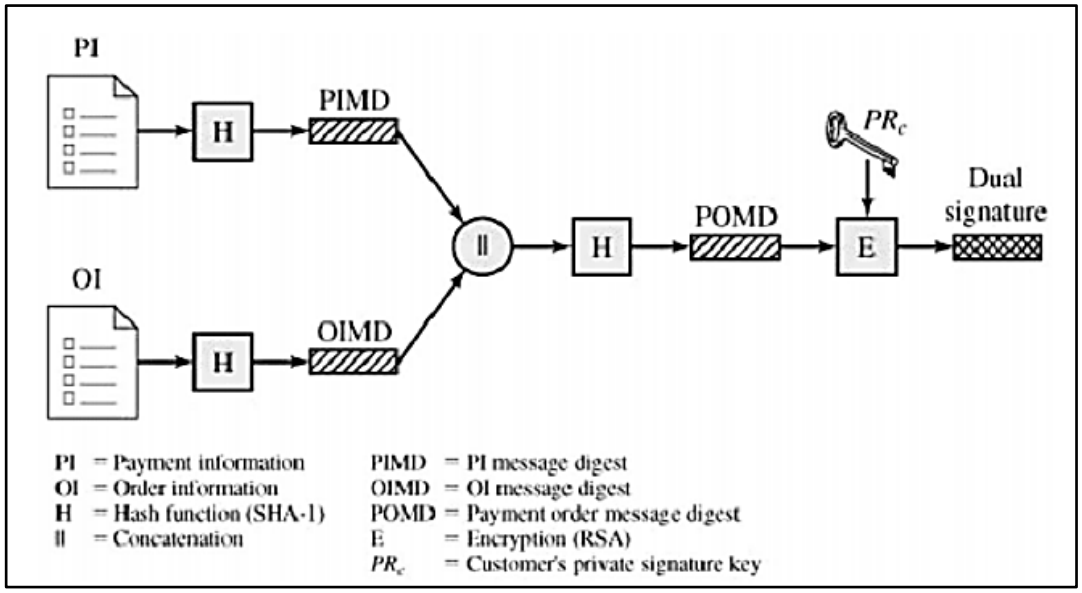

Figure 3.1: The Dual Digital Signature.

Source: http://www.idc-online.com

This system was initially introduced by the USA government. The USA government had adopted the idea of an electronic money transfer system, due to its desire to convert more than a billion financial movements from the paper transfer system to the electronic transfer system.

The EFT is characterized by a high degree of security, ease of use, and reliability, but it should be applied correctly to have these advantages.

3.4.1 The concept of EFT

The Electronic Fund Transfer System is the process of granting permission to a bank to carry out credit or debit money transfers. A money transfer is an electronic transfer from one bank account to another bank account. The transfer process is done electronically via telephones, computers, and modems instead of using paper, (Arcari, Lewis and Donnald, 2004).

The money transfer operations are executed via the Automated Clearing House (ACH). The ACH is a network owned and authorized by the banks participating in the electronic money transfer system.

Since 1978, the EFT Corporation has allowed companies and institutions to collect their financial transfers electronically via the Automated Clearing House (ACH). This service was distinguished from the old system (the paper system) in that it is faster and more capable of processing various financial transfer services. For example, the service of direct deposit of paychecks which can be collected when they are due, and the scheduled payments service.

3.4.2 The process of EFT

In the EFT, the customer signs a one-time authorization form for the benefit of the beneficiary (for example, the merchant). This form allows the specified value to be deducted from the customer's account according to a specific time order (daily, weekly or monthly). The electronic money transfer form differs from the check-in in that its validity applies to more than one transfer. Usually, the bank and the customer deal with brokers (Mediators) whose job is to provide the necessary software, (Mthembu, 2010).

The customer sends the money transfer via modem to the Mediator. The broker collects the money transfers and sends them to the Automated Financial Clearing

House (ACH), which in turn sends the electronic money transfer form to the customer's bank.

The client's bank compares the money transfer (received from the clearinghouse) with the customer's balance. Notice of insufficient balance to the broker to return the notification to the customer. However, if the balance is sufficient to cover the value of the money transfer, the transfer value is transferred to the beneficiary's account (the bank or the merchant) at the time of payment specified in the form.

If the merchant wants to implement the financial transfers through the ACH without going through an intermediary, the merchant must buy the special software that allows this process to take place. In this case, the customer approves the payment form attached to a certified check in favor of the merchant.

Then, the merchant sends the credit to the automated clearinghouse, which in turn sends the credit to the bank to deduct the amount from the customer's account.

Then, transfer it to the merchant's account. In this case, there is no need to verify the adequacy of the customer's balance, because a certified check guarantees this.

3.4.3 The advantages of EFT

There are several advantages of using the EFT system as shown below, (Anderson and Lanen, 2002).

1. One-Time Payments:

The agreement on the time of deduction and payment of the value of the transfers guarantees the organization of payments without any doubt about the possibility of payment at the specified time.

2. Convenient:

The automated clearing process eliminates the need for the customer and merchant to visit the bank to deposit the value of money transfers. That can be facilitating the matter and raising the effectiveness of the work system.

3. Safety and Security:

Automated clearing and electronic money transfers have eliminated the fear of paper checks being stolen and the need to move cash.

4. Improve Cash Flow:

The electronic delivery of cash transfers increases the reliability of cash flow and the speed of money transfer.

5. Reduce Paperwork:

This is to reduce reliance on paper forms, traditional checks, and other paperwork.

6. Money saving:

The automated clearing system network reduced the costs of managing the clearing operations.

7. Promotes Customers Satisfaction:

The speed and low cost of electronic transfers ensure customer satisfaction and consolidate their confidence in dealing with the merchant or company.

3.5 The Electronic Data Interchange System (EDI)

Electronic Data Interchange system (EDI) is a set of standards that are used in the exchange of business information between the computers of business partners. In addition, it can be used in the achievement of business transactions in an electronic manner that does not support paper, (Crook, and Kumar, 1998).

The electronic data exchange system transfers the information related to inquiries, purchase orders, pricing, order status, and scheduling of appointments. In addition, they transfer information related to shipping, reception, invoice payments, contracts, production data, and sales. The electronic data exchange system does not depend on the types of computers, software systems, or processes used at work.

3.5.1 The software of the EDI

The software of the electronic data exchange system has many advantages to suit various business applications. The most important of these advantages are, (Wang, and Seidmann, 1995).

1. Easy to Upgrade:

There is the progress made in trade through electronic data exchange systems. That required this software to be easy to upgrade to be able to keep up with developments and benefit from the latest modifications.

2. Multi-Network Connectivity:

This software should not place any restrictions on communication with the main networks through which data is exchanged.

3. The ability to deal with several standards:

The Business partners exchange electronic documents using different standards, so the software had to meet this need.

4. Printing support:

Some companies require hard copies of incoming letters to them, and software needs to support this.

5. Ease of Mapping:

A large company that deals with a large number of partners needs software that allows easy reconstruction of the documents.

In addition, it should be in line with other software applications used by this company.

The companies have two options to carry out electronic communications. The first option is the use of direct transmission, and the second is the value-added networks (VANs).

The direct transfer method is characterized by being simple, easy, and inexpensive, but one of its disadvantages is the possibility of transmission errors.

In the case of using value-added networks (VANs), the company cooperates with another company (third party) providing this service in order to enable electronic communication with business partners.

The VANs provide all the equipment that business partners need to securely transmit and receive information. In fact, VANs are more expensive than direct transmission, but they are also more efficient in transfer due to their ability to transfer protocols (Protocol Conversion). That means, they allow communication between commercial partners who have different computer systems.

The VANs reduce phone bills because their charges depend on the amount of data transferred, not the transmission distance. Companies that provide this service include AT&T, Sterling, and IBM.

3.5.2 The operation of EDI

The electronic exchange software at the sending party converts first the document into a standard format. Then, a value-added network phone number dials in, and the message in a file inside the sending computer is transferred to an e-mail box on the VAN. This enables commercial partners' software to retrieve the file from the e-mail box. In addition, it interprets the message it contains, checks its compatibility with its electronic exchange standards, and then store it, (Benjamin, David and Morton, 1990).

A Functional Acknowledge message is sent to inform the sender if the message has been received or not. In addition, it informs the sender in the event of any communication problem. Furthermore, it informs the sender whether or not the message complies with standards for electronic data exchange.

Then, the recipient has two options for dealing with the message. The first option is by using EDI translation software to produce a printed copy.

The second option is by reconstructing the message in a format that suits their computer applications before performing any further processing of the message.

3.5.3 The benefits and limitations of EDI

Many benefits can be obtained using the EDI, (Freier, Karlton,and Kocher, 2011).

1. It can Reduce the running costs, as this system reduces the effort exerted in dealing with documents and mail work. In addition, it can reduce the expenses spent on managing these documents.
2. The EDI can help saving time, as this system allows information to be transferred faster than it was previously.
3. The EDI can help to improve internal management by reducing paperwork, reducing the inconvenience of ringing the phone, reducing entry errors, as well as speeding up the production of reports.
4. The EDI can help to improve the relationship between customers and merchants. More specifically, the information is passed faster between them by reducing the time spent to secure communication between the two parties.

Therefore, the electronic data exchange system increases the competitiveness of the company that adopts it. That is because it saves time, effort, and money. As a result, it is not surprising the increasing number of large companies that adopting this system.

Even the EDI has many benefits; it has also some limitations, which are:

1. The relatively high fixed cost:

Despite the many advantages of the electronic data exchange system, its fixed cost ranges between $ 50,000 and $ 2 million, which makes it unsuitable for medium and small companies.

2. The need to deal with old systems (sometimes):

Some companies that use the electronic data exchange system still have to follow their old system to keep customers who do not use the new system. That means, they need to keep additional records.

3. Some communication problems:

Problems of this type arise when the business partner's line is constantly occupied.

4. The tendency of resisting change:

The lack of knowledge and education of some business partners, or employees, makes them not welcome automated procedures and methods. Therefore, it is necessary to solve this problem by training and teaching them.

3.6 The Secure Sockets Layer Protocol (SSL)

3.6.1 An overview

The issue of security of all kinds of transactions over the internet has become an important matter even with the need for some requirements. The basic security of transactions begins with the "Secure Sockets Layer" (SSL) protocol. This protocol was developed by Netscape to act as a layer of software. Its role is to separate a specific program such as the browser and the mechanism of transmitting data over the network protocols like the TCP / IP protocols, (Bisel, 2007).

The SSL protocol provides internet users with a secure communication channel. Users, who visit commercial internet sites, sometimes need to send sensitive

information such as a credit card or bank account number. The problem they have is the fear of intruders who intercept the flow of information and steal the information.

The SSL is designed as a security feature with an internet service that provides a secure path through encrypted communications between users and ensures the trust of internet contents.

The dynamism of the Internet dictates the need to find another system to verify the identity of the user. If, for example, someone wants to buy a commodity from your virtual store securely, he will not have enough time to search for and verify your public key, but he will need another automatic way to verify your identity and the SSL 3.0 protocol provides a solution to the verification problem From User Identity with Digital Certificates.

The server and client programs can agree on the encryption method function used by the SSL protocol. The server itself can authenticate to the client by sending an unencrypted digital certificate.

The digital certificate includes information about the company that owns the server. In addition, the digital certificate includes the public key of the server. The certificate is signed electronically by a trusted authority that granting digital certificates. This means the client has verified the validity of the information related to the company that owns the internet server and considers that the commercial activities are legal. When the customer trusted the server, he/she can trust the certificate signed by them.

Digital certificate awarding agencies do not provide their services for free. There are little few of these agencies including RSA and Verisign. To generate digital certificates for use within the organization's internal internet, the certificate server program can be used.

The customer and the provider must agree on a method for exchanging the key between them. In addition, they should have an agreement on the encryption method and the codes.

The SSL 3.0 protocol requires that the two parties agree on a set of randomly generated keys in order to fill all security weaknesses. These random keys are eliminated after the end of the communication session between them.

The practicality of internet security measures is very difficult. The SSL 3.0 protocol defines several methods of key exchange, while Microsoft IIS 4.0 and Netscape Enterprise Server 3.0 only adopt the RSA method, a method pioneered by RSA Data Security.

The SSL protocol has become the standard protocol that has imposed itself in secure transactions and in other exchanges over the internet. Most major Internet servers support the SSL 3.0 protocol, including C2NET, IBM / LOTUS, O'Reilly, and Microsoft. The IETF engineers see the development of internet technologies that use the protocol SSL 3.0 as the basis for a proposed open standard such as Transport Layer Security TLS.

All indications are that the safe trading dynamic continues to evolve and will have new standards and will export law changes. However, the three basic concepts (verification, encryption, and data integrity) that constitute safe transactions will remain the same.

3.6.2 The goals of secure online transaction that use the SSL protocol

Secure online transactions using SSL aims to accomplish three goals:

1. Ensure the confidentiality of information exchanged between two parties.

This information could be an e-mail, a message, a financial transaction, or anything else, and this requires the use of a specific method for encrypting data.

2. Enabling the recipient to detect any modification made to the message during its transmission. That is to ensure the integrity of the message.

3. Enabling each party to verify the identity of the other party and confirm that the person actually wanted and be able to immediately detect any attempt to impersonate.

3.6.3 The applications of SSL protocol

SSL can be used in the connection between two computers or applications requiring protection. The following are a group of practical applications for SSL, (Huan, 2013).

1. The SSL provides high security and creates a safe browsing environment on the internet. That can be applied on some sites that need privacy, and secure communications between.
2. The browsers' security is not sufficient to ensure more security of systems such as Secure Database Access Systems or Remote Object Access Systems (COBRA). Therefore, using the SSL protocol can be more secure. Other applications include indirect security (such as Proxy Server) and some Java applications can be used.
3. Banks and financial companies can use SSL to develop banking programs that use remote access and need a strong encryption method. Some applications that run outside the internet browser allow customers to audit their accounts (Account Balance) and other financial businesses that require a secure connection from a distance.
4. Many systems use SSL to create remote access and administrative applications. By using SSL, it is easy to create the secure circulation of information from a distance to control and access systems and to manage activities and system resources.
5. The SSL can create booking systems on the Internet and transfer secure information. Organizations that adopt SSL applications that can allow their customers to book tickets securely without notice of sales staff.

3.6.4 The structure of SSL protocol

The SSL system layer is located between the Transport Layer and the Application Layer that contains HTTP as shown in figure (4.2). The TCP / IP dominates communication and data routing on the internet, (Hickman, and Elgamal, 1995).

The other protocols such as HTTP and IMAP (Internet Messaging Access Protocol) are implemented at the top of TCP / IP. This means that all users in TCP / IP support and help implement applications typically such as displaying web pages and mail.

The SSL protocol is used to ensure the security of information in three steps. The first step is by the authentication that ensures sending data to the correct server and that server is secure too.

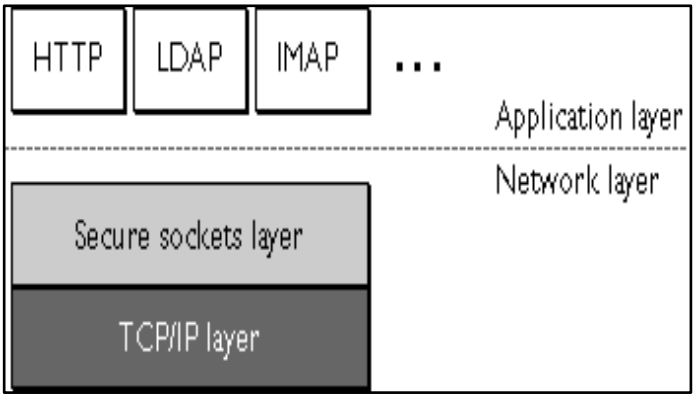

Figure 3.2: The Structure of SSL Layer.

Source: Chou, (2002).

The second step is the encryption that ensures sent data is only read by the secure target server. The third step is data integrity which ensures that the data received by the target server is not modified in any case.

The server is designated for verifying the client and the client is designated for authentication and verification of the server. They are authorized to establish a secure and encrypted connection. These capabilities are a basic address for secure communication on the Internet and networks that support TCP / IP.

The SSL has two protocols. The first protocol is the record protocol, which is located at the top of the transport layer. The record protocol is defined as the general form used for sending encapsulation. That is, any message is divided into a record of 32,767 bytes, each message has a header, and inside the record, there are three contents:

1. MAC-DATA: Message Authentication Code.
2. Actual-Data: The data currently sent.
3. Padding-Data: Padding-Data, to ensure that the data is made of a set of blocks and expires after the MAC is calculated.

The second protocol is called the handshake protocol. This protocol is located at the top of the SSL Record Protocol. It manages how messages between the client and the server are switched and forwarded when they initiate an SSL connection. These exchanges are designed to facilitate the following actions:

1. Server authentication for the client.
2. Client authentication of the server.

3. It allows the client and server to choose encryption algorithms and encrypted messages (cipher).
4. Using encryption techniques (Public Key) to create joint security.

3.7 The Security Elements of SSL Protocol

1. The SSL allows the user to authenticate the identity of the server. That means, the SSL enables the client to use standard technologies such as the Public Key Encryption method. The goal of that is to make sure that the server's certificate is authentic and that it is issued by a trusted source.

This authentication is very important especially when the user wants to send sensitive information such as credit card numbers on the network. In addition, when the user wants to make sure that the receiving server is the same as the intended server (verification of identity).

2. The SSL allows the server to authenticate and verify the identity of the user using the same technologies. That is, the client's certificate is valid and legitimate and is available from the server’s list of certificates.

These operations are very important, for example, if a bank sends private financial information to a customer and wants to verify the identity of the recipient of that information.

3. The SSL requiring all information sent between the client and the server to be encrypted. This process is to ensures that there is a high degree of confidentiality. Confidentiality is very important for both the client and server at any operation or special connection. In addition, all data sent encrypted by SSL is protected using special tools of detection technology.
4. The SSL protocol supports the use of different types of encryption algorithms. That is to enable applying it in various operations such as authenticating the server and client with each other. In addition, it can be used in the trade of certificates and session keys.

Client and server can support different combinations of encryption types depending on some factors. these factors are the SSL version and regulatory policies regarding permissible encryption strength. For example, the 128-bit key strength is not permitted outside the US.

The other example is The Handshake protocol. This protocol is defined as the process of authentication of the client and server with each other. It uses tools of encrypted messages, sends certificates, and establishing a session key.

The SSL supports the following encryption algorithms:

- Data Encryption Standard (DES): An encryption algorithm used by the US government.
- Digital Signature Algorithm (DSA): The electronic signature algorithm is part of the electronic authentication standard used by the US government.
- Key Exchange Algorithm (KEA): developed by Rivets.
- Message Digest Algorithm (MD5): An encryption algorithm used by the US government.
- RC2 & RC4: Symmetric encryption algorithm used by the US government.
- Public Key Algorithm (RSA): The public key algorithm for both encryption and authentication was developed by Rivest, Shamir, and Adleman.
- RSA Key Exchange: A key exchange algorithm for SSL charting based on RSA algorithm.
- Secure Hash Algorithm (SH-1): An encryption algorithm used by the US government.
- SKIPJACK: Conventional Symmetric Key algorithm used by the US government.
- TRIPLE DES: a practical implementation of DES (Three Times).

3.8 The Symmetric and Public Encryption Process Using SSL Protocol

The SSL protocol uses a set or a combination of symmetric and public encryption algorithms. The traditional Symmetric algorithms are much faster than the public key algorithms. However, the public key algorithms work with better authentication techniques,(Zhenzhong and Yao, 2011).

An SSL session begins with an exchange of messages and is called a handshake. The public key technologies for the client allow the client and server to collaborate in establishing a session by symmetric key to use for fast encryption. The programing

details of the messages exchanged during the Handshake process are as follows steps:

1. Assuming we have implemented the RSA Exchange algorithm. The client sends to the server the cipher encrypted settings, randomly generated data, and other information the server needs to contact the client via SSL.

Then, the client sends their own testimony, in the case of a request for resources from the server, and then the client's authentication is required. Cipher encrypted settings

2. The server sends to the client the cipher encryption settings, randomly generated data, and other information the client needs to connect to the server via SSL, In addition, the server sends its own certificate, if the client needs server authentication.
3. The client needs some information sent from the server to authenticate the server. If the server is not authenticated, the client is warned of this problem and knows that the session cannot be established in this case. If the authentication is successful, we go to the next step.
4. Using all the data that was generated in the handshake so far, the client (using the current encryption method) creates a key called (Premaster Secret) for the session. This key is encrypted by the server's public key, which is obtained from the server certificate acquired from Step 2.
5. If the server requests authentication of the client (which is an optional step), the client will authenticate and send another piece of data that is unique and identifiable to both the server and the client, along with his certificate.
6. If the server requests client authentication, the server tries in this case to verify the client. If the client cannot authenticate, the session is terminated. If the client is able to authenticate, the server uses its own key to decode the premaster secret. Then begins the same steps that the client did, and the master secret is generated.
7. Both the client and the server use the master key to generate the session key. The session key always (Symmetric Key Algorithm) and is used to encrypt and decrypt the information exchanged in the SSL session. In addition, it is

used to verify the integrity of the information and detect any changes in the data between transmission time and receiving time.

8. The client sends a message to the server indicating that the messages sent by the client are encrypted with the session key. Then, it sends a separate message indicating that the handshake has ended.
9. The server sends a message to the client informing it that the future messages will be encrypted with the session key. It also sends a separate message indicating that the handshake has ended.
10. The SSL Handshake is now complete and the SSL session has started. The client and server are using session keys for Encrypt and Decrypt for exchanged data.

3.9 The other Requirements of Applying the SSL Protocol

It is important to indicate that applying the SSL protocol needs some requirements. First, the certificates of both the client and the server have to encrypt some pieces of data using the public key. The private key can only decode the codes, (Oppliger, Hauser and Basin, 2006).

Second, in the case of server authentication, the client encrypts the premaster secret with the server's public key. The private key of the server can correctly decode the code.

Therefore, the client can securely be linked to the public key that belongs to the server with its private key. In addition, the premaster secret cannot be decrypted. The keys required for the session can be generated and in this case, the session ends.

Finally, in the case of client authentication, the client encrypts some random data with the customer’s private key. Thus creating an electronic signature (Digital Signature) and the public key in the client’s certificate that is present at the server. If the server cannot authenticate the electronic signature, the session is expired.

3.10 The Electronic Certificate of the SSL Protocol

Authentication in SSL is done through the use of electronic certificates. These certificates are (x.509) files and applications for electronic signatures. The certificate

is signed with the private key of the certificate authority. Therefore, the certification authority must verify the identity of the person requesting the certificate.

Doing that can prevent anyone from forge the certificate. That is because it bears the electronic signature of the certificate server. For this, we need a certificate from the certification authority in order to ensure the electronic signature of the certification authority with the public key found in the certification process.

In general, the electronic certificates have the fooling information:

- Version
- Serial number
- Signature algorithm ID
- Issuer name
- Validity period
- Subject user name
- Subject public key information
- Issuer unique ID

3.10.1 Types of the electronic certificates

There are three types of electronic certificates:

1. The client certificate (personal): This certificate is used to authenticate the client with the serve
2. The server certificate: This certificate is used by the internet server to authenticate itself to the client.
3. The certificate authority certificate: This certificate is for the certification server that gives its holder the right to issue certificates.

3.10.2 The authentication of the client certificate

The SSL protocol can control access to an internet server or any virtual directory that includes SSL. This control of access can be done by requesting a client certificate.

Client certificate authentication occurs when the client tries to log in to a server that supports SSL. Then, the server requests a certificate (X.509) from the client in order identity the client's to be authenticated. After the client has been successfully authenticated, site resources are granted to the client.

3.11 Create SSL Session

To create a SSL session, the protocol must be able to process certificates on both the client and server and this includes processing requests and appropriate responses. In addition, the client must be able to verify the certificate. The server requests the certificate and the user be allowed to submit the certificate on demand. This requires the client to store and manage the certificate. Finally, the server must be able to request a certificate to verify client certificates, [62].

An SSL session that encrypts all data between the client and the server is created using the following steps that shown in figure (3.3):

1. The internet browser establishes a secure connection to the webserver.
2. The internet server sends the browser a copy of its certificate. The certificate enables the browser to confirm the identity of the server and the integrity of the web content.
3. The web browser and the server are engaged in a negotiating exchange to determine the degree of encryption to use to secure communications. Typically, 40 Bit or 128 Bit encryption is stronger. However, 128 Bit is currently permitted only in the US and Canada due to US government export restrictions.

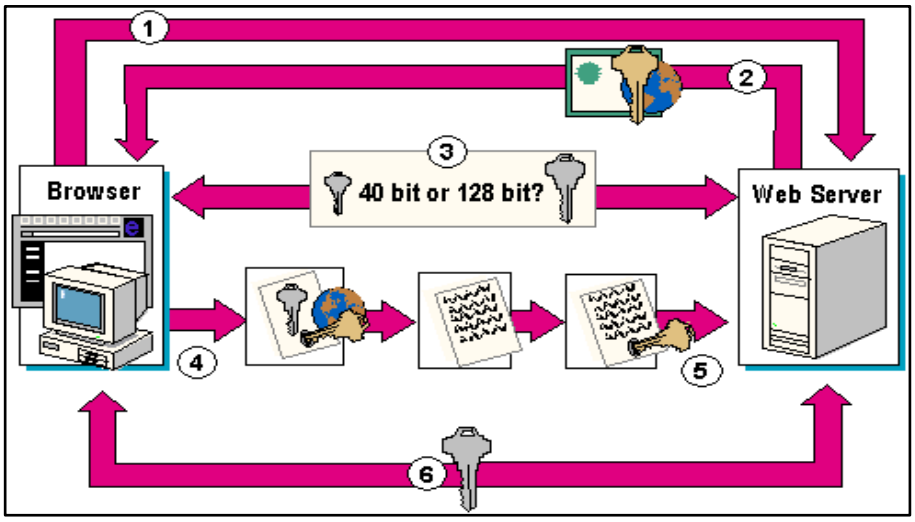

Figure 3.3: The Steps For an SSL Protocol Session.

Source: Oppliger, et al, (2006).

4. The internet browser generates the session key and encrypts it with the public server key. Then, the webserver sends it. Using its own private key, the server

decrypts the session key and establishes a secure channel. The internet server and browser use the session key to encrypt and decrypt the data exchanged.

It is important to indicate that before implementing the SSL protocol, the appropriate certificates and keys must be ready. When applying SSL to add security features to the site, an electronic certificate must be obtained.

In addition, the system must be registered with an external certificate authority that extracts the certificates. In some cases like “Microsoft Certificate Server”, it removes the need to extract certificates from a third party. It also gives the user complete control over the certificates, which is a component of the Internet Information Server.

To obtain an electronic certificate from an external certification authority, use the key manager to generate a pair of keys for the system. Then email the certificate request file to the certification authority. The certification authority will respond by sending the electronic certificate.

4. THE EMPIRICAL WORK (APPLYING THE E-COMMERCE SECURITY TOOLS ON ELRYAN WEBSITE)

This chapter is the empirical work of the study. In this chapter, the work will be on one of the E-commerce websites, which is (The Elryan online shopping market). This website was selected because it is one of the Iraqi online shopping markets. The problem is that the online transactions (specifically, online payments) in Iraq still not secure from both sides (online markets and banks). That can cause many problems to customers' accounts.

The site has a plan to start an online payment feature with two private banks. Even the site was designed to do an online payment, some of the sites' managers complained about security issues regarding customers' accounts. Therefore, they decided that this website must have some e-commerce security checks to fix any possible security weaknesses.

In general, the empirical work of this chapter has four steps:

1. A general review of the site operation system and components. The goal of this step understand how the site work and what security features it has.
2. A security check is applied on the Elryan online shopping market website. The E-commerce security criteria will be applied on this website. The goal of this step is to identify any possible security weakness.
3. After identifying any security weaknesses, E-commerce security tools will be applied to fix these problems.
4. Tests will be applied to ensure that the security tools are working and the website security weaknesses are removed.

4.1 Step One (The General Review)

Before starting the security check, it is important to look over some details of the site. That includes general description, the site's system, and others. Doing that can help better understand how it works and what are its security features.

4.1.1 The description of the site

The Elryan shopping website is a commercial website on the internet that sell different types of household goods. Its address is (https://www.elryan.com/ar/). The main page of the site displays the different household products that grouped based on their use. For example, electronics group, furniture group, and kitchen group.

There are four groups of people working and using this site. The first group is the administration group. This group is the supervising authority who are responsible for designing and managing the website. People in this group deal with all customers who are entering the site and respond to their questions.

In addition, they manage the subscribers (such as adding or deleting a subscriber). They also contact the providers to obtain new products. They process customer orders and payments. It is important to indicate here that payments method is cash until now. That is, the many is given the delivery person who is usually one of the site employees. Finally, they manage the site's updates such as deleting, or adding or updating products, advertising, and others.

The second group is the providers. They are the people, factories, companies, and wholesale stores that provide the products to the site. The site's management deals with suppliers by either purchasing products or obtaining them with their participation.

The third group is the subscribers. They are a group of users who have subscribed to the site by filling out the subscription form and have paid the subscription fees. Those individuals usually get discounts on purchasing, fast deliveries, and special offers. The subscribers pay fees by depositing manually (cash or check) the specified amount to the site's bank account. When the payments are received, they will be able to enjoy all site advantages that giving to them.

The fourth group is the guests or reviewers. They are all regular browsers of the site, and they are entitled to correspond with the administration of the site. They can buy products as guests but they do not receive any discounts or special offers.

They can also fill out the site's subscription form and pay the specified fees to become official subscribers.

4.1.2 The site properties

The site is designed based on the SSL protocol and has the following general properties:

1. The site is far away from the design complexities of popular e-commerce sites. It is easy and simple to buy and sell.
2. The number of pages, links, images that slow loading objects are low. That can make the site's navigation very easy.
3. The site has good and fast contact between management, suppliers, subscribers, and users.

4.1.3 The site components

The site has two types of components, which are the operational and the security components. The operational components are:

- SSL server device that placed in a safe place.
- Windows NT or later.
- Internet Information Server (IIS).
- Microsoft Certificate Server.
- Microsoft Key Manager.

The security components of the site are:

- The site's server can issue certificates to authenticate clients.
- The site's server can create (public and private) key pairs.
- The site uses the HTTPS protocol instead of the HTTP protocol to secure the web directory.
- The site can create a subscriber certificate that will be asked about when entering the site.

4.1.4 The site's system features

The site's system has several features, which are:

- The system divides the visitors into two groups (subscribers and users), and each group of them has different advantages.

- The system identities the subscribers by the subscriber's user name and password that is sent via mail.
- The system has the online payments feature with both groups of product providers and customers. However, this feature is not active because managers are scared about security issues related to other parties' bank accounts.
- The system allows only the authorized administration managers to do all operations that take place on the site. For example, they do the operations of buying products from suppliers; sell products to customers, accepting subscription requests, responding to visitors' questions, and other activities.

4.2 Step Two (Security Check)

In this step, a security check is applied on the Elryan online shopping market website. The E-commerce security criteria will be applied on this website. The goal of this step is to identify any possible security weakness. This section has two types of security checks. The first type is related to check basic internet security. The second type is checking the SSL security elements.

The check is done by creating three user accounts on the site. One account is a subscription account, one account is a provider account, and the other is a user (guests) account. The bank accounts information of all three was entered on the site. The online payments were done from the three accounts to three different banks. Then, the check started as explained in the below sections.

4.2.1 Checking the basic internet security

There are some basic internet security concepts that are important to check when sharing information on websites.

These concepts were discussed in chapter two of this study on pages (3-4). The below checks were applied on the site:

1 -The confidentiality check

The information shared online is said to be confidential when no one can copy or use them without authorization. When the information is read or copied by someone who is not authorized, this is known as (loss of confidentiality). Some types of

information especially the banks' accounts information have very important and private confidentiality while others not.

The check of confidentiality shows that not only the authorized site's managers can see the banks' accounts information of the customers. The authorized site's managers are the managers who are responsible for processing the online payments. This issue can be a security problem that has to be fixed.

2 -The integrity check

The information is said to have integrity when no one can modify them without authorization. If the information can be easily modified, this process is known as (loss of integrity).

That includes both unauthorized modifications, human error, and deliberate tampering. All of these cases make the information lose its integrity, especially when dealing with critical information such as financial data, electronic fund transactions, and military data.

The check of integrity shows that only the authorized site's managers can modify the critical information through several steps that ensure the security of this information. Therefore, the site has no security problem related to integrity.

3 -The data availability check

The availability is the ability to access the information. If the information can be easy to access, that resulting in (loss of data availability).

Availability of information is often the most important characteristic of a business that relies on information. For example, airline schedules, online reservations, and inventory systems. When the user tries to access or edit the information, the accessing request will be denied.

The check of availability shows that only the authorized site's managers can access and modify the information through several steps that ensure the security of this information.

For example, if a customer pays online for a product, and later decides to cancel, he/she cannot do that directly. However, the customer has to request a cancelation of the order, and then an authorized manager can process it and send the money back. Therefore, the site has no security problem related to availability.

4- The authentication check

It is the process of identifying the individuals. This process can be done by using certain procedures such as requesting names, addresses, phone numbers, PINs, and passwords. In some cases, the authentication can be done using vital criteria, such as a signature, or physical tools such as a fingerprint.

The check of authentication shows that the site required the users to enter names, addresses, phone numbers, and passwords when making online payments.

However, when the user enters the information incorrectly, there is no limit to retrying. That is, the user can enter the password as many times as he wants. This is considered a security problem because attackers can use this security weakness to access the user's information. Therefore, the site has a security problem related to authentication.

4.2.2 Checking the SSL security elements

As mentioned before, the Elryan site is using the SSL protocol. Therefore, the SSL protocol security elements must be checked when sharing information online. These concepts were discussed in chapter three of this study on pages (16-19). The below checks were applied on the site:

1- Checking the confidentiality of information exchanged between two parties:

The two parties who make online transactions can be the site managers and the providers, or the site managers and the customers. The exchanged information could be an e-mail, a message, a financial transaction, or anything else.

The check on the confidentiality of information exchanged between two parties shows that the site has no security problems related to this issue. That is any exchanged information stays safe, and only authorized individuals can access them.

2- Checking for the public key encryption:

The SSL allows the user to authenticate the identity of the server. That means, the SSL enables the client to use the Public Key Encryption method. The goal of that is to make sure that the server's certificate is authentic and that it is issued by a trusted source.

This authentication is very important especially when the user wants to send sensitive information such as credit card numbers on the network. In addition, when the user wants to make sure that the receiving server is the same as the intended server (verification of identity).

The check for the public key encryption shows that the site is using this security feature, and there is no security problem related to this issue.

3- Checking for the client's certificate:

The SSL allows the server to authenticate and verify the identity of the user. That is, the client's certificate is valid and legitimate and is available from the server's list of certificates.

The check shows that the site is able to verify the identity of the user. That is, the site can verify that the client's certificate is valid and legitimate. Therefore, there is no security problem related to this issue.

4- Checking the acceptance of different types of encryption algorithms.

The SSL protocol supports the use of different types of encryption algorithms. That is to enable applying it in various operations such as authenticating the server and client with each other.

Unfortunately, even The SSL protocol supports the use of different types of encryption algorithms, the check shows that some providers and banks use encryption algorithms that are not supported by the SSL. This can be a security problem.

4.3 Step Three (Fixing the Security Problems)

The security problems identified in step two are:

- The confidentiality problem: Not only the authorized site's managers can see the banks' accounts information of the customers.
- The authentication problem: The user can enter information such as an incorrect password as many times as he wants. This is considered a security problem because attackers can use this security weakness to access the user's information.

- The encryption algorithms agreement: Some providers and banks use encryption algorithms that are not supported by the SSL.

After identifying these security weaknesses, they will be fixed as follows:

1- The confidentiality problem is solved by changing the authorized system of the site. That is, not all authorized site managers can see the banks' accounts information of the customers. However, one change enables **some** of the top-level authorized site managers to see **some** of the banks' accounts information of the customers. For example, they can see only the bank name and the last four digits of the bank account.

2- The authentication problem is solved by preventing the users from entering information such as incorrect passwords many times. They can now enter it three times, then any other attempt will be denied, and an alert message will be sent to the account owner. The message informs the account owner that someone tries to use his account, so he has to contact the site managers to verify this action.

3- The encryption algorithms agreement problem was not solved, but there were two suggested solutions. The first solution is to update the site so it can accept most of the encryption algorithms. This solution looks good, but it is expensive.

The second solution is to deal only with the parties that use encryption algorithms supported by SSL. This solution is not costly, but it is not good for customers and providers. For example, a customer has to open a bank account with a specific bank to be able to deal with the site. In short, this solution can create a business limitation problem.

4.4 Step For (The Test)

Tests were applied to ensure that the security tools are working and the website security weaknesses are removed.

Two of the top-level authorized site managers were asked to look at the banks' accounts information of a customer. They could see only the bank name, bank owner name, address, and last four digits of the bank account.

Two non-authorized site managers were asked to look at the banks' accounts information of a customer. They could not see any information about the customer's bank account.

Four different users were asked to enter incorrect passwords many times. They could enter it three times, then any other attempt was denied, and an alert message was sent to their phones and e-mails. The messages informed them that someone tries to use their account, so they have to contact the site managers to verify their actions.

Figure (4.1) shows the whole process of checking and fixing the site's security problems. In addition, the programming code for fixing the security problems is shown in appendix A.

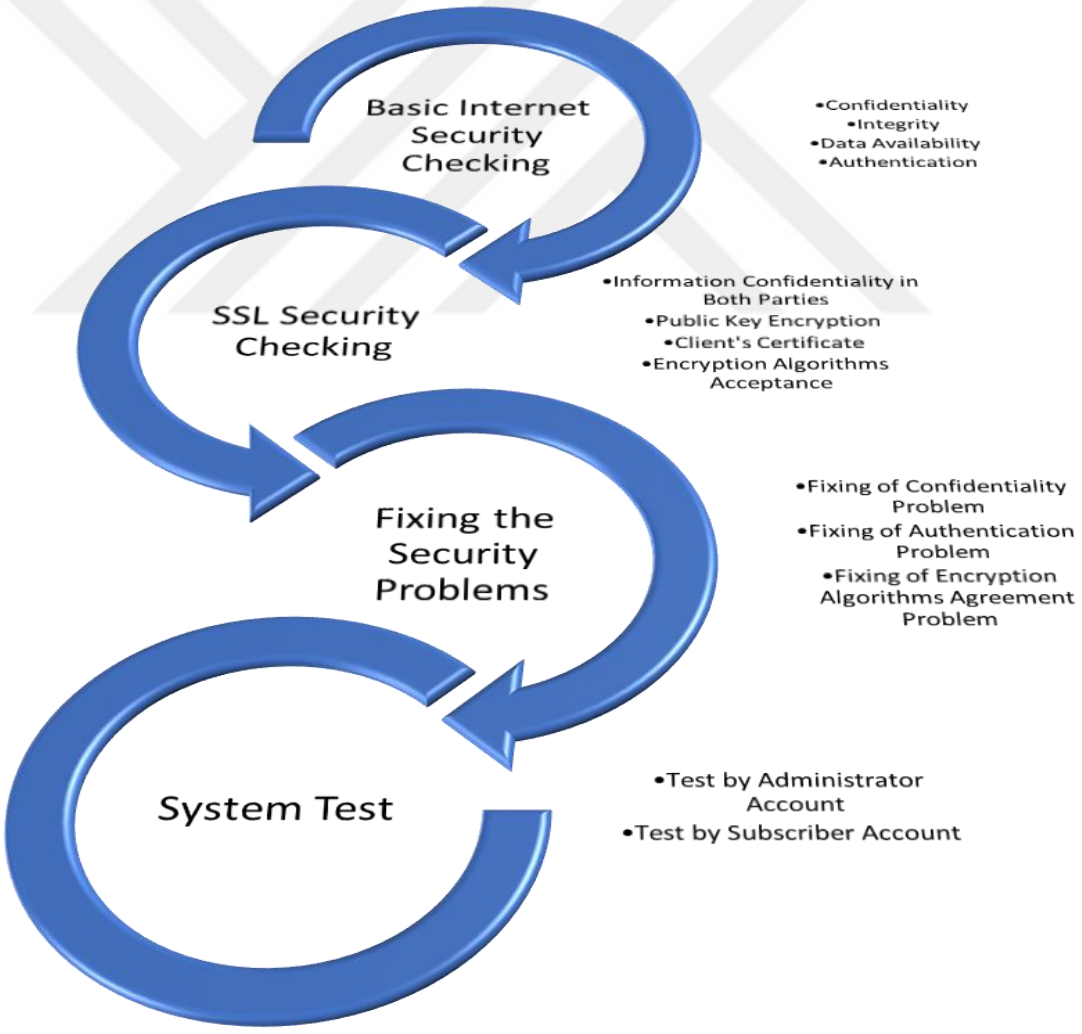

Figure 4.1: The Whole Process of Checking and Fixing The Site's Security Problems

5. CONCLUSION AND RECOMMENDATIONS

This research is an early study in the field of information security of e-commerce. Many security issues need to be further studied and seriously discussed. What this study has discussed and analyzed are the issues of information security.

The cornerstone of the security system depends on the designs of the security network protocols. Therefore, the more powerful these protocols were designed, the more difficult their applications are to penetrate. Many generations of protocols have emerged as a response to the weaknesses of their predecessors.

Recent web languages and script languages have internal security features that can provide security and protection for programs and applications such as e-commerce sites. The ongoing improvement in tracking applications and monitoring online activities can help to avoid or minimize the risks caused by security weakness.

It is important for software engineering to take into account the security issues when designing systems. That can help to improve the security of the networks that are sensitive to penetrations.

This study was applied to one of the Iraqi E-commerce websites. The website is (The Elryan online shopping market). This website was selected because the online transactions (specifically, online payments) in Iraq still not secure from both sides (online markets and banks). That can cause many problems to customers' accounts.

In addition, the site has a plan to start an online payment feature with two private banks. However, some of the site managers complained about security issues regarding customers' accounts. Therefore, they decided that this website must have some e-commerce security checks to fix any possible security weaknesses.

Four steps were done to check the site for any possible security problem and to fix this problem if found. The first step was reviewing the site operation system and components.

The second step was the security check to identify any possible security weakness. The third step was applying security tools to fix the security problems. The final step

was testing the system to ensure that the security tools are working and the website security weaknesses are removed.

Three security problems were found on the site. The first problem was the confidentiality problem. The problem was that not only the authorized site's managers could see the banks' accounts information of the customers. The second problem was the authentication problem. User can enter the information such as incorrect password as many times as he/she wants. The third problem was the encryption algorithms agreement. It means that some providers and banks use encryption algorithms that are not supported by the SSL, which is used in the site system.

The first two security problems were fixed, and the site was tested. The results showed that the security weaknesses were removed and the site is secure for online transactions.

The encryption algorithms agreement problem was not solved directly, but there were two suggested solutions. The first solution is to update the site so it can accept most of the encryption algorithms. The second solution is to deal only with the parties that use encryption algorithms supported by SSL. Therefore, the site's managers can select one of these solutions, and then the problem will be solved.

REFERENCES

Al-Haidari, F., Gutub, A., Al-Kahsah, K. and Hamodi, J., (2009). May. Improving security and capacity for arabic text steganography using 'Kashida'extensions. In 2009 IEEE/ACS International Conference on Computer Systems and Applications (pp. 396-399). IEEE.

Anderson, R.D.,(2014). Viruses, Trojans, and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz. Tort Trial & Insurance Practice Law Journal, pp.529-610.

Anderson, S.W. and Lanen, W.N.,(2002). Using electronic data interchange (EDI) to improve the efficiency of accounting transactions. The Accounting Review, 77(4), pp.703-729.

Arcari, R., Lewis, J. and Donnald, E., (2004). The Electronic Fund Transfer System (EFTS). Journal of the Medical Library Association, 92(4), p.493.

Atkins, D., Buis, P., Hare, C., Kelly, R., Nachenberg, C., Nelson, A.B., Phillips, P., Ritchey, T. and Stean, W., (1997). Internet security. New Riders,, pp.173-232.

Bajaj, K.K., Nag, D. and Bajaj, K.K., (2005). E-commerce. Tata McGraw-Hill Education.

Barr, R. E. (1991). Are EDI and EFT in Your Tax Filing Future?. Journal of Systems Management, 42(4), 32.

Bellovin, S.M., (1998) August. Cryptography and the Internet. In Annual International Cryptology Conference (pp. 46-55). Springer, Berlin, Heidelberg.

Benjamin, R.I., David, W. and Morton, M.S.S., (1990). Electronic data interchange: how much competitive advantage?. Long range planning, 23(1), pp.29-40.

Bingi, P., Mir, A. and Khamalah, J., (2006). The challenges facing global e-commerce. Information Systems Management.

Bisel, L.D., (2007). The role of SSL in cybersecurity. IT Professional, 9(2), pp.22-25.

Borella, M., Grabelsky, D., Lo, J. and Taniguchi, K., (2001). Realm specific IP: protocol specification. Oct. 2001. RFC 3103.

Boss, A.H.,(2000). The Uniform Electronic Transactions Act in a Global Environment. Idaho L. Rev., 37, p.275.

Brandel, R.E. and Geary, A., (1981). Electronic Fund Transfers. The Business Lawyer, pp.1219-1236.

Chakrabarti, A. and Manimaran, G., (2002). Internet infrastructure security: A taxonomy. IEEE network, 16(6), pp.13-21.

Choi, S. Y., Stahl, D. O., & Whinston, A. B. (1997). The econo[mics of electronic][[[commerce (pp. 12-25). Indianapolis, IN: Macmillan Technical Publishing.

Crook, C.W. and Kumar, R.L., (1998). Electronic data interchange: a multi-industry investigation using grounded theory. Information & Management, 34(2), pp.75-89.

Ding, W., Yan, Z. and Deng, R.H., (2016). A survey on future Internet security architectures. IEEE Access, 4, pp.4374-4393.

El Ismaili, H., Houmani, H. and Madroumi, H., 2014. A secure electronic transaction payment protocol design and implementation. IJACSA) International Journal of Advanced Computer Science and Applications, 5(5), pp.172-180.

Freier, A., Karlton, P. and Kocher, P.,(2011). The secure sockets layer (SSL) protocol version 3.0 (Vol. 11). RFC 6101.

Goyal, S., (2012). A Survey on the Applications of Cryptography. International Journal of Science and Technology, 1(3).

Grossman, J., (2012). The state of website security. IEEE Security & Privacy, 10(4), pp.91-93.

Gunasekaran, A., Marri, H. B., McGaughey, R. E., & Nebhwani, M. D. (2002). E-commerce and its impact on operations management. International journal of production economics, 75(1-2), 185-197.

Gupta, H. and Sharma, V.K., (2011). Role of multiple encryption in secure electronic transaction. International Journal of Network Security & Its Applications, 3(6), p.89.

Hare, C., 2011. Simple Network Management Protocol (SNMP).

Hawkins, S., Yen, D.C. and Chou, D.C., (2000). Awareness and challenges of Internet security. Information Management & Computer Security.

Hickman, K. and Elgamal, T., (1995). The SSL protocol

Householder, A., Houle, K. and Dougherty, C., (2002). Computer attack trends challenge Internet security. Computer, 35(4), pp.sulp5-sulp7

Howard, J.D.,(1997). An analysis of security incidents on the internet 1989-1995. Carnegie-Mellon Univ Pittsburgh PA.

Huan, T., (2013). The Application of SSL Protocol in Computer Network Communication. In Intelligence Computation and Evolutionary Computation (pp. 779-783). Springer, Berlin, Heidelberg.

Jestratjew, A. and Kwiecien, A., 2012. Performance of HTTP protocol in networked control systems. IEEE Transactions on Industrial Informatics, 9(1), pp.271-276.

Kaufman, L.M., (2009). Data security in the world of cloud computing. IEEE Security & Privacy, 7(4), pp.61-64.

Kessler, G.C., (2004). An overview of TCP/IP protocols and the internet. InterNIC Document, Dec, 29, p.42.

Khan, B., Alghathbar, K.S., Khan, M.K., AlKelabi, A.M. and AlAjaji, A., (2010). Using arabic CAPTCHA for cyber security. In Security Technology, Disaster Recovery and Business Continuity (pp. 8-17). Springer, Berlin, Heidelberg.

Khare, R., (1998). TELNET: the mother of all (application) protocols. IEEE Internet Computing, 2(3), pp.88-91.

Kim, D., & Solomon, M. G. (2013). Fundamentals of information systems security. Jones & Bartlett Publishers.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision support systems, 44(2), 544-564.

Kravets, O., (2013). Mathematical modeling of parameterized TCP protocol. Automation & Remote Control, 74(7).

Lee, G., (2015). A Study on Improving Security Controls in the Electronic Financial Transaction. Journal of the Korea Institute of Information Security & Cryptology, 25(4), pp.881-888.

Lee, M. and Lee, J., (2012). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. Information Systems Frontiers, 14(2), pp.375-393.

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G. and Wolff, S., (2009). A brief history of the Internet. ACM SIGCOMM Computer Communication Review, 39(5), pp.22-31.

McCrohan, K. F. (2003). Facing the threats to electronic commerce. Journal of Business & Industrial Marketing.

Mthembu, M.A., (2010). Electronic Funds Transfer: Exploring the Difficulties of Security. J. Int'l Com. L. & Tech., 5, p.201.

Nemat, R.,(2011). Taking a look at different types of e-commerce. World Applied Programming, 1(2), pp.100-104.

Oppliger, R., Hauser, R. and Basin, D., (2006). SSL/TLS session-aware user authentication–Or how to effectively thwart the man-in-the-middle. Computer Communications, 29(12), pp.2238-2246.

Panurach, P., (1996). Money in electronic commerce: Digital cash, electronic fund transfer, and ecash. Communications of the ACM, 39(6), pp.45-50.

Partridge, C. and Pink, S., (1993). A faster UDP (user datagram protocol). IEEE/ACM Transactions on Networking, 1(4), pp.429-440.

Pawlowski, B., Noveck, D., Robinson, D. and Thurlow, R., (2000). The NFS version 4 protocol. In In Proceedings of the 2nd International System Administration and Networking Conference (SANE 2000.

Piper, F., (1996). April. Basic principles of cryptography. In IEE Colloquium on Public Uses of Cryptography (pp. 2-1). IET.

Riabov, V.V., (2005). Smtp (simple mail transfer protocol). River College.

Shankar, K., Lakshmanaprabu, S.K., Gupta, D., Khanna, A. and de Albuquerque, V.H.C., (2020). Adaptive optimal multi key based encryption for digital image security. Concurrency and Computation: Practice and Experience, 32(4), p.e5122.

Shiquan, H., 2008. FTP Protocol Analysis and Security Research [J]. Microcomputer Information, 6.

Strader, T.J. and Shaw, M.J., (1997). Characteristics of electronic markets. Decision Support Systems, 21(3), pp.185-198.

Vlasov, A. V. (2017). The evolution of E-money.

Vysotska, V., Rishnyak, I. and Chyryn, L., (2007). February. Analysis and evaluation of risks in electronic commerce. In 2007 9th International Conference-The Experience of Designing and Applications of CAD Systems in Microelectronics (pp. 332-333). IEEE.

Thekkath, C.A., Nguyen, T.D., Moy, E. and Lazowska, E.D., (1993). Implementing network protocols at user level. IEEE/ACM Transactions on Networking, 1(5), pp.554-565.

Wang, E.T. and Seidmann, A., (1995). Electronic data interchange: Competitive externalities and strategic implementation policies. Management Science, 41(3), pp.401-418.

Waters, B., (2009, August). Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In Annual International Cryptology Conference (pp. 619-636). Springer, Berlin, Heidelberg.

Wigand, R. T. (1997). Electronic commerce: Definition, theory, and context. The information society, 13(1), 1-16.

Yu, H.C., Hsi, K.H. and Kuo, P.J., (2002). Electronic payment systems: an analysis and comparison of types. Technology in Society, 24(3), pp.331-347.

Zhenzhong, W. and Yao, W., (2011, August). An improvement SSL protocol application research. In Proceedings of 2011 International Conference on Electronic & Mechanical Engineering and Information Technology (Vol. 8, pp. 4010-4013). IEEE.

Zimmermann, P.R., (1998). Cryptography for the Internet. Scientific American, 279(4), pp.110-115.

APPENDICES

Appendix A: Programing Code

The programming code of fixing the site's security problems

Appendix A

```
protected void Button1_Click(object sender, EventArgs e)
   {
      string username = TextBox1.Text;
      string password = TextBox2.Text;
      string connection =
ConfigurationManager.ConnectionStrings["ElryanConnectionString"].ConnectionStr
ing;

      SqlConnection conn = new SqlConnection(connection);
      conn.Open();
      string querycommand = "select ID, Genre from Customers where ID=@ID";
      SqlCommand cmd = new SqlCommand(querycommand, conn);
      cmd.Parameters.AddWithValue("@ID", username);
      SqlDataAdapter sda = new SqlDataAdapter(cmd);
      cmd.ExecuteNonQuery();
      DataTable dt = new DataTable();
      sda.Fill(dt);
      if(counter>=4)
      {
```

```
        Page.ClientScript.RegisterStartupScript(this.GetType(), "CallMyFunction",
"alert('You are Tried More Than Three Times');", true);
      }
      else if (dt.Rows.Count > 0)
      {
        string datausername = dt.Rows[0][0].ToString();
        string datapassword = dt.Rows[0][1].ToString();
        if (datausername == username && datapassword == password)
        {
                                    counter=0;
          Response.Redirect("cardpanel.aspx");
        }
        else
        {
          Page.ClientScript.RegisterStartupScript(this.GetType(),
"CallMyFunction", "alert('Invalid Login');", true);
        }
      }
      else
      {
        counter++;
                          Page.ClientScript.RegisterStartupScript(this.GetType(),
"CallMyFunction", "alert('Username or Password is Invalid');", true);
      }
    }
```

RESUME

EDUCATION:

1. High School: 1987 graduated from Al-Rumady High School.

2. Bachelor: 2013 graduated from the University Of AL-Maaref Univrsity College, Engineering Department, Computer Engineering Technology

PROFESSIONAL EXPERIENCE AND REWARDS:

Preidency Of Dewan Al-Waqf AL-Saony Iraq.

Worked as Computer Engineer