إقرار

أنا الموقع أدناه مقدم الرسالة التي تحمل العنوان:

E-Payment model with Gateway and QR code
نموذج دفع إلكتروني باستخدام بوابة وكود QR

أقر بأن ما اشتملت عليه هذه الرسالة إنما هي نتاج جهدي الخاص، باستثناء ما تمت الإشارة إليه حيثما ورد، وإن هذه الرسالة ككل، أو أي جزء منها لم يقدم من قبل لنيل درجة أو لقب علمي أو بحثي لدى أية مؤسسة تعليمية أو بحثية أخرى.

DECLARATION

The work provided in this thesis, unless otherwise referenced, is the researcher's own work, and has not been submitted elsewhere for any other degree or qualification

اسم الطالب: أسماء عدنان محمد قاعود Student's name:

التوقيع: Signature

التاريخ: 6/5/2015 Date:

Islamic University – Gaza
Deanery of Higher Studies
Faculty of Engineering
Computer Engineering Department

E-payment model with Gateway and QR code

Asmaa Adnan Gaoud

Supervisor

Dr. Aiman Abu Samra

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Computer Engineering

2015 _ 1436

بسم الله الرحمن الرحيم

الجامعة الإسلامية – غزة
The Islamic University - Gaza

مكتب نائب الرئيس للبحث العلمي والدراسات العليا هاتف داخلي 1150

الرقم Ref ج س غ/35/
التاريخ Date 2015/03/30

نتيجة الحكم على أطروحة ماجستير

بناءً على موافقة شئون البحث العلمي والدراسات العليا بالجامعة الإسلامية بغزة على تشكيل لجنة الحكم على أطروحة الباحثة/ **أسماء عدنان محمد قاعود** لنيل درجة الماجستير في **كلية *الهندسة*** **قسم هندسة الحاسوب** وموضوعها:

E-Payment model with Gateway and QR code
نموذج دفع إلكتروني باستخدام بوابة وكود QR

وبعد المناقشة التي تمت اليوم الاثنين 10 جمادى الآخر 1436هـ، الموافق 2015/03/30م الساعة الثانية مساءً، اجتمعت لجنة الحكم على الأطروحة والمكونة من:

د. أيمن أبو سمرة	مشرفاً ورئيساً	.....
أ.د. محمد مكي	مناقشاً داخلياً	.....
د. رشدي الحمامرة	مناقشًا خارجيًا	.....

وبعد المداولة أوصت اللجنة بمنح الباحثة درجة الماجستير في **كلية *الهندسة*/ قسم هندسة الحاسوب.**

واللجنة إذ تمنحها هذه الدرجة فإنها توصيها بتقوى الله ولزوم طاعته وأن تسخر علمها في خدمة دينها ووطنها.

والله ولي التوفيق،،،

مساعد نائب الرئيس للبحث العلمي و للدراسات العليا

أ.د. فؤاد علي العاجز

P.O. Box 108, Rimal, Gaza, Palestine fax: +970 (8) 286 0800 فاكس Tel: +970 (8) 286 0700 هاتف ص.ب. 108 الرمال، غزة، فلسطين
public@iugaza.edu.ps www.iugaza.edu.ps

Acknowledgements

First and above all, I praise God, the almighty for providing me this opportunity and granting me the capability to proceed successfully.

This thesis appears in its current form due to the assistance and guidance of several people. I would therefore like to offer my sincere thanks to all of them.

I would like to express my deepest gratitude to my advisor, Dr. Aiman Abu Samra, for his excellent guidance, caring, patience, and providing me with an excellent atmosphere for doing research.

I also extend my thanks to prof. Mohammad Mikki and Dr. Rushdi Hamamreh the members of thesis discussion committee.

I warmly thank and appreciate my mother and father-a lot of thanks to them their material and spiritual support in all aspects of my life.

I also would like to thank my brother, sisters, for they have provided assistance in numerous ways.

I want to express my gratitude and deepest appreciation to my lovely sweet children my son "Adnan", and daughter "Menna" , for there great patience and understandings.

Finally, I would like to thank my husband. he was always there cheering me up and stood by me through the good times and bad.

I can just say for all above people thanks a lot for everything

Abstract

An online payment system allows a customer to make a payment to an online merchant or a service provider. Payment gateway is a channel between customer and payment processor. Gateway should use various security tools to secure a customer's payment information like debit or credit card information. However, the security provided by a payment gateway cannot completely protect a customer's payment Information. The merchant also has the ability to obtain the payment information in some form. Furthermore, many merchants have no standard payment policy. So they can not provide a secure payment environment to their customers.

Consequently, this exposes a customer's payment information to risks. It could be stolen by hackers and spammers.

In this thesis we propose a new approach to payment systems in which a customer's payment information cannot be obtained by a merchant. A customer sends his payment information directly to a payment gateway and a payment gateway, upon verifying the transaction, sends a payment to the appropriate merchant. We use the QR code to simplify the process and to make the process more secure, simple, and fast .

تلخيص أطروحة الماجستير

الباحث-- م.أسماء عدنان قاعود

نظام الدفع عبر الإنترنت (الدفع الالكتروني) هو نظام يسمح للعملاء بالتسديد ودفع الاموال للتجار أو المزودين بالسلع الكترونيا "على الإنترنت". هناك ما يسمى ببوابة الدفع وهي قناة بين العملاء ومعالج الدفع تساعد في تامين نقل المعلومات بسرية. مع العلم بأنه عند استخدام نظام الدفع الالكتروني يجب استخدام أدوات و أنظمة مختلفة من شأنها تأمين معلومات الدفع للعميل مثل الخصم أو بطاقة الائتمان من المعلومات. ومع ذلك، فإن السرية التي توفرها بوابة الدفع لا يمكن أن تحمي تماما معلومات الدفع التي تخص العميل أو المستهلك. التاجر أيضا يمكن أن تكون لديه القدرة على الحصول على معلومات الدفع التي تخص العميل بشكل ما لذلك لزم من الباحثين في مجال امن نقل المعلومات أن يكثفوا جهودهم من أجل الوصول لحل أفضل يضمن أمن معلومات المستهلك مع العلم بأنه حتى اللحظة لا يمكن الحديث عن بيئة آمنة كليا تحمي معلومات المستهلك بشكل مطلق .

ونتيجة لذلك، يمكن أن تتعرض معلومات الدفع العميل للمخاطر. كما يمكن أن تتم سرقتها من قبل المتسللين والمتطفلين.

لذلك حاولنا في هذه الأطروحة أن نضع بين أيديكم مقترحا يحاول أن يجد حلا لحماية معلومات المستهلك من السرقة وتأمين نقل هذه المعلومات بالسرية المطلوبة ،حيث حاولنا أن نصمم م نهجا جديدا لأنظمة الدفع التي من خلالها لا يمكن الحصول على معلومات الدفع الخاصة بالعميل من قبل التاجر. حيث إن العميل يرسل معلومات الدفع مباشرة إلى بوابة الدفع وبوابة الدفع بعد التأكد من البيانات، ترسل بيانات الدفع إلى التاجر المناسب. كما حاولنا أن نستخدم كودQR لتأمين سهولة عملية الدفع الالكتروني وتبسيطها وجعل هذه العملية أكثر أمانا و سرعة في الإنجاز .

TABLE OF CONTENTS:

LIST OF FIGURES:

List of Tables

List of Abbreviations

QRG: Quick response code And E-payment With Gateway
e-payment: Electronic Payment
e-check : Electronic Check
ACH: Automatic Clearing House Network
CA: Certificate Authority
QR code : Quick Response Code
E-Cash: Electronic Cash
SSL: Secure Socket Layer
SET : Secure Electronic Transaction
TLS: Transport Layer Security
NACHA :National Automated Clearing House Association
RFDI: Receiving Depository Financial Institutions
ODFI: Originating Deposit Financial Institution
DPM: Dot-Pin Marking
ATCH: Automated Transaction Clearing House .

Chapter One

Introduction

1.1. Background:

In a modern world where we are able to do almost everything on-line (banking, shopping, communicating, storing and sharing personal information...), it is nowadays a critical matter to be able to access these services in the most secured manner. Indeed, as viruses and cracking methods become more complex and powerful by the day, the available security techniques must improve as well, allowing users to protect their data and communications with the maximum confidence.

The idea of paying for goods and services electronically is not a new one since 1970s and early 1980s, a variety of schemes have been proposed to allow payment to be effected across a computer network. After a period of exponential growth, 930 million people have internet access worldwide. The electronic payment system started at the end of 1996 and in the earlier part of 1997, a huge variety of different payment methods developed by both academic researcher and commercial interests some of these were launched in the market field to reach a critical mass.

The electronic payment (e-payment) is a method of value exchange in electronic commerce, where the value is transferred via the internet and communication technologies, the electronic payment systems have evolved from traditional payment systems and consequently, the two types of systems have much in common.

1.1.1. How Electronic Payment Works?

When it comes to payment options, nothing is more convenient than electronic payment. You don't have to write a check, swipe & credit card or handle any paper

money; all you have to do is enter some information into your Web browser and click your mouse. It's no wonder that more and more people are turning to electronic payment - or e-payment ~ as an alternative to sending checks through the mail.

1.1.2. Methods and Types of Electronic Payment:

An electronic payment is any kind of non-cash payment that doesn't involve a paper check. Methods of electronic payments include credit cards, debit cards and the ACH (Automated Clearing House) network. The ACH system comprises direct deposit, direct debit and electronic checks (e-checks).
For all these methods of electronic payment, there are three main types of transaction:

1. A one-time customer-to-vendor payment is commonly used when you shop online at an e-commerce site; such as Amazon. You click on the shopping cart icon, type in your credit card information and click on the checkout button. The site processes your credit card information and sends you an e-mail notifying you that your payment was received.[1]

   On some Web sites, you can use an e-check instead of a credit card. To pay by e-check, you type in your account number and your bank's routing number. The vendor authorizes payment through the customer's bank, which then either initiates an electronic funds transfer (EFT) or prints a check and mails it to the vendor.

2. You make a recurring customer-to-vendor payment when you pay a bill through a regularly scheduled direct debit from your checking account or an automatic charge to your credit card. This type of payment plan is commonly offered by car insurance companies, phone companies and loan management companies. Some long -term contracts (like those at gyms or fitness centers) require this type of automated payment schedule.

3. To use automatic bank-to-vendor payment, your bank must offer a service called online bill pay. You log on to your bank's Web site, enter the vendor's

information and authorize your bank to electronically transfer money from your account to pay your bill.

In most cases, you can choose whether to do this manually for each billing cycle or have your bills automatically paid on the same day each month.

1.2. QR codes:

QR codes (Quick Response codes) were introduced in 1994 by Denso-Wave [2], a Japanese company subsidiary of Toyota. Initially, these codes where conceived as a quick way to keep track of vehicle parts, being nowadays extremely popular in Asian countries like Japan, South Korea, China or Taiwan and becoming more and more popular in western countries by the day.

Quick Response codes are two-dimensional bar codes, so they can be read from any direction in 360; can store up to 4,296 alphanumeric characters (or up to 1,817Japanese kanjis), which is much more than the 20 digits that a traditional bar code can store; have a great deal of resistance to damage, being readable even if they are partially damaged; and they are easy and quick to read with a camera-based device. Its versatility has made them quite popular among some industries, particularly in the advertisement world, where these are today widely used as a way to quickly store an URL by scanning it with a camera-equipped mobile device.

On the other hand, QR codes are unfortunately only understood by machines and not by human beings. This means that scanning QR codes may entail some security issues: the user doesn't really know what is behind the QR code, so she might be scanning malicious code without being aware.[3]

PayPal has made purchasing items over the Internet much easier and now is incorporating itself in QR codes. With smart phones and QR codes, you can store banking account information into your phone, so instead of carrying a bunch of cards around with you, all you will need is your cell phone. You will be able to go into a store, pick out an item, and instantly scan it's barcode to check out. As for receipts, I am sure there is a way that it can be stored in your phone for a 30 day period. Eventually over time, everything will be able to be purchased using our cell phones.

All our credit card and bank account information will be able to be shared simply through scanning a QR code.

Not only can the codes be used for purchasing items but also for paying bills! What a great way to save time and money, not have to buy checks anymore, or taking the time to sit down and pay bills. Bill comes in the mail, open it up, scan the code, paid. For myself, this technology will certainly help me make sure I am not late on my bills. QR code are making it possible to pay my dues instantly instead of having to set time aside to write a check, balance my account, and mail the check.

1.3. Thesis purpose:

This thesis proposes a new approach to electronic payment in which a customer's payment information cannot be obtained by a merchant. A customer's payment information is usually a debit or credit card detail, and providing it to a merchant during e-payment exposes this sensitive financial information to various risks. Some of these widely known risks are data tampering, stealing credit card details and credit card fraud.

A merchant may or may not exploit customer data but can definitely store it. In that case, if a merchant's server or system is not secure enough to prevent intrusion of data stealers, spammers, spyware, malware and hackers, customer data may be stolen and misused.

Hence, to avoid the issue of data mishandling or unsecured data on the merchant side, we propose a payment method that does not send customer payment information to merchants and allows only payment gateways to deal with it. Payment gateways are secure and reliable, because they comply with the standard data security rules and communicate with banks and credit card companies using the most secure methods and technologies.

Also we use the QR code technique to make the electronic payment more and more usable and secure.

Using the QR code technique with e-payment gateway will:

- Increase e payment system security.

- Increase reliability.
- Increase eligibility.
- Increase efficiency.
- Give e payment system high usage cost or customers and merchants.
- Error correction.
- QR code store many kinds of data, so it will be very suitable in marketing to store the value and the description of any product.

1.4. Problem area:

The internet is currently helping and facilitating online purchases and make payment very flexible .this has lead to a new market for companies on which the number of customers is frequently increasing.

The techniques used in the e payment system fields has some problems in security, speed, usability, and flexibility.

So we improve a new system that will solve and interact with this problems, our system will use e-payment system with gateway and will use the QR code technique to choose the product you want to buy.

When a customer's payment information is sent to merchant, the merchant has the capability to obtain the customer's payment information like credit card number, credit card issuers, expiration date,,,,,,,,etc. Even if a merchant receives a customer's payment information in an encrypted form ,he can save the encrypted information and decrypt it later .The current payment systems allow a merchant to obtain some form of a customer's payment information so that merchant can claim the validity of a transaction . However, a merchant doesn't necessarily need a customer's payment information to prove the validity of a transaction. Other information related to a purchase can be used to prove the validity of a transaction.

Frauds that occur on the internet today are mostly from hackers, fraud merchant's, spammer's and data thieves who place attacks on networks and personal computers to corrupt and steal information. Hence , to avoid these risks, it is desirable not to send

a customer's payment information to a merchant at all ,because it creates the possibilities of security breach and information leaks from a merchant side.

1.5. Thesis overview :

In this thesis, we propose an e-payment system in which a customer's payment information is sent directly to a payment gateway, instead of sending it through a merchant. This prevents a customer's payment information from being manipulated by a merchant. It differs from current approaches where customer's payment is sent to a merchant and the merchant forward it to a payment gateway.

Also in our proposed model we use QR code , in which a customer use his smartphone camera to scan the QR code that is printed on the product, this smartphone has an application that decrypt and understand the QR code and give the customer description of the product, then the customer decide whether to accept buying product or deny.

Hence, in this thesis we develop a new approach to an e-payment system in which a customer's payment information is directly sent to a payment gateway that allows only the rightful merchant to obtain the payment ,and the use of QR code will make e-payment process more simple , secure, fast and reliable

1.6. Research Questions:

From our earlier discussion above a research question has been formulated in order to make research this is stated below:

- What is e payment process?
- What is QR code?
- How can e-payment process be more secure?
- What security can be given to the e-payment systems using gateway technique?
- What security can be given to the e-payment process by using QR code?
- What is the using network on the system?
- What are the algorithms that can be used on e-payment system with gateway and QR code?

1.7. Thesis disposition :

The boundaries for interpretation of the suggestions and results presented in this thesis summarized below in fig 1.1

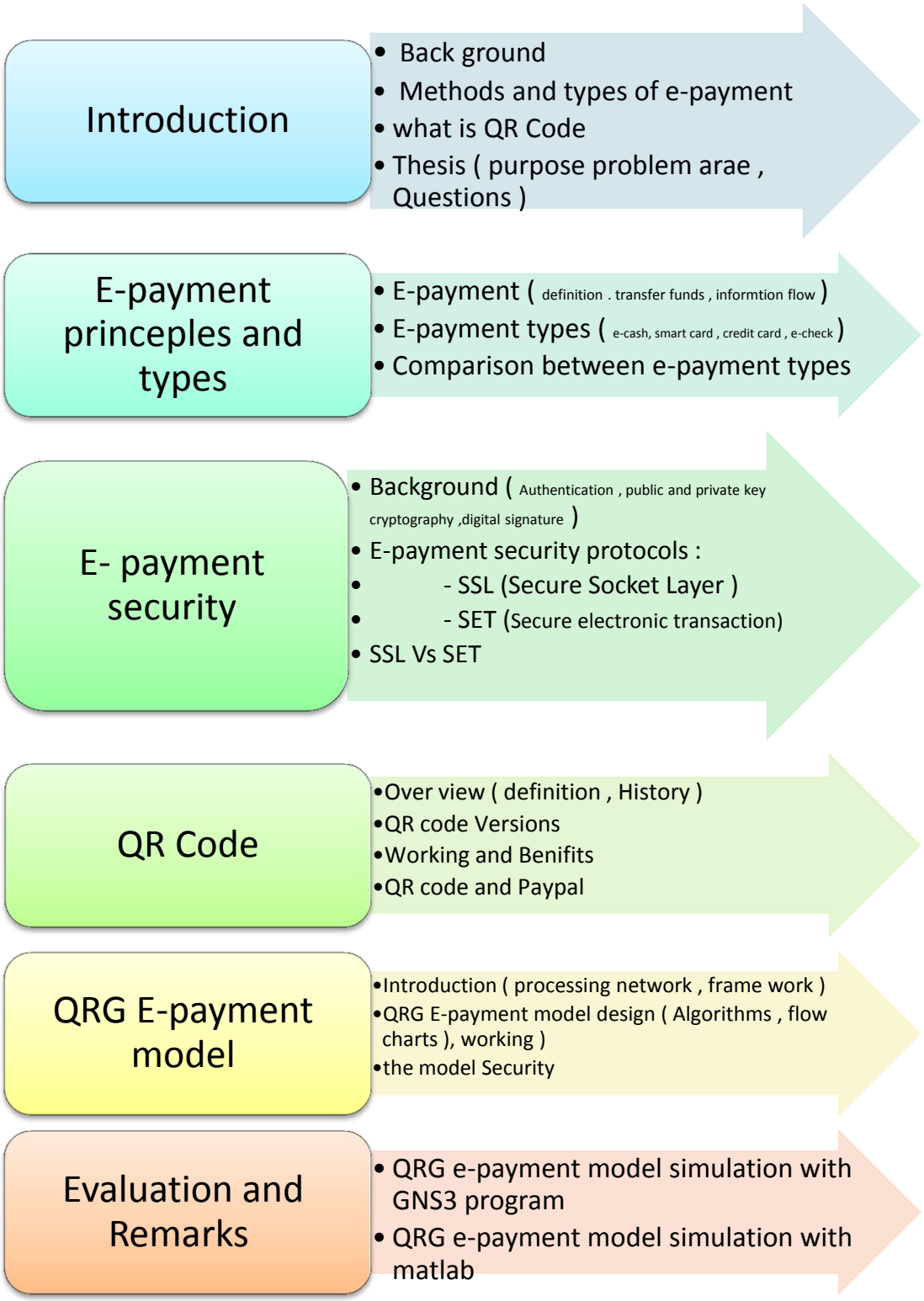


Fig 1.1: thesis main gools

Chapter 2

E-payment principles and types :

2.1. Introduction

The Internet has become the most active trade intermediary within a decade. Also, Internet shopping simplify the marketing process by allowing consumers to sit in their homes and buy an enormous variety of products and services from all over the world easily .

In recent years there has been significant development of e-payment systems and, in particular, of electronic payments around the world. And as you will see later in our thesis that debit and credit cards have gradually complemented and replaced the usual paper. The diagram shown in fig (2.1) describe e-payment process.

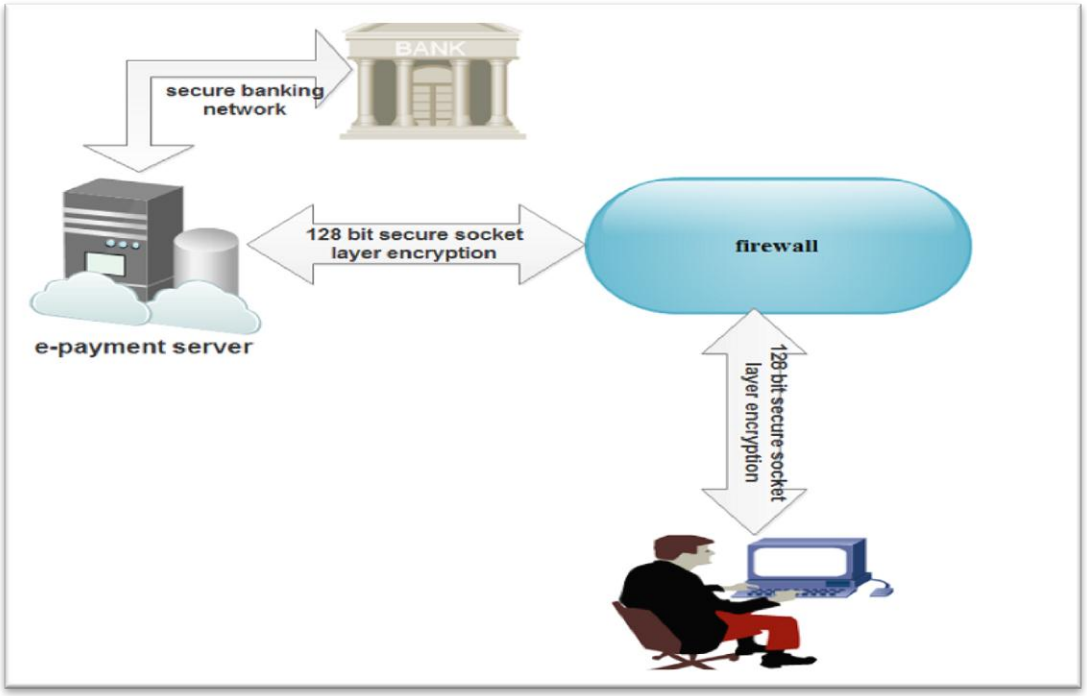


Fig (2.1) –e payment diagram

E-Commerce or Electronics Commerce sites use electronic payment where electronic payment refers to paperless monetary transactions. Electronic payment has revolutionized the business processing by reducing paper work, transaction costs, labor cost. Being user friendly and less time consuming than manual processing, helps business organization to expand its market reach expansion. [5]

2.1.1. What is e-payment?

E-payment is a form of a financial exchange that takes place between the buyer and seller facilitated by means of electronic communications, which must be secure between all components of e-payment process.

2.1.2. The Components of an e-Payment Solution:

In their most simple form, e-payments are represented in fig 2.2 diagram:

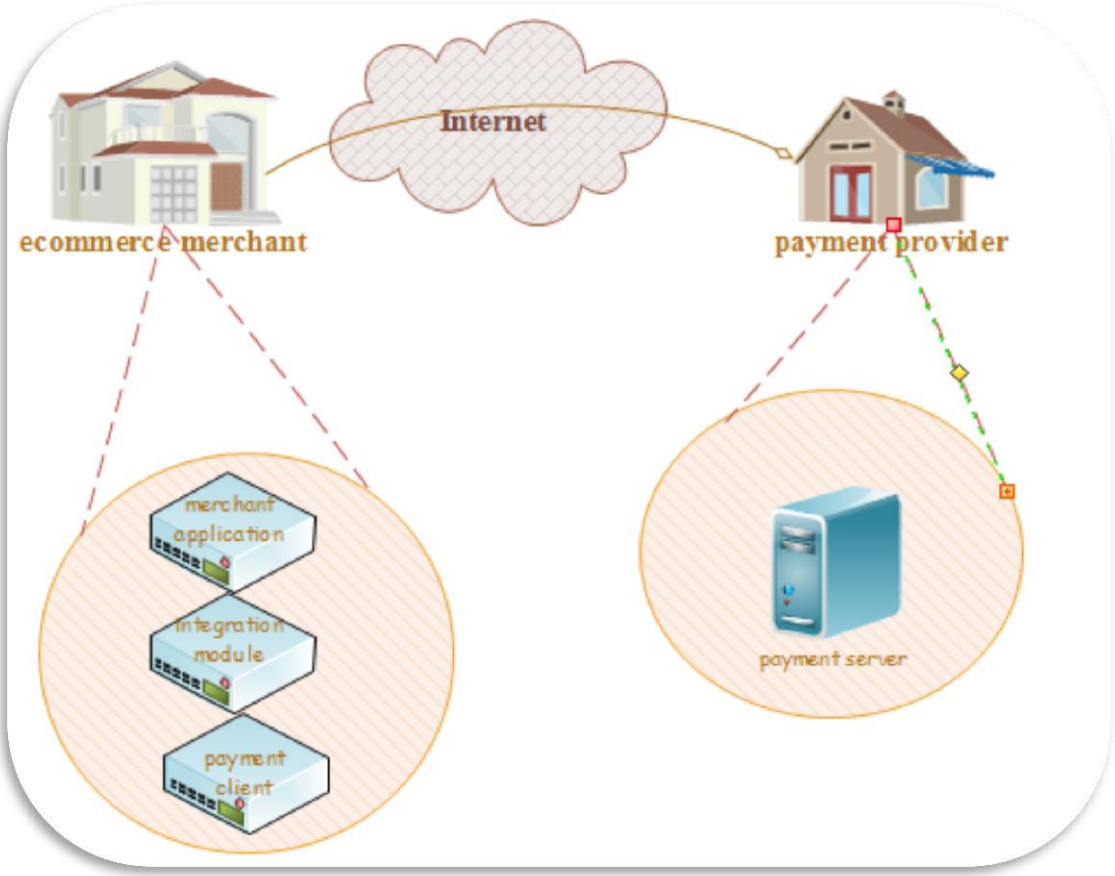


Fig (2.2).e-payment components

- **The Merchant application** is a business application/website on the merchant's system that uses payment Client to process payments.
- **The Integration module** is a communication bridge between the merchant application and payment Client.
- **Payment Client** provides secure communication between the merchant application and the payment Server. Payment Client can be integrated with a number of systems including merchant applications, Interactive Voice Response (IVR) systems, and integrated ERPs .
- **Payment Server** processes merchant Digital Orders.
- **The Payment Provider** enables the merchant to accept payments online.

2.1.3. How e-Payments Transfer Funds

E-Payments transfer funds via the following steps:

1. A customer who decides to purchase an item from an online business is transferred to a secure server where he or she enters a credit card number into a form.
2. The information entered into the secure server is encrypted using security technologies.
3. The payment information moves to the online transaction server where the payment is authorized (or declined), depending on whether the credit card number is valid and the customer has sufficient credit to cover the purchase.
4. If the credit card information is valid and funds are available, the information is transmitted to the institution or organization that receives payments owed to the merchant and a deposit is made to the merchant’s bank account.
5. The customer is informed that the transaction has been processed and shipping the goods has been initiated.

2.1.4. About e-Payment Information Flows

This section describes how information is transferred between the merchant application and the Payment Server.

The Merchant Application To process a payment, the merchant application must send the required information to the Payment Server. The merchant application uses the Payment Client to send this information to the Payment Server using two messages:

Digital Order is sent by the Payment Client to the Payment Server to provide transaction information.

Digital Receipt is sent from the Payment Server to the Payment Client to indicate the outcome of the transaction (that is, successful or otherwise).

A **Transaction** is the combination of a Digital Order and a Digital Receipt. For each customer purchase or order, merchants may issue several transactions.

Payment Client To securely communicate transaction information between the merchant application and the Payment Server, the Payment Client: Formats, encrypts and digitally signs a Digital Order from the merchant application; and Sends the Digital Order to the Payment Server Receives the Digital Receipt, decrypts it and processes the results.

The Payment Server to complete the transaction the Payment Server:
- processes the Digital Order.
- Transfers funds from the cardholder's account to the merchant's Payment Provider account and Returns a signed and encrypted Digital Receipt to Payment Client.[57]

2.2. Types of e payment:

The following types of electronic payments are most common today. That said, it is important to realize that new payment types are continual being discovered and there are additional methods that exist or are being developed continuously.

- **Instant paid or cash "**electronic cash **"**
- **Debit or prepaid "**smart card , electronic purse or e-wallet**"**
- **Credit or postpaid "**credit card, electronic checks **"**

2.2.1. E-cash:

E-cash is money in electronic form , stored in a way similar to any other data ,the digital representation of e-cash typically contains the coin identity number ,blinded users identity and digital signature of the issuer .

a user having the right kind of device can withdraw this money from his bank in a way similar to withdrawal of paper currency ,the user can later spend this electronic money for purchasing an item from a merchant .at some later point of time ,the merchant will have to deposit the values obtained from the user to the bank for its redemption.

2.2.1.1. Conceptual frame work:

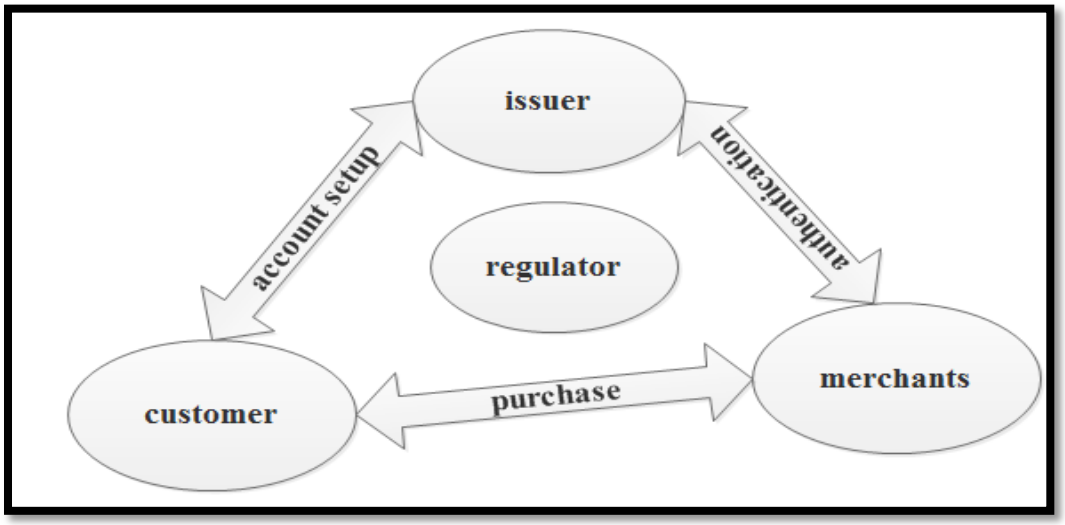
In fig 2.3 there are four major components in an electronic cash system (Issuer, customer, merchant and regulator)

For e-cash transaction to occur we need three stages:

1- **Account setup:** customers will need to obtain e cash accounts through certain issuers, merchants who would like to accept e cash will also need to arrange account from various e-cash issuers, issuers typically handle accounting for customers and merchants.

2- **Purchase:** customers purchase certain goods or services and give the merchants tokens which represent equivalent e-cash .purchase information is usually encrypted when transmitting in the networks.

3- **Authentication :** merchants will need to contact e-cash issuers about the purchase and the amount of e-cash involved , e-cash issuers will then authenticate the transaction approve the amount of e cash involved.



Fig((2.3) components of electronic cash system

2.2.1.2. Transaction types in electronic cash payment system:

Three types of transactions:

- Withdrawal: the payer transfers some of money from the bank account to his or her payment card.
- Payment: the payer transfers the money from the card to the payee.
- Deposit: the payee transfers the money received to the bank account.

2.2.1.3. E-cash model:

The complete e-cash model for e-cash working system discussed in more details in fig (2.4)

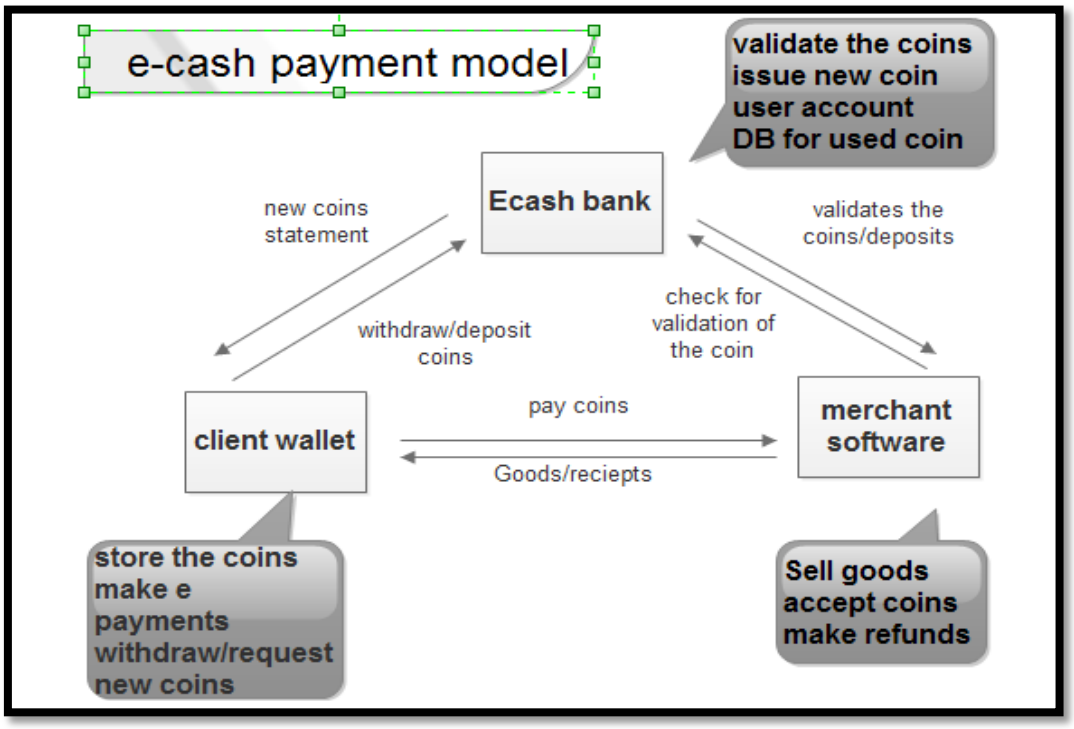


Fig (2.4) e cash model and flow chart

The complete process and steps of e-cash model are discussed in more details in fig (2.5) below

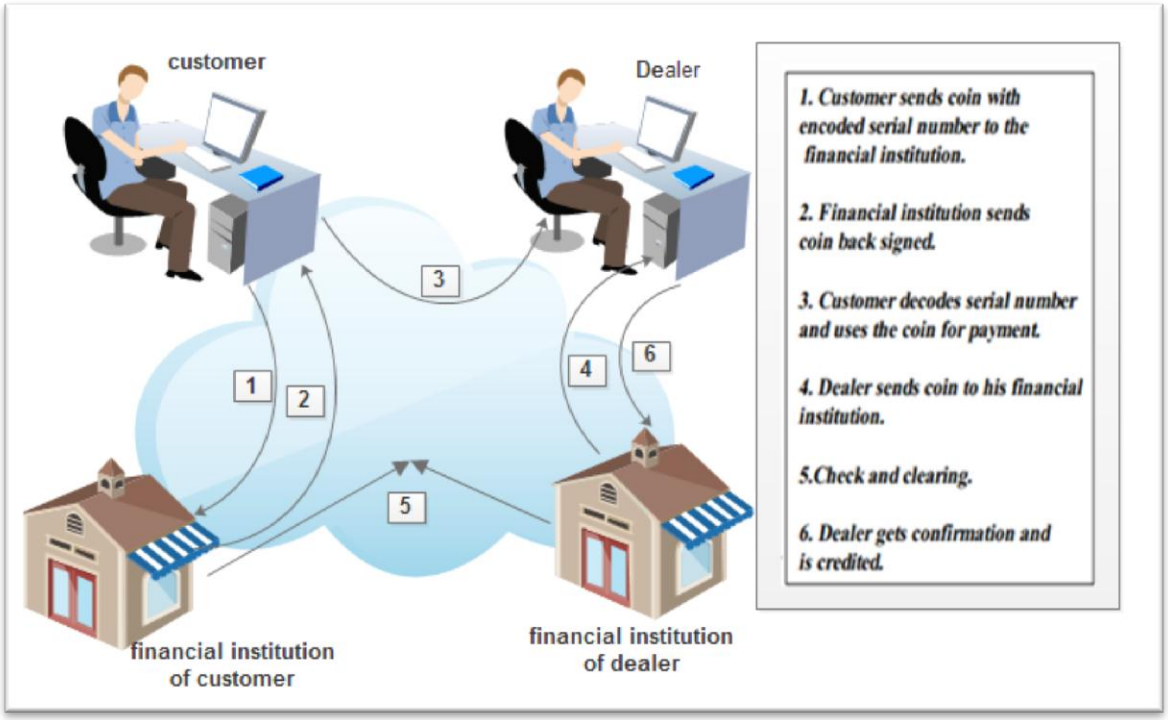


Fig (2.5) description of e cash process

2.2.1.4. E-Cash Structure

e-cash structure could be identified as a string of bits that represents certain values such as reference number and digital signature, which could be used for the security purpose to prevent forgery and criminal and protect it from the illegal copy and forgery activities further, the model modified the structure of the reference number to support tractability[6] . the e-cash structure shown in figure (2.6).

Currency[28]	Value[29]	Reference[30]	Digital Signature[31]	Digital Watermark[32]

Fig 2.6 e-cash structure

2.2.1.5. Challenges in e cash:

Being a data file in the electronic form, it is very easy to reproduce or make duplicate copies of e-cash. Therefore, there are some well-known challenges in this domain.

1. Double spending

This is the act of spending the electronic cash more than the allowed number of times (usually one) by the owner of the cash.

2. Colluding of merchants

It may be possible that more than one merchants can combine and form an illegal group to produce fake double spent cash.

2.2.1.6. Advantages of e-cash:

- Transferring e-cash on the internet costs less than processing credit card transactions because conventional money exchange systems require banks, bank branches, clerks, automated teller machines, and an electronic transaction system to manage, transfer, and dispense cash. Operating this conventional money exchange system is expensive.

- E-cash does not require authorization of payments, unlike credit card transactions. [10]

2.2.3. Smart card:

A smart card, typically a type of chip card, made of a plastic with an embedded microprocessor chip that holds important financial and personal data . This data is usually associated with either value, information, or both and is stored and processed within the card's chip. The card data is transacted via a reader that is part of a computing system. The microprocessor chip is loaded with the relevant information and periodically recharged.

In addition to these pieces of information, systems have been developed to store cash onto the chip. The money on the card is saved in an encrypted form and is protected by a password to ensure the security of the smart card solution. In order to pay via smart card it is necessary to introduce the card into a hardware terminal. The device requires a special key from the issuing bank to start a money transfer in either direction. Smart cards can be disposable or rechargeable. smart cards are in use today in several key applications, including healthcare, banking, entertainment, and transportation.

2.2.3.1. Why Smart Cards

Smart cards improve the convenience and security of any transaction. They provide tamper-proof storage of user and account identity. Smart card systems have proven to be more reliable than other machine-readable cards, like magnetic stripe and barcode, with many studies showing card read life and reader life improvements demonstrating much lower cost of system maintenance. Smart cards also provide vital components of system security for the exchange of data throughout virtually any type of network. They protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. The costs to manage password resets for an organization or enterprise are very high, thus making smart cards a cost-effective solution in these environments. Multifunction cards can also be used to manage network system access and store value and other data.

Smart cards have been extensively used in the telecommunications industry for years. Smart-card technology can be used to hold information on health care, transportation, identification, retail, loyalty programs and banking, to name a few. Smart cards enable information for different purposes to be stored in one location. The microprocessor chip can process different types of information, and therefore, various industries use them in different ways.[7]

2.2.3.2. Types of Smart Card

Smart cards are broadly classified into two groups:

Contact: This type of smart card must be inserted into a special card reader to be read and updated. A contact smart card contains a microprocessor chip that makes contact with electrical connectors to transfer the data.

Contact-less: This type of smart card can be read from a short distance using radio frequency. A contact-less smart card also contains a microprocessor chip and an antenna that allows data to be transmitted to a special card reader without any physical contact.

2.2.4. Credit card :

2.2.4.1. Credit Cards and Electronic Commerce

At the broadest level, the credit card processing models in e-commerce transactions can be classified into two categories, based on who takes on the job of processing credit cards and making payments. These two models are

(a) Without involving a payment gateway:

This follows the traditional (manual) approach of credit card processing. Here, a third party (called a payment gateway) is not involved in the credit card processing. Therefore, it is left to the merchant to process credit cards online.

(b) Involving a payment gateway:

In this type of credit card processing mechanism, a third party specializing in credit card processing, i.e. the payment gateway, is involved. What is a payment gateway, and why is it required?

The payments related to e-commerce transactions pose the following difficulties:

1. Settlement of payment by physical means slows down the process and is inconvenient.
2. The buyer and seller are not physically present at the same place during the transaction and may often be completely unknown to each other. Therefore, although they may be genuine, their identities need to be authenticated.
3. The Internet being a public network, raw transmission of payment data (e.g. credit card and amount details) to the merchant or any other party is highly unsafe.

A payment gateway facilitates e-commerce payments by authenticating the parties involved, routing payment related data between these parties and the concerned banks/financial institution in a highly secure environment and providing general support to them.

The merchant ties up with a payment gateway, which takes on the responsibility of processing credit cards on the merchants behalf. The payment gateway ties up with all the banks and financial institutions whose participation is required for effecting electronic payments, relieving the merchant of these responsibilities. The payment gateways are independent companies offering payment solutions to merchants for effecting online payments.

2.2.4.2. Credit Card Processing Without a Payment Gateway

This model of processing credit cards is very similar to the way shops and restaurants process credit cards in the manual scenario. The same process is imitated using the Internet technologies. This happens as follows.

- **Stage 1: Verification**

In this step, the credit card details of the customer are verified with the help of a number of financial institutions. Let us understand the process shown in Figure (2.7)

1. The customer provides the credit card details such as the credit card number, expiry date and the customer's name as it appears on the credit card, to the merchant and the customer.
2. The merchant would forward this information (via another SSL-enabled session) to its own bank, known as the acquiring bank.
3. The acquiring bank would then forward these credit cards details, in turn, all the way, to the customer's bank, known as the issuing bank via the card association.

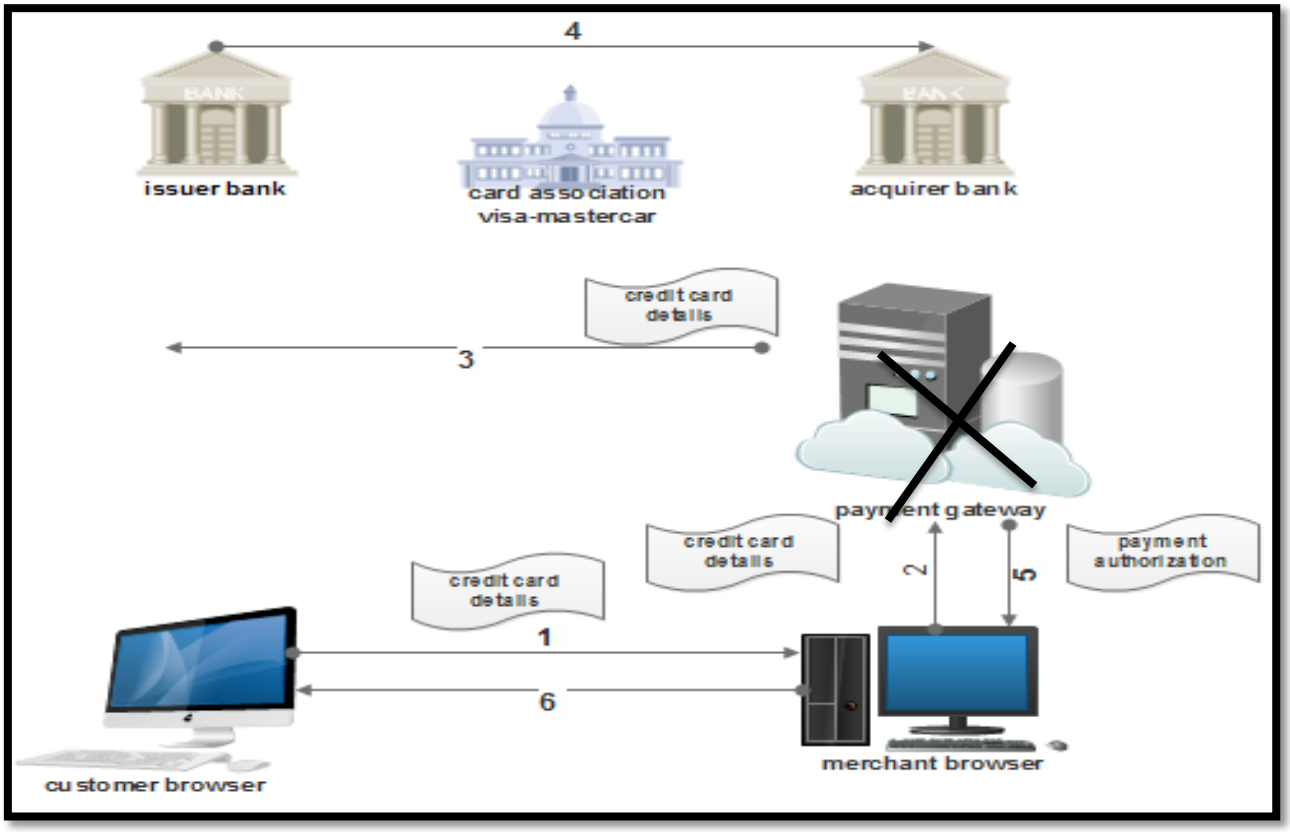


Fig (2.7) steps of credit card verification stage

4. The card-issuing bank would verify information such as the credit card details, the customer's credit limit, whether the credit card is in the list of stolen credit cards, etc. and send an appropriate status back to the merchant's acquiring bank.
5. The merchants acquiring bank would then forward the status message back to the merchant.
6. Depending on whether the credit card was validated successfully or not, the merchant would either process the order, or reject it and inform the customer accordingly.

- **Stage 2: Payment**

Having verified the credit card details of the customer, the actual payment processing has to happen now. This is shown in Figure (2.8)

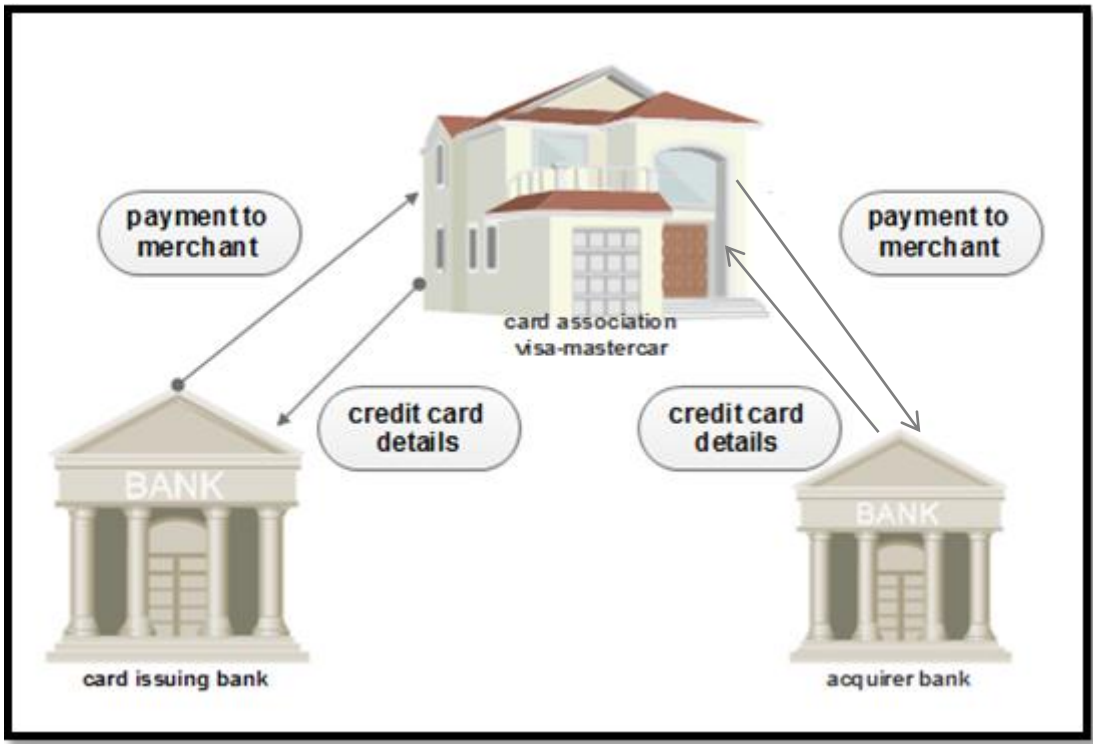


Fig (2.8) Steps of credit card payment stage

The merchant would collect all such credit card transactions that took place in a particular day, and send their list to its acquiring bank for obtaining payment for them. The acquiring bank would then interact with the various card-issuing banks through the card-association clearing house (a financial institution that settles credit card payments between banks, i.e. Visa or MasterCard)

This process causes funds transfer from the issuing banks to the acquiring bank, and then to the merchant's account.

2.2.4.3. Credit Card Processing Involving a Payment Gateway

Let us now take a look at the concept of involving a third party the payment gateway In electronic commerce transactions. Let us draw a conceptual framework for electronic commerce payment processing transactions, when a payment gateway is involved, as shown in Figure (2.9).

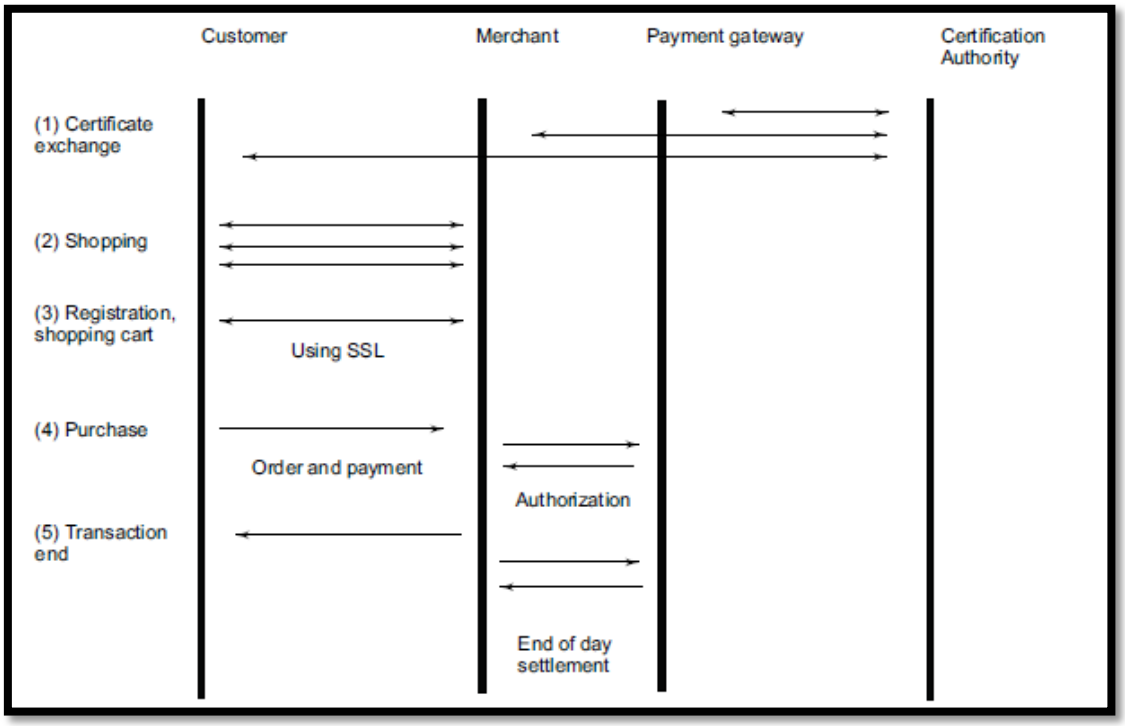


Fig (2.9)Flow of credit card processing involving a payment gateway

As Figure (2.9) illustrates, the interaction between a customer, a merchant, a payment gateway and a certification authority consists of many steps. These steps are as follows.

1. Usually all the concerned parties (i.e. the customer, the merchant and the payment gateway) obtain digital certificates from a certification authority.

2. Then, the customer interacts with the merchants site, adding, removing, or changing products .Finally, the user confirms the transaction.

3. Placing the order and making payment follow step 2.

4. The merchant, at this stage, obtains a payment authorization from the payment gateway. If this is successful, the transaction is considered to be complete.

Finally, the settlement between the merchant and the payment gateway takes place in the form of many such payment requests being put together in a batch, and processed. This usually happens offline, that is, after normal working hours. For this, the merchant sends a list of all payments expected to be received from the payment gateway. The payment gateway, in turn, uses the information of payment records and interacts with the acquiring bank and the card-issuing bank to debit the customer account and credit the merchant account. This is shown in Figure (2.10).

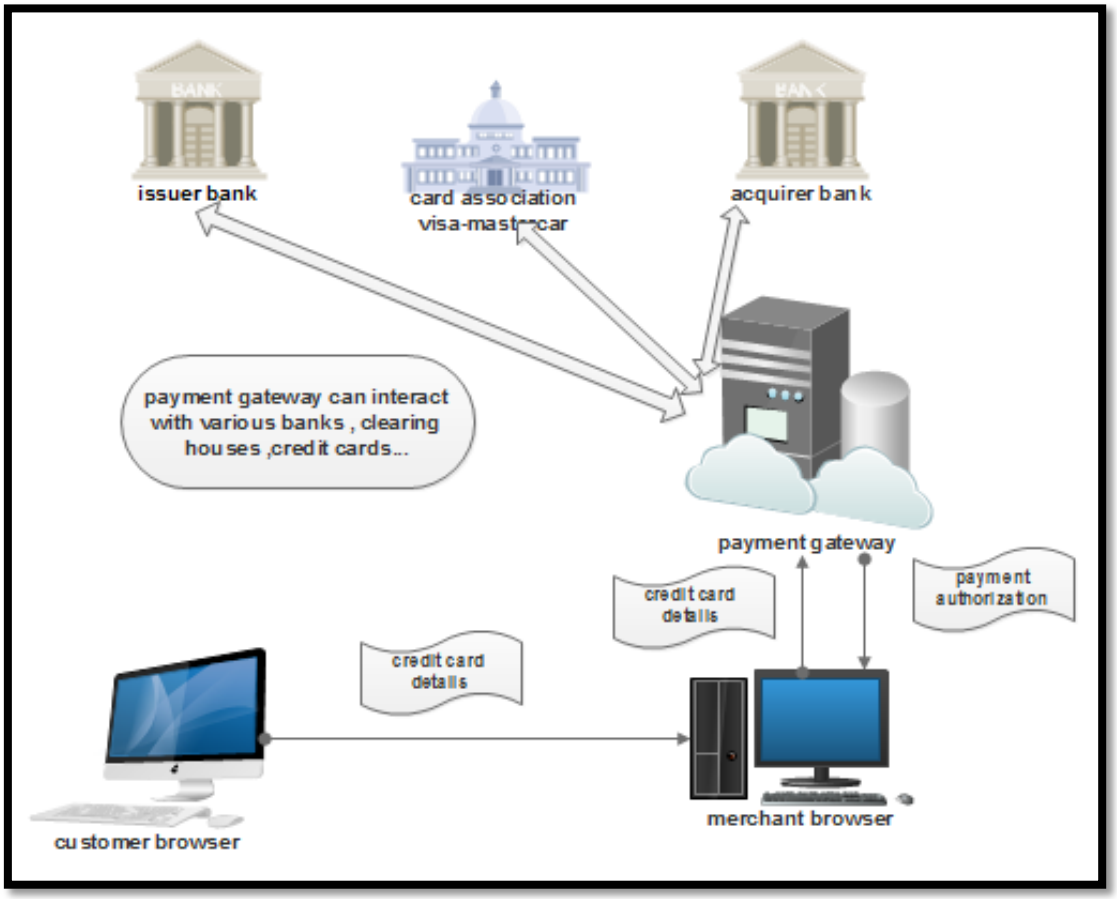


Fig (2.10):Credit card with gate way process

.

2.2.5. E-check:

e-Check, a new payment instrument combining the security, speed and processing efficiencies of all-electronic transactions with the familiar and well-developed legal infrastructure and business processes associated with paper checks, An e-Check is a computer document (or file) that can be easily processed by any

application and exchanged between systems using any appropriate communications medium.

Electronic checks can be exchanged directly between parties by any means, such as email, the World Wide Web, or private Value Added Networks (VAN) services.

The e-Check provides rapid and secure settlement of financial accounts between trading partners over open public or proprietary networks. These networks can be interconnected with the existing bank clearing and settlement systems infrastructure. Little pre-arrangement is required, other than agreeing on how to exchange the check.

2.2.5.1. How e-check works?

Electronic check conversion is a simple method of processing payments, and the changes to how you do business are minimal. One of this Method's greatest advantages is that you can electronically submit checks instead of having to physically take them to the bank, saving you time and increasing employee efficiency.

e-Checks work the same way a check does. As you can see in the below diagram Fig(2.11) but e-check make this process electronically without any paper

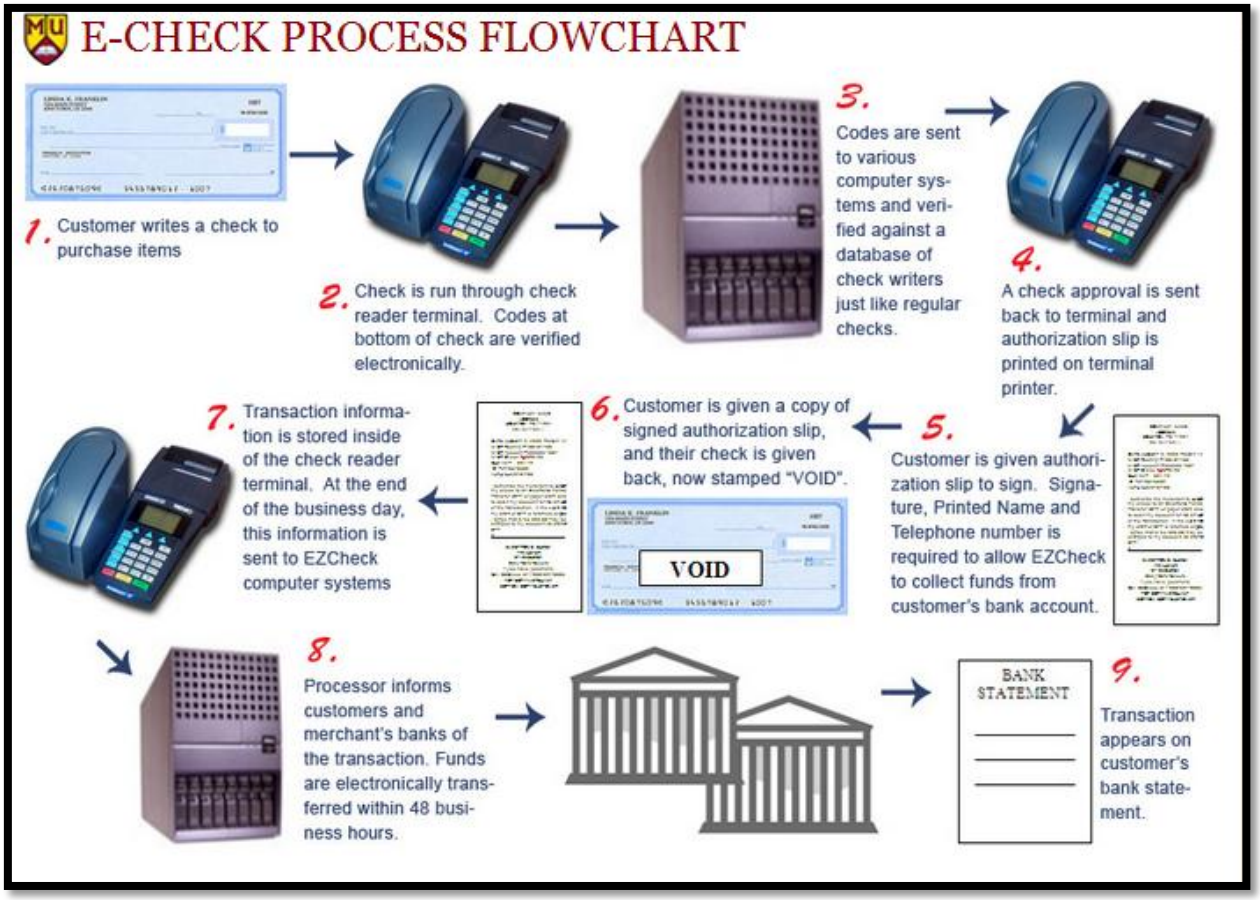


Fig (2.11)How e-check work?

1- a purchaser fills a purchase order form, attaches a payment advice (electronic check), signs it with his private key (using his signature hardware), attaches his public key certificate, encrypts it using his private key and sends it to the vendor.

2- The vendor decrypts the information using his private key, checks the purchaser's certificates, signature and check, attaches his deposit slip, and endorses the deposit attaching his public key certificates. This is encrypted and sent to his bank.

3- The vendor's bank checks the signatures and certificates and sends the check for clearance. The banks and clearing houses normally have a private secure data network.

4- When the check is cleared, the amount is credited to the vendor's account and a credit advice is sent to him.

5- The purchaser gets a consolidated debit advice periodically.[6]

2.2.5.2- HOW ARE ELECTRONIC CHECKS MADE SECURE?

e-Check has an array of strong security features, which make it a safe new payments offering, suitable for use in unsecured environments like the Internet. E-Checks use both technology and business practice security safeguards, including state of the art digital signatures, hardware tokens, duplicate detection, blinded account numbers, activation, and current banking practices[17,18].

Electronic check conversion leverages the latest information protection features such as encryption and message authentication. Because of this, many retail merchants, merchant service providers, and financial institutions consider it to be one of the most secure payment methods in the electronic payment processing industry.

- **Authentication.** Merchants must verify that the person providing the checking account information has the authority to use that checking account. There are a number of authentication services and products available to merchants, including:

    - Digital signatures. Digital signatures (or digital certificates) are a way of encrypting information that gives the receiver a more reliable indication that the information was sent by the claimed sender. They are used by programs on the Internet to confirm the identity of a customer to concerned third parties, serving a similar purpose as a handwritten signature. Digital signatures cannot be easily tampered with or imitated and are easily transportable, thereby making them a reliable method for verifying identity when implemented correctly. Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature.
    - Public key cryptography. Public key cryptography is an encryption/decryption security method that uses one key to encrypt a sent message and another to decrypt it. With electronic check conversion, the private key is a secret mathematical calculation used to create the digital signature on the e-check, and the public key is the corresponding key given to anyone who needs to verify that the sender signed the e-check and that

the electronic transfer has not been tampered with. Public key cryptography is another way to ensure authenticity of the electronic transfer of funds.

- **Duplicate detection.** Duplicate prevention and detection is another way to reduce fraudulent activities. Financial institutions have software and operational controls in place to prevent duplication of the scanned electronic representations of customer checks.
- **Encryption.** The ACH (appendex I) Network automatically encrypts messages using 128-bit encryption and a secure sockets layer (SSL).

2.2.5.3. Advantage of e-check :

Using electronic check conversion to process your customers' payments holds many benefits over paper checks:

- **Reduced processing costs.** In general, the cost to process an e-check is substantially less than that of paper check processing or credit card transactions; e-checks require less manpower to process and eliminate incidental costs such as deposit and transaction fees that accompany paper checks. With e-checks, you can save up to 60% in processing fees.
- **Funds received sooner.** Businesses that use electronic check conversion have funds deposited almost twice as fast as those using the traditional check processing method, with billing companies often receiving payments within one day.
- **Increased sales.** If your business didn't accept paper checks in the past, you can expand the payment options available to your customers and increase sales by offering e-checks. If you are converting from accepting paper checks to e-checks, you can still expand your customer base by being able to accept international and out-of-state checks without the worry of fraud; e-checks require account validation and customer authentication processes that identify bad checks within seconds.
- **Simple, safe, smart.** Electronic check conversion is easy to set up and relies on the ACH Network for processing, the same reliable and trusted funds transfer system that handles Direct Deposit and Direct Payment. Plus, e-

checks are a smart choice for the environment, helping to reduce more than 67.4 million gallons of fuel used and 3.6 million tons of greenhouse gas emissions created by transporting paper checks.

- **Fewer errors and reduced fraud.** E-checks are processed using an automated system, which cuts down the number of people who must handle the check, reducing the potential for error and fraud. Merchant service providers also maintain, monitor, and check files against negative account databases that store information about individuals or companies that have past records of fraud to help decrease fraudulent activity.

2.2.6. Comparison between electronic payment systems :

The electronic payment system- the ability to pay electronically for goods and services purchased online- are an integral part of e-commerce and an essential infrastructure for e-commerce models. One of the major reasons for the widespread of e-commerce transactions is perhaps the rapid development and growth of various electronic payment systems .The present part of the study revealed many electronic payment systems and broadly these electronic payment system can be grouped or classified into four categories: (1) Online Credit Card Payment System (2) Online Electronic Cash System (3) Electronic Check System and (4) Smart Cards based Electronic Payment System. These payment systems have numbers of requirements: e.g. security, acceptability, convenience, cost, anonymity, control, and traceability. Therefore, instead of focusing on the technological specifications of various electronic payment systems, the researcher has distinguished electronic payment systems based on what is being transmitted over the network; and analyze the difference of each electronic payment system by evaluating their requirements, characteristics and assess the applicability of each system[6] . Table (2.1) presents the comparison of various electronic payment systems .

Table (2.1)comparison between E-payment types[6]

Features	Online Credit Card Payment	Electronic Cash	Electronic check	Smart Cards
Actual Payment Time	Paid later	Prepaid	Paid later	Prepaid
Transaction information transfer	The store and bank checks the status of the credit card	Free transfer. No need to leave the name of parties involved	Electronic checks or payment indication must be endorsed	The smart card of both parties make the transfer
Online and offline transactions	Online transactions	Online transactions	Offline transfers are allowed	Offline transfers are allowed
Bank account involvement	Credit card account makes the payment	No involvement	The bank account makes the payment	The smart card account makes the payment
Users	Any legitimate credit card users	Anyone	Anyone with a bank account	Anyone with a bank or credit card account
Party to which payment is made out	Distributing Bank	Store	Store	Store
Consumer's *transaction risk*	Most of the risk is borne by the distributing bank,	Consumer is at risk of the electronic cash	Consumer bears most of the risk, but the	Consumer is at risk of the smart card getting

	consumers only have to bear part of the risk	getting stolen, lost, or misused	consumer can stop check payments at any time	stolen, lost or misused
Current degree of popularity	Credit card organizations check for certification then total the purchases. Therefore, it can be used internationally, and is the most popular payment type	Unable to meet financial internet standards in the areas of expansion potential and internationalism	Can't meet international standards, therefore it's not very popular	Credit card organizations check for certification then total the purchases. Therefore it can be used internationally, and is becoming more widely used.
Anonymity	Partially or entirely anonymous	Entirely anonymous	No anonymity	No anonymity
Small payments	Transaction costs are high. Not suitable for small payments	Transaction costs are low, suitable for small payments	Allows stores to accumulate debts until it reaches a limit before paying for it. Suitable for small payments	Transaction costs are low. Allows stores to accumulate debts until it reaches a limit before paying for it. Therefore, it is suitable for small payments
Database	Safeguards	Needs to safeguard a large database,	Safeguards	Safeguards

safeguarding	regular credit card account information	and maintain records of the serial numbers of used electronic cash.	regular account information	regular account information
Transaction information face value	Can be signed and issued freely in compliance with the limit	Face value is often set, and cannot be changed	Can be signed and issued freely in compliance with the limit	Can be deducted freely in compliance with the limit
Real/Virtual world	Can be partially used in real world	Can only be used in the virtual world	Limited to virtual world, but can share a checking account in the real world.	Can be used in real or virtual worlds.
Limit on transfer	Depends on the limit of the credit card	Depends on how much is prepaid	No limit	Depends on how much money is saved
Mobility	Yes	No	No	Yes

After analysis and comparison of various modes of electronic payment systems, it is revealed that it is quite difficult, if not impossible, to suggest that which payment system is best. Some systems are quite similar, and differ only in some minor details. Further, all these systems have ability or potential to displace cash. Added to this,

widely different technical specifications make it difficult to choose an appropriate payment system.

Advantages and disadvantages of e-payment system:

Electronic Payments or e-payments refer to the technological breakthrough that enables us to perform financial transactions electronically .E-payments have several advantages, which were never available through the traditional modes of payment. Some of the most important are:

- Privacy
- Integrity
- Compatibility
- Good transaction efficiency
- Acceptability
- Mobility
- Low financial risk
- Anonymity
- Perhaps the greatest advantage of e-payments is the convenience. There is no waiting for a merchant or business to open. Vacationers and others away from home need not worry that they forgot to drop off the payment for the utilities or mail the check for their credit card bill. They can simply pull up their account online and pay their bills on the road.

- This leads to the second best benefit of e-payments- they save time.. E-payments have reduced the amount of time spent on bill management or payment by about 60%.

- The cost of e-payments is yet another benefit. For the majority of merchants, vendors, and businesses, there is no fee or charge to pay online. For others, the fee is nominal. Compared to the cost of postage, check writing fees and trips to the post office, individuals paying their bills online can save hundreds of dollars per year. In this day and age, reducing expenses is quite important for many individuals.

On the flip side, with so many benefits to using e-payments, it's important to remember that there are negative aspects too.

- Some of the biggest downsides of e-payments are the lack of authentication, repudiation of charges and credit card fraud. There is no way to authenticate or verify that the individual entering the information online is who they say they are. There is no request for picture identification or even a signature. Therefore, an unauthorized user may carry out transactions in your name before you have time to alert authorities the information has been taken. Because no identifying information is provided at the time of the online payment, an individual may have an extremely hard time disputing a charge later. Further, given the benefits of convenience and speed that come along with e-payments, this creates the perfect opportunity for fraudulent credit card transactions.

- One of the other disadvantages of e-payments is that most sites require you to open an online account with them. You need to register with the institution in order to be authorized to perform money transactions with them. While the overall payment process is efficient, the initial registration to a given site can be time-consuming. It also involves a username and a password, which implies the need of password protection, to maintain an e-payment account at each organization. If a person has more than one or two accounts, e-payments can become extremely cumbersome.

- Finally, despite the belief of many to the contrary, e-payments are secure. They may even be more secure than the old fashion way of mailing in a check. According to most sources, most instances of identity theft occur by stealing mail out of a person's mailbox or from discarded trash, not over the Internet. Encryption technology allows an individual's personal financial data to be scrambled before it is sent electronically. It also lowers the risk of human error by reducing the number of people touching the payment once it leaves the payer.

Anyone considering using an electronic payment system for paying monthly bills should carefully consider how that organization's electronic payment system works. Ask what lead time the system will require from them in order to make sure their payments are being made timely. And, most importantly, find out what safeguards are in place to prevent unauthorized individuals from obtaining or using their information and resolving payment conflicts. Users should learn what protections are in place with respect to fees and penalties applied to improperly processed payments. Every need or obligation is different, and for some, the electronic payment services may be of great help.

Chapter Three

E-payment Security:

3.1. Background

Secure electronic funds transfer is crucial to e-commerce. In order to ensure the integrity and security of each electronic transaction and other EPSs utilize some or all of the following security measures and technologies directly related to EPSs: Authentication, public key cryptography, digital signatures, certificate, certificate authorities, SSL, S-HTTP, secure electronic transmission (SET).

Authentication:

This is the process of verification of the authenticity of a person and /or a transaction. There are many tools available to confirm the authenticity of a user. For instance, passwords and ID numbers are used to allow a user to log onto a particular site.

Public Key Cryptography:

Public key cryptography uses two keys , one public and one private , to encrypt and decrypt data, respectively. Cryptography is the process of protecting the integrity and accuracy of information by encrypting data into an unreadable format, called cipher text. Only those who possess a private key can decrypt the message into plain text.

Public key cryptography uses a pair of keys, one private and one public. In contrast, private key cryptography uses only one key for encryption. The advantage of the dual-key technique is that it allows the businesses to give away their public key to anyone who wants to send a message. The sender can then encrypt the message with the public key and send it to the intended businessman over the

Internet or any other public network; the businessman can then use the private key to decrypt the message. Obviously, the private key is not publicly known .

Digital Signature:

Rather than a written signature that can be used by an individual to authenticate the identity of the sender of a message or of the signer of a document; a digital signature is an electronic one. E-check technology also allows digital signatures to be applied to document blocks, rather than to the entire document. This lets part of a document to be separated from the original, without compromising the integrity of the digital signature. This technology would also be very useful for business contracts and other legal documents transferred over the Web.

A digital signature includes any type of electronic message encrypted with a private key that is able to identify the origin of the message. The followings are some functions of digital signature.

- **The authentication function:** The term digital signature in general is relevant to the practice of adding a string of characters to an electronic message that serves to identify the sender or the originator of a message.
- **The seal function:** Some digital signature techniques also serve to provide a check against any alteration of the text of the message after the digital signature was appended.
- **The integrity function:** This function is of great interest in cases where legal documents are created using such digital signatures.
- **The privacy function:** Privacy and confidentiality are of significant concerns in many instances where the sender wishes to keep the contents of the message private from all hut the intended recipient.

E- payment security:

There have been many studies of e-payment security. Security in E-commerce was described in the paper written by Dhilon [58] who introduce the stages to be provided for online purchase, the approach is based on encryption and compression for making information unreadable. However, E-payment security has become a

consistent and growing problem as new internet technologies and application are developed; it needs new architecture to adapt to many changes. Al-SLamy [59] described the role of Pretty Good Privacy (PGP) to provide confidentiality, authentication, compression and segmentation services for E-payment security. Byung Lee [60] introduced The Advanced Secure electronic payment (ASEP) which use ECC (Elliptic Curve Cryptosystem), SHA (Secure Hash Algorithm) and 3BC (Block Byte Bit Cipher) instead of RSA and DES in order to improve the strength of encryption and the speed of processing.

There are a few different protocols that are used for online security today. The most common security mechanism is SSL. Some of the others include TLS, and SET.

3.2. Secure Socket layer (SSL):

3.2.1. Introduction:

In 1994 Netscape communication developed a network authentication protocol known as secure socket layer "SSL" . SSL is a commonly protocol used to encrypt messages between web browsers and web servers . It encrypts the datagrams of the Transport Layer protocols. SSL is also widely used by merchants to protect the consumer's information during transmission, such as credit card numbers and other sensitive information. SSL is used to provide security and data integrity over the Internet and thus plays an important role. SSL has now become part of Transport Layer Security (TLS), which is an overall security protocol.

3.2.1.1. Where does SSL fit in ?

TCP/IP protocol is responsible for making all communication possible on the internet, on the top of TCP/IP protocols there are application protocols such as HTTP and FTP, SSL fits in between the application protocol and TCP/IP[4] as shown in fig(3.1).

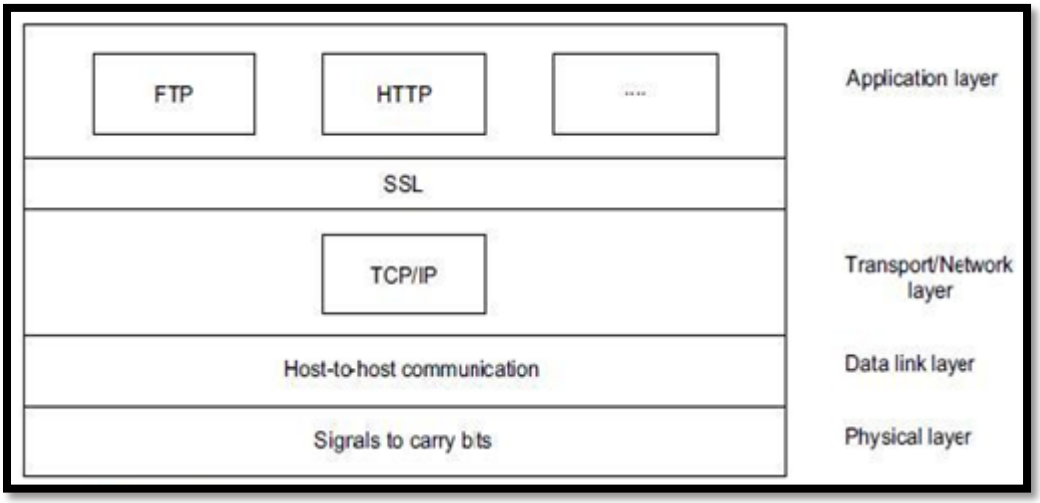


Fig 3.1:Where SSL fits?

SSL uses TCP / IP on behalf of the higher level protocols it allows an SSL enabled server to authenticate itself to an SSL enabled client and allow the client to authenticate itself to the server, this allows both computers to establish an encrypted connection [3].

3.1.2. SSL sub protocols :

3.2.2.1. SSL handshake protocol :

Is used for exchanging a series of messages between an SSL enabled server and an SSL enabled client when the first establish an SSL connection .

SSL handshake protocol perform the following:

- Authenticate the server to the client.
- Allow the client and the server to select the cryptographic algorithm
- Optionally authenticate the client to the server.
- Use asymmetric key encryption technique to generate shared socket.
- Establish an encrypted SSL connection.

3.2.2.2. SSL record protocol:

Transmit data between the client and the server, this is used after the SSL handshake protocol had established an encrypted SSL connection between client and server[11]

3.1.3.How SSL work ?

- SSL use combination of asymmetric key and symmetric key encryption technique.
- An SSL session start with an exchange of a group of messages called the SSL handshake.
- The steps involved in the handshake can be described in brief as shown in fig (3.2)

The SSL handshake is thus complete , and the SSL session start the client and the server use the session keys to encrypt and decrypt the data they send to each other and to validate its integrity.

3.1.4. Advantages of SSL:

- **Authentication:** Permits Web-enabled browsers and servers to authenticate each other.
- **Access Limit:** Permits controlled access to servers, directories, files, and services.
- **Data Protection:** Guarantees that exchanged data cannot be corrupted without detection.
- **Information Share:** Permits information to be shared by browsers and servers while remaining out of reach to third parties.

3.1.5. Disadvantages of SSL:

- **Simple Encryption:** This might increase the chances of being hacked by computer criminals.
- **Stolen Certificate / Key:** One important drawback of SSL is that certificates and keys that originate from a computer can be stolen over a network or by other electronic means.
- **Point-to-Point Transactions:** SSL handles only point-to-point interaction.
- **Customer's risk:** Customers run the risk that a merchant may expose their credit card numbers on its server; in turn, this increases the chances of credit card frauds.
- **Merchant's risk:** Merchants run the risk that a consumer's card number is false or that the credit card won't be approved.
- **Additional overhead:** The overhead of encryption and decryption means that secure HTTP (SHTTP) is slower than HTTP.

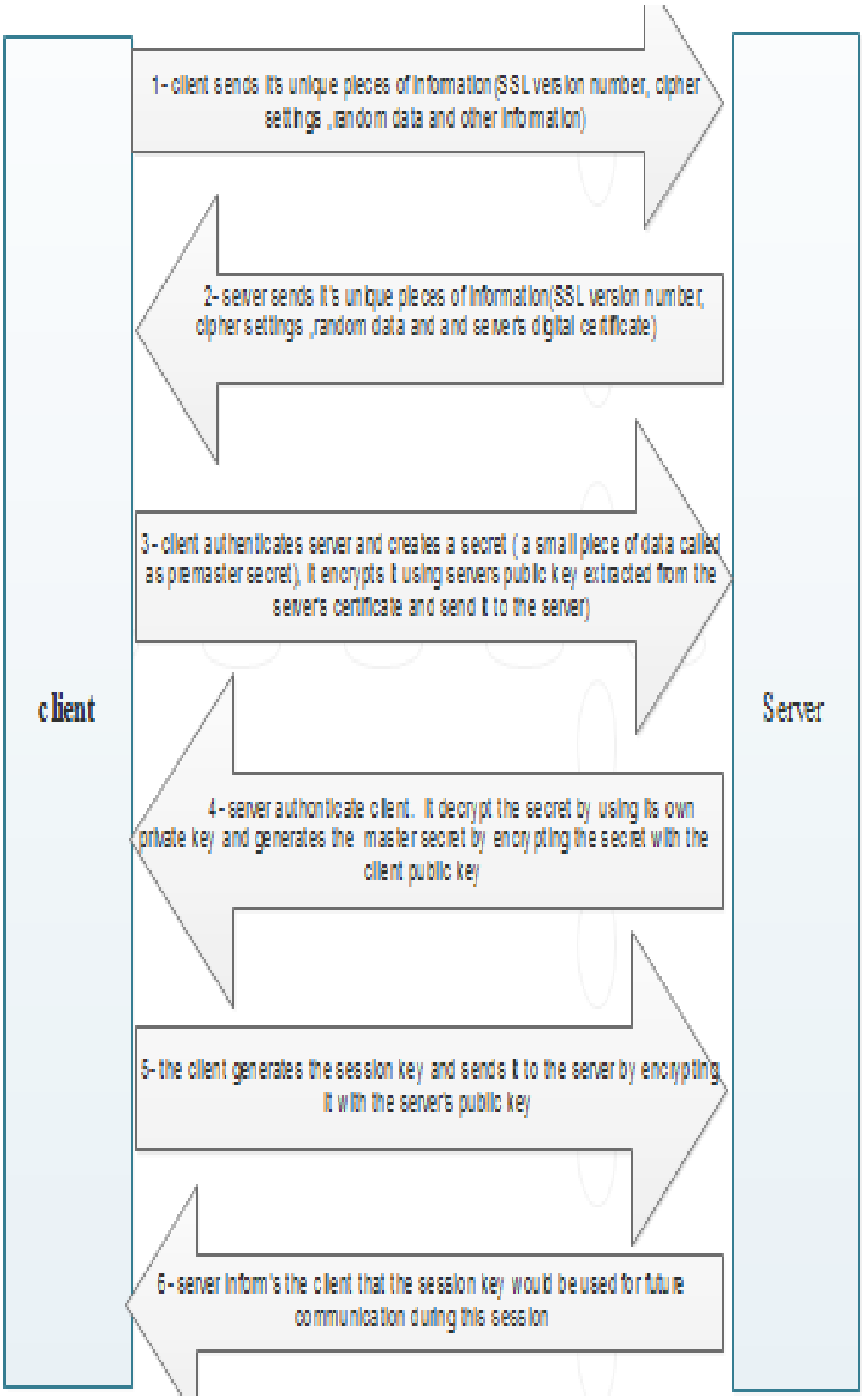


Fig 3.2:SSL handshake protocol

3.2. Secure Electronic Transaction (SET):

The secure electronic transaction is an open encryption and security specification. The work on this area began in 1996 by master card and Visa jointly started from that time there have been many tests of the concepts, and the first generation of SET was appeared in 1998 SET isn't a payment system, instead it is asset of security protocols and formats that enable the users to employ the existing credit card payment infrastructure on the internet in secure manner[12].

SET services can be summarized as follows:

1- It provides a secure communication channel among all the parties involved in an ecommerce transaction.

2- It provides authentication by the use of digital certificate s.

3- It ensures confidentiality.[13]

3.2.1. SET participants:

- **Card holder:** is an authorized holder of payment card such as master card or visa that has been issued by an issuer this term is used interchangeably with customer.
- **Merchant:** person or organization that wants to sell goods or services to card holder.
- **Issuer:** is responsible for the payment of the card holders debit, provides a payment card to the card holder.
- **Acquirer:** has relationship with merchants for processing payment card authorization and payment
- **Payment gateway:** this task that can be taken by the acquirer or by an organization as dedicated function**,** specifically in SET the payment gate way acts as an interface between SET and the existing card payment network for payment authorization.
- **Certificate authority:** (CA) this is an authority that is trusted to provide public key certificates to card holder , merchant and payment gateway.[4]

3.2.2. SET process:

1- The card holders open an account "with bank that support electronic payment mechanism".

2- The card holder receives a certificate , the certificate also contains details such as the card holder , public key and its expiration date.

3- The merchant receives a certificate.

4- The card holder places an order "shopping card process " the list of items appear on the card holder browser , the merchant sends detailed such as the list of items selected back to the card holder.

5- The merchant is verified.

6- The order and payment details is sent: card holder sends the order and payment details to the merchant along with the card holders digital certificate.

7- The merchant request payment authorization: the merchant forward the payment details sent by the card holder to the payment gate way and request the payment gateway to authorize the payment .

8- The payment gateway authorize the payment .

9- The merchant confirms the order.

10- The merchants provides goods services.

11- The merchant requests payment: the payment gateway interacts with the various financial institution such as the issuer , acquirer and the clearing house to effect the payment from the card holders account to the merchants account.

This steps appears in fig (3.3)

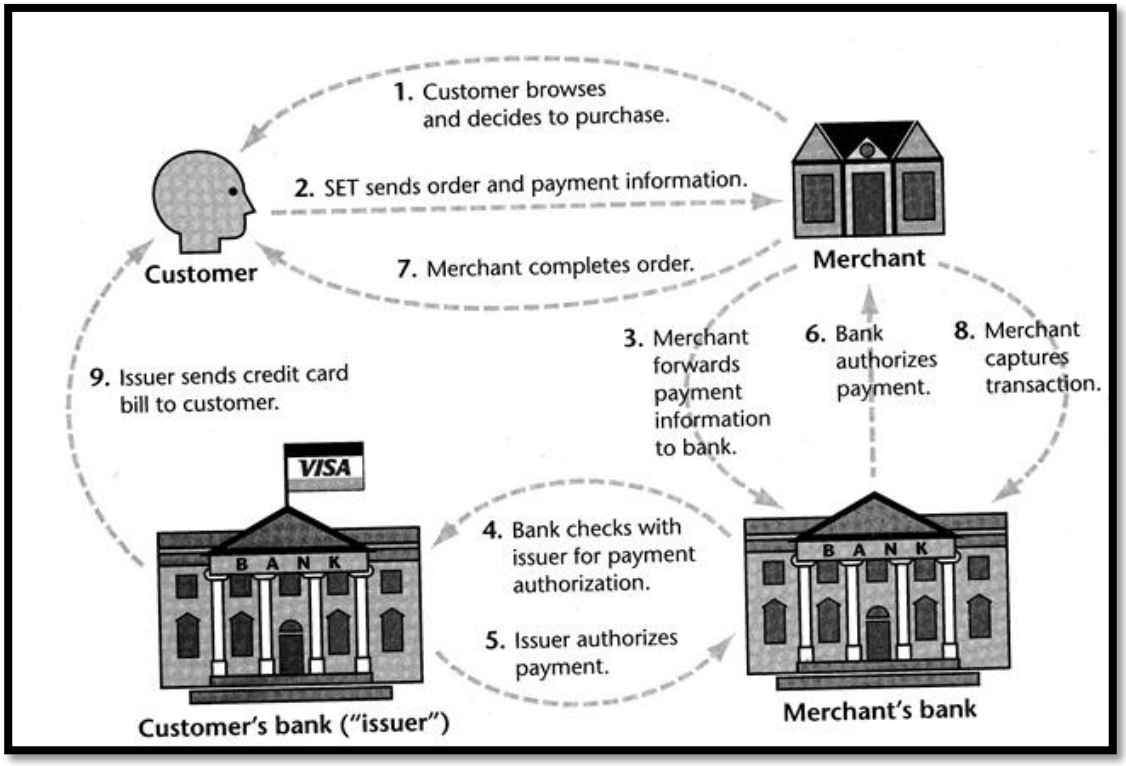


Fig (3.3) SET Process

3.2.3. SET internals:

The major transaction supported by SET is: purchase request, payment authorization, and payment capture.

3.2.3.1. Purchase request :

1- **Initiate request:** as shown in Fig 3.4 **,** In order to send set messages to the merchant the card holder should certificate the merchant.

There are three agencies involved (Financial institution , certification authority and payment gateway)

Fig (3.4) initial request

Initiate response : as shown in Fig 3.5

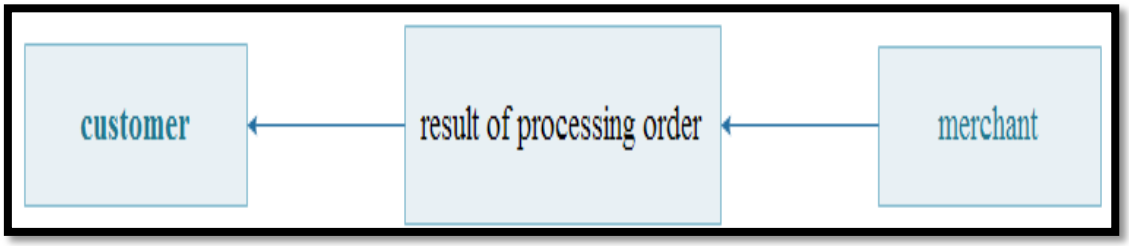


Fig (3.5) Initial response

As you can see in fig 3.4 The purchase response message includes message acknowledging the order and it references the corresponding transaction number, the merchant signs the message using its private key, the message and its signature are sent along with the merchants digital certificate to the card holder.

3.2.3.2. Payment authorization:

The payment authorization step happens when the merchant sends the payment details to the payment gateway, the payment gateway verifies these details and authorizes the payment

1- **Authorization request :** as shown in Fig 3.6

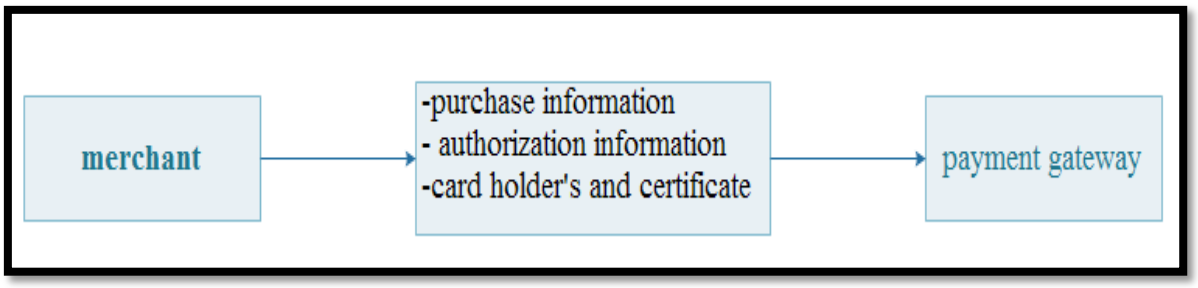


Fig (3.6)Authorization request

2- **Authorization response :** as shown in Fig 3.7

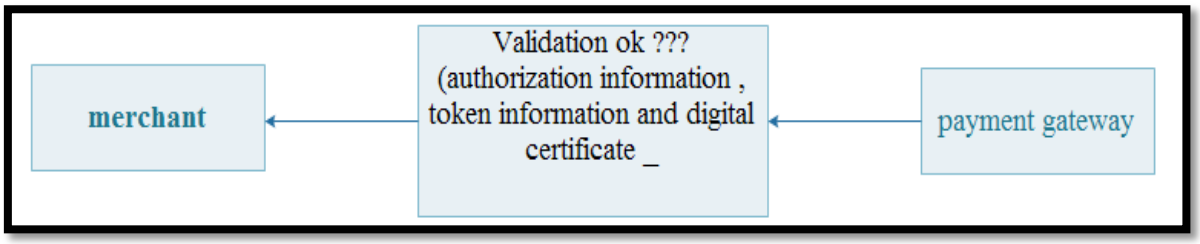


Fig (3.7) authorization response

With this authorization from the payment gateway the merchant can provide goods or services to the cardholder

3.2.3.3. Payment capture:

1- **Capture request :** as shown in Fig 3.8

Here the merchants generates ,signs and encrypt a capture request block that include the payment account and transaction id

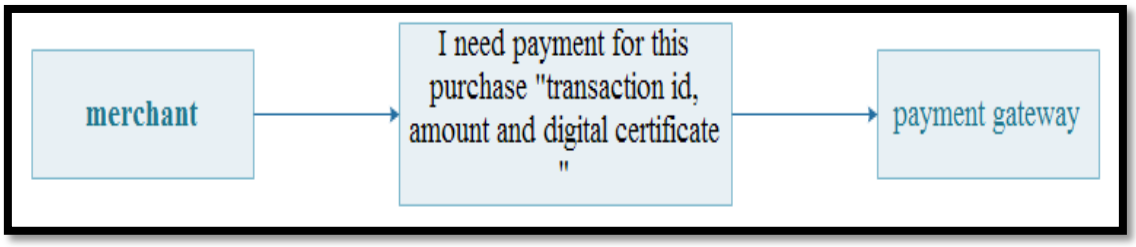


Fig (3.8) capture request

This request result in a funds transfer to the merchant account

2- Capture response :

In this step ,the gateway notifies the merchant of the payment as you can see in fig (3.9)

Fig (3.9) capture response

3.2.3.4. SET Model :

Fig (3.10) shows the simplified SET model for atypical purchase transaction

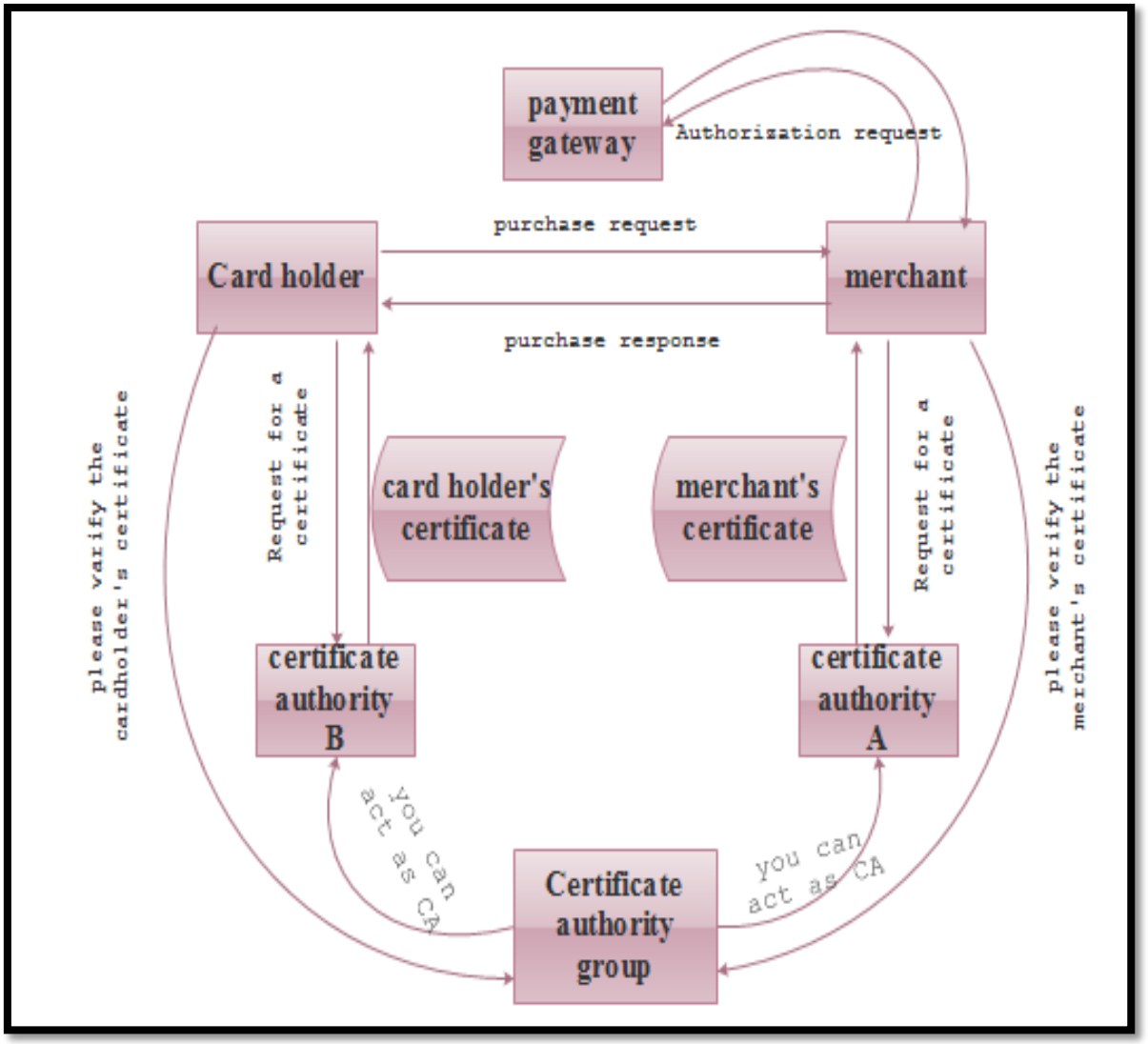


Fig (3.10) summary flowchart of SET model

The three main parties involved in the actual transaction are: card holder, merchant and payment gate way.

3.3. SSL versus SET:

Table (3.1) SSL Vs SET

Issue	SSL	SET
Main Aim	Exchange of data in an encrypted form	E-commerce related payment mechanism
Certification	Two parties exchange certificate	All the involved parties must

		be certified by a trusted third party
Authentication	Mechanisms in place , but not very strong "only merchant authentication"	Strong mechanism for authenticating all the parties involved " mutual authentication"
Risk of merchant fraud	Possible , since customer gives financial data to merchant	Unlikely since customer give financial data to payment gate way
Risk of customer fraud	Possible , no mechanisms exists if a customer refused to pay later	Customer had to digitally sign payment instructions
Action in case of customer fraud	Merchant is liable	Payment gateway is liable
Practical usage	High	Low at the moment , expected to grow
Mobility	Good , can be used in any machine	Fair restricted on computer install SET certification
Efficiency	Good	Fair , due to the complex cryptography
Popularity	Very adopted	Not very adopted

This table tells us that SET is standard used in complex authentication mechanism . However , there is no such mechanism for SSL. Data is transferred securely in SSL however this is not possible using SET.

The whole point is where's SSL is was created for exchange secure messages via the internet ,SET was specifically designed for secure e-commerce transaction

3.4. 3D Secure protocol:

In spite of its advantages SET has one limitation ,it doesn't prevent a user from providing someone else's credit card number . the credit card number is protected from the merchant. However how can we prevent card holder from using another

person's credit card. Consequently a new protocol developed by visa called 3D secure.

The main difference between SET and 3D secure is that any card holder that wishes to participate in a payment transaction involving the usage of 3D secure protocol has to enroll on the issuer bank 's enrollment server, that is before card holder makes a card payment, she must enroll with the issuer bank's enrollment[14]. This process is shown in fig(3.11)

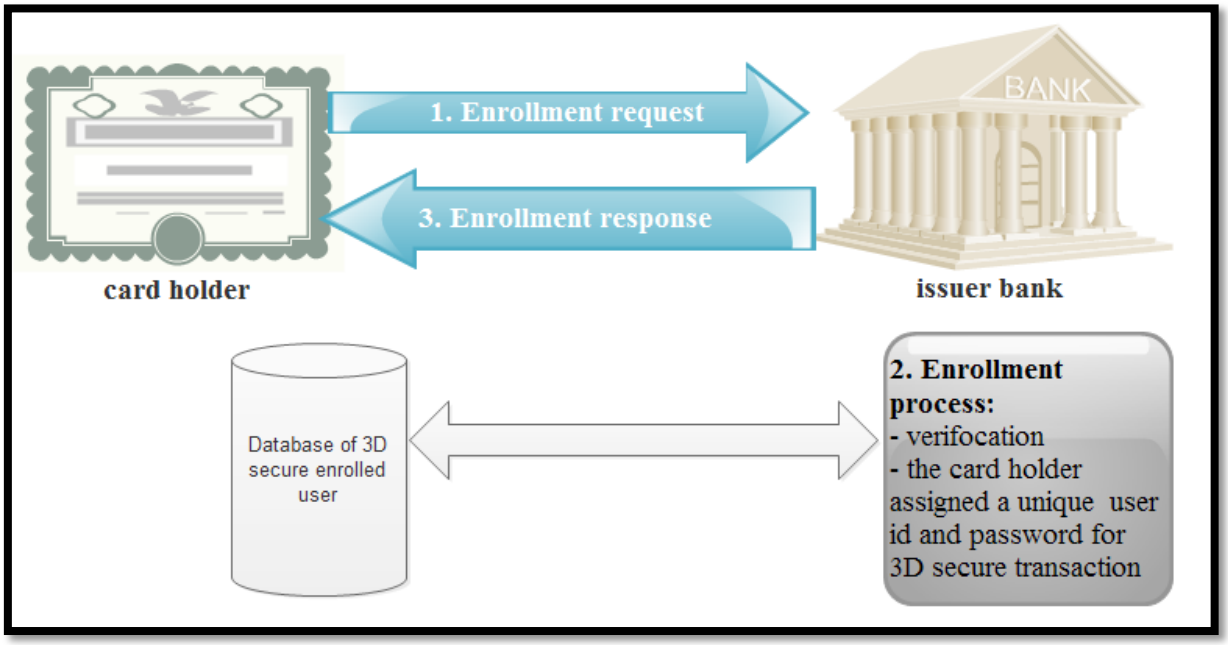


Fig (3.11)3D secure protocol

Chapter Four

QR Code

Whether you are in a coffee shop, a retail store or reading a magazine, you probably can’t help notice the black and white squares with funny patterns on products, billboards and ads. These little squares with funny patterns are called QR codes (Quick Response) codes. These are not new, they have been around for quite some time. But still, very few know how to use them and how they would benefit from doing so.

4.1. Overview of QR codes:

QR codes--barcodes that when read by smartphones take users to online content Developed initially by an auto parts manufacturer in Japan to track parts in its production plants, QR codes have been used for years in Asia for marketing purposes and have been gaining popularity in North America over the last year--especially as smartphones gain wide public acceptance.

It's easy to install a QR code reader application on a smartphone, and these apps are readily available and often free of charge from the various app stores

The Quick Response Code was developed in 1994 for the automotive industry by a Toyota subsidiary. The QR code is a 2 dimensional barcode that can be read optically, for instance using a mobile phone camera. The code can contain data such as web site URLs, product descriptions or v-Cards (electronic business cards). Today QR codes are primarily used for advertising, linking printed media with online media (such as web sites, YouTube videos or online product brochures). Another usage area for QR codes that is growing in popularity is for mobile payments. Using QR codes is free, it doesn’t require any form of license. QR codes is not the only way to link the printed and online world, other technologies include Microsoft Tags and NFC (Near Field Communication) were used .

4.2. What is a QR code?

A QR code is a two-dimensional code (2D code, matrix code), this means it contains data not only in one dimension (e.g. horizontally from left to right like the barcodes on the products in e.g. your grocery store) but also in a second dimension (vertical and horizontal). The acronym QR is short for “Quick Response”.

QR codes are also often called 2D barcodes. However, this notation is not correct, because it means “a two-dimensional code consisting of bars” although a QR code consists of pixels (so-called “modules”) instead of bars.

The QR code was invented by the automotive industry. Toyota asked their supplier Denso Wave to develop a barcode to safely and easily identify components.

QR generators were originally used in industrial applications. Therefore, they had to be easily printable in form and size as well as staying legible when partially destroyed or dirty.

Like other codes, the QR code symbol can be captured with imaging devices like a camera and then digitally processed. A software prepares the captured image data until it can be algorithmically processed according to the QR code standard so the QR code content can be read.

Because of the excellent error correction (they can be read even if up to 30 % of the surface gets destroyed) and the high memory capacity (in comparison with other bar codes), the QR code also gained traction outside the automotive industry. Modern mobile phones are powerful enough to run QR code reading software and also usually provide a camera. This combination brought up a variety of possibilities to use the QR code to easily transfer data without typing to the peoples new communication center, the smartphone. Therefore, a widespread use of QR codes became possible with the recent smartphone boom and the increasing spread of mobile internet.

4.3. History of QR code:

A QR code is essentially an enhanced version of the average barcode. However, they can hold roughly 350 times the amount of information that could be stored on a typical one dimensional barcode. Since QR codes can store information in two directions, they are considered a matrix type or 2D code. QR codes have been used in other countries, such as Japan, for many years, but are just now becoming popular in the United States. It is likely they will spread to worldwide everyday use over the next few years. The summary below provides an idea of the timeline of code creation.

1952 – The first patent is issued for a barcode type device to Joseph Woodland and Bernard Silver. However, this was originally for a circular barcode which rarely saw any use.

1966 – The barcode sees its first commercial use, although lack of industry standard caused problems.

1970 – The Universal Grocery Products Identification Code (or UGPIC) was created to standardize the industry. The Monarch Marking company manufactures the first bar code reading equipment for retail use.

1973 – Over the next few years, the UGPIC was transformed into the UPC code which we all know today.

1974 – The first UPC scanner is installed in a supermarket in Ohio.

1981 – The United States Department of Defense begins using the code to identify all items made for the military.

1986 – Companies like FedEx began using barcode and handheld scanners to track packages.

1988 – Intermec Corporation creates the first 2D barcode.

1994 – The QR code is invented by the Denso Wave company to track the vehicle manufacturing process.

2000 – The first smartphone was released by Ericsson, the R380. At this point, it had much more limited capabilities than smartphones seen today.

2001 – Palm released the first phone to be capable of web browsing.

2010 – The first QR code scanner and reader applications are released for a variety of smartphone platforms in the US.

2011 – QR codes begin to gain prominence in America thanks to some large company campaigns such as Best Buy and Macy's.

As you can see the timeline for the usage of QR codes is really just beginning. Who knows where they will take us in the next ten years. At this point, we can only wait and see. However, what is clear is that they are becoming more and more prominent with each passing year, which is why they could become the key to a successful marketing campaign for your business. Now is the time to stake your claim as a QR code marketer before your competitors have the chance.[20]

4.4. versions of QR code :

There are 40 different versions of QR codes with different data capacities. Version 1 consists of 21 X 21 modules from which 133 can be used for storing the encoded data. Version 40, which is the largest QR code, has 23,648 modules which can be used for storing data. This practically means that it can hold up to 4296 alphanumeric characters [21], [22]. Here we use as an example version 2,as shown in Figure (4.1), which is the size that is most widely used, and based on [23], [24], [25], [26] analyze the structure of theQR Code.-[27]-

(1)Finder Pattern: The three identical structures that are located in the upper corners and in the bottom left corner enable the decoder software to recognize the QR code and determine the correct orientation. These patterns also allow 360 degree (omni-directional) high-speed reading of the code. These structures consist of a 3 X 3 black square surrounded by white modules that are again surrounded by black modules.

(2) Separators: The white separators that surround the Finder Patterns have width of one pixel and make it easier to distinguish the patterns.

(3)Timing pattern: A sequence of black and white modules that help the decoder software to determine the width of a single module.

(4) Alignment Pattern: This pattern allows the QR reader to correct for distortion when the code is bent or curved. The alignment pattern appears on version 2 and higher and the number of alignment patterns used depends on the version selected from the encoding.

(5) Format Information: This section consists of 15 bits and contains the error correction rate and the selected mask pattern of the QR code. The error correction level can be identified from the first two modules of the timing pattern as appear in figure (4.2). The format information is read first when the QR code is decoded.

(5) Data: After the data is converted into Reed-Solomon-encoded data bits, it is stored in 8 bit parts (code words) in the data section.

(6) Error Correction: The data code words are used in order to generate the error correction (EC) code words, which are stored in the error correction section.

(8) Remainder Bits: This section contains empty bits if the data or the error correction bits cannot be divided into 8 bit code words without a remainder.

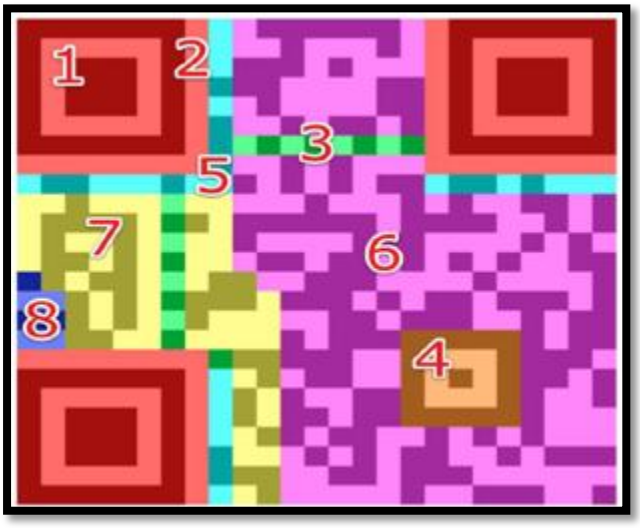


Fig 4.1:Structure of QR code version 2 [27,28]

QR codes are able to encode different types of data, such as numeric, alphanumeric, binary, Kanji or control codes. Another big advantage of QR codes is that they are readable from different angles and the data can be decoded successfully

even if the code is partially dirty or damaged. This is because of the error correction that QR codes have[11]. There are four different error correction levels; Low(L), Medium(M), Quartile(Q) and High(H)(see also Figure (4.2))which can tolerate up to 7%, 15%, 25% and 30% damage, respectively. The error correction level along with the type of encoded data influences also the capacity of the QR Code. Higher error correction levels increase the percentage of code words used for error correction and thus decrease the amount of data that it is possible to be stored in a code. That is the reason why the error correction level L is usually preferred. An additional feature of the QR codes which increases the contrast of the picture and thus helps the reader software to decode the QR code is called masking. With masking, the generated QR codes have an equal distribution between black and white modules. The appropriate mask is automatically chosen by the encoding software while creating the QR code.-[28]-

Fig 4.2:Error correction level of QR code

4.5. Uses of QR Codes:

QR codes are used to store contact information, geo-location data and text. Nevertheless, the most common usage is encoding URLs. The abilities that QR codes have were discovered very fast and, along with the increased use of smartphone, led to wide use of QR codes[30]. The industry of marketing is widely using QR codes as a supplementary way of advertising.[31]. Customers are able to purchase a product

or pay for a service through a QR code since some companies have adopted the so called “one-click” payment [32]. In this case, a customer that wants to buy a product uses a QR code software reader on his smartphone to scan the QR code that is included in the promotional poster of the product. Then he/she is led either to an intermediate payment agent or to the company’s web page to purchase the product. PayPal, which is one of the biggest payment companies, has already adopted this payment practice in some countries. Of course, security issues arise especially when someone transfers money using this method.

Furthermore the versatile use of the QR Codes can be confirmed by the numerous uses that are presented in the literature. In [36] QR codes have been used for physical access control in combination with other security enhancing methods. In their paper Kao et al. proposed a safe authentication system by combining QR codes and the One Time Password technique (OTP). Their design includes a main server which holds the user information, a mobile application that generates QR codes, and a client PC with a camera in order to scan the QR code. In order to be authenticated, the user has to show to the client PC the QR code that the mobile application on his smartphone created. This QR code actually encodes an encrypted password, which was generated by the main server. This authentication scheme offers a good level of security; however, there are still some security issues on this model that remain open.

QR codes have also been used as a means to enhance digital government services in order to effectively distribute valuable information to the public [37]. In this case, QR codes are used to increase citizen participation and provide an enhanced experience and make the information exchange more interactive. Scanning a QR code can help to navigate through park trails by presenting maps to the users. Furthermore they can act as a supplemental material for education since they can be used with games that reward the active users that participate in scientific exploration competitions. QR codes were also proven to be an ideal means when it comes to sharing information between people who participate in the same social event [38] or when the goal is to trivially and effectively share information in order to support the learning process [18],[19]. Furthermore, interesting and creative uses of QR codes are presented in [40] and [39] where QR Codes are used as a surface on which an

augmented reality application is deployed and as a result, impressive 3D virtual objects are produced and displayed to the user.-[27]-

, so in summary QR code can be used in the following fields :

- **Manufacturing (**Product traceability, Process control, Order and time tracking, Inventory and equipment management)
- **Warehousing and logistics (** Item tracking)
- **Retailing (**Point-of-purchase product identification, Sales management, Inventory control)
- **Healthcare(**Medical records management, Patient identification, Medication tracking, Equipment and device tracking)
- **Life sciences** (Specimen tracking)
- **Transportation (**Fleet management, Ticketing and boarding passes)
- **Office automation (**Document management)
- **Marketing and advertising**(Mobile marketing, Electronic tickets, coupons, payments and loyalty, programs)

Mobile marketing has been very popular in Japan, Korea and the Netherlands for several years, and has recently seen rapid growth in North America, where the QR Code is increasingly appearing in print and online advertising, as well as on signs, billboards, posters, business cards, clothing and other items. By scanning a QR Code with a smartphone, consumers can be connected to a relevant Web page or receive targeted marketing messages such as a special offer, discount coupon, product or store information, etc.

In addition, scanners are now available that are specially designed to read a QR Code displayed on the LCD screen of a smartphone. The code can contain a user's electronic ticket or coupon, electronic payment information, loyalty-program identification, etc. –[39] –

4.6. How QR code work:

Learn how QR codes work and why they are able to hold so much information and why custom QR codes are possible.

A person or company, uses a QR code generator to make a QR code that leads to readable, interesting content which they post somewhere it is likely to get scanned. When a consumer comes along, they take out their smart phone, open the QR reader application that came preinstalled on their phone or they downloaded from some kind of application store, and scan the code. The consumer spends more time on the company's page and is more likely to make a purchase or sign up for something, or interact with the company or person in some way then someone who saw a URL or a catch phrase in an ad. That's the essentials.

But what about the technology behind QR codes, how does it work?

QR codes are a lot like the UPC barcodes that are found on every item in the grocery store. The difference between UPC barcodes and QR codes is that QR codes hold information in both the vertical and horizontal directions, while UPC barcodes only hold information only in the horizontal direction. This means that QR codes can hold a lot more information. Approximately 350 times more information.

This information is held in the modules of the code. (The black and white dots.) There are 40 “Versions.” The word version refers to the size of the code symbol in modules. A version one code is 21 modules by 21 modules. A version 40 code is 177 by 177. To go up a version, you add four modules to each side of the symbol. The more modules a code has, the more information it can store.

The physical size of a QR code can be adjusted by changing the size of its modules. This is usually the method that QR code generating sites use to change the size of the QR code symbol.

QR codes can generate a lot of traffic and purchases for your company's website or product, or for your project, if you use them wisely. You could lose potential customers if scanning your QR code is a disappointing experience. To make your QR count, all you have to do is follow a couple of simple guidelines.

1. Always check your code before you get it printed up. Make sure it works and...

2. if your QR code is a link, make sure it is to a website that is optimized for mobile viewing.
3. Make sure your audience knows what to do with your code. If you live in an area that is unfamiliar with QR codes write, “Scan me with your smart phone's QR reader!” underneath your code. You might even want to add instructions on how to download a QR code reader.
4. Place your code in a good location. Some considerations for this include visibility and connectivity. A store front window might be ideal, because after hours, people can pass by your shop, scan your code and shop online.
5. Be sure to offer motivation for scanning your code. Have your code link to a coupon for your product or brand, or to exclusive content like photos or videos. There are a lot of options out there for this, but your potential customer is more likely to stay on your page, and therefore more likely to make a purchase, if they have something interactive to do.
6. If there is plain text in your ad, let your QR code content be different. The redundancy of seeing the same flyer you scanned on your cell phone screen makes users feel like they wasted their time.[40], [41]

4.7. QR Codes Are Mobile Gateway for Bank Marketers:

As the use of smartphones increases, more and more marketers are leveraging QR, or quick response, codes to drive prospects and customers to promotional content or to expand a conversation. While usually a black and white square, QR codes can also be colorful and can have patterns or logos embedded in them and around them, as long as the code itself works properly.

To access, the viewer only needs to download one of several free QR code reader apps on to their smartphones (some phone are already loaded with this application). When the viewer sees a QR code on a poster, billboard, print advertisement or even on a product itself, they focus their camera on the image and the application will recognize the code and automatically open up the link to an offer, video or other unique content in the phone’s browser giving the marketer the ability to share

information or offers immediately at a very low cost (marketers can generate QR codes for free).

While many QR codes are general in nature and used in mass channel marketing, these codes can also send a person to a landing page to collect additional insight before sending them to the content or a personalized QR code can be generated to deliver personalized messages on direct mail, email and other direct channels. Since the QR code is unique and tied to a specific recipient, the marketer will have the ability to see who responds to a marketing piece and when. This type of data could then be used to further refine and personalize marketing messages or for targeted follow-up campaigns.

Other benefits of this tool include:

- **Anytime, Anywhere Marketing -** Since any smartphone can decode and special software is not needed, your message can be made available anywhere a person carries their phone.
- **Channel Shift -** QR codes make it easier to move from mass media or even print based marketing to the web increasing the effectiveness of a campaign and integrating media.
- **Tracking -** QR codes can measure how many people are using the code and at what time. By having easily traceable analytics, firms can view results and know if their QR code campaign is successful. If using personalized QR codes, this enhances the value of the insight to the household or customer/prospect level.
- **Cost Savings -** Instead of continuously reprinting promotional or sales material, a QR code can be used to direct a prospect or customer to continuously updated content or offers.

There are some drawbacks, however. For instance, not everyone has a smartphone or is familiar with QR codes, and scanning is not always intuitive. Therefore, QR codes should usually be accompanied with text such as, “Scan with your barcode scanner on your phone.”

QR codes are used in banks to leverage customer's interactivity and immediacy

Some banks use QR codes in conjunction with billboard or display advertising where space is limited and also to provide additional information.

The key to using QR codes is that the rewards one gets for scanning a code need to be valuable. This form of marketing works best in conjunction with a special offer not available elsewhere or to deliver unique content when customers or prospects are not in front of their computer. In other words, QR codes should not be used to simply take customers to more printed material.

Here are additional ways banks could leverage the power of a QR code:

- Supplement billboard, print or branch marketing with video content that more fully describes a promotion or provides a special offer.
- As a replacement or supplement for a traditional product brochure rack in a branch allowing for product offers and continuously updated product information.
- Link to bank spokesperson or other representative of influence in the bank (economic reviews, annual shareholder meetings, etc.).
- Promotional offer for mobile banking customers in branch or on website.
- ATM screen integration to provide expanded information or offer instead of traditional receipt printout.
- Supplemental information in conjunction with a direct marketing campaign (sweepstakes entry, branch locator, video program description).
- Updated rates and/or competitive grids and linkage to online financial management tools.
- A means to capture permission-based mobile phone numbers, email addresses and other customer insight.

4.8.QR code benefits:

The QR Code's unique design gives it many unique advantages and benefits, including:

- **Fast, omnidirectional scanning:** Position-detection patterns in three corners of a symbol allow the QR Code to be read from any angle within 360 degrees, eliminating the need to align the scanner with the code symbol.
- **High-capacity data storage:** A single QR Code symbol can contain up to 7,089 numerals—over 200 times the amount of data as a traditional 1-D barcode.
- **Small size:** A QR Code can hold the same amount of data contained in a 1-D barcode in only one-tenth the space.
- **Error correction:** Depending on the error-correction level chosen, a QR Code symbol can be decoded even if up to 30% of the data is dirty or damaged.
- **Many types of data:** The QR Code can handle numerals, alphabetic characters, symbols, Japanese, Chinese or Korean characters and binary data.
- **Distortion compensation:** A QR Code symbol can be read even if its image is on a curved or otherwise distorted surface.
- **Linkability:** A QR Code symbol can be divided into up to 16 smaller symbols to fit long, narrow spaces. The smaller symbols are read as a single code, regardless of the order in which they are scanned.
- **Direct Marking:** The QR Code's high degree of readability under low-contrast conditions allows printing, laser etching or dot-pin marking (DPM) of a symbol directly onto a part or product.

4.9. QR code and paypal:

4.9.1. paypal:

- an online payment service that allows individuals and businesses to transfer funds electronically.
- PayPal enables any individual or business with an email address to securely, easily and quickly send and receive payments online.

1.9.1.1. How paypal works:

Figure 4.3. show how paypal work with online merchants (paypal.com) .First ,while shopping online ,a paypal account holder must choose paypal at the checkout/payment page .

Once selecting the paypal option ,the account holder can either use their paypal account or debit/credit card for the purchase . the specified payment method is then sent securely to the paypal holder's account . the option is also given for an account holder to transfer funds to and from the paypal account and primary bank account , once this transaction has been approved the payment process complete .

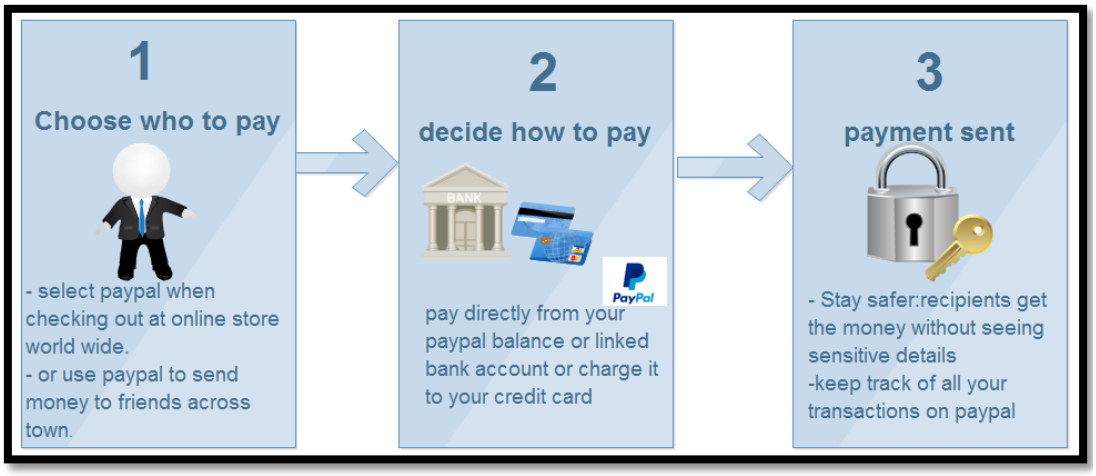


Fig (4.3) How paypal work ?

There are three main account types in PayPal, a personal account, a premier account and the third is a business account. The first, a personal account, is mainly for users who shop online and prefer not to give out their credit/debit card information. This particular account is free to sign up. The second, the premier account, is for individuals who do some selling online and would need to have funds deposited into their account. The last account type is for business use. It allows the company to create a merchant account and accepts all types of payments. PayPal charges a low transaction fee across all types of accounts when money is deposited or a payment is made.[42]

4.9.2. Key features of PayPal:

- **Trust:** PayPal signals trust to participants in online commerce and into payment transactions due to its unique closed-loop business model.
- **Integration:** PayPal operates cross-border and cross-currency, and builds on prevalent consumer preferences which typically differ from one country to another.
- **Interoperability:** PayPal to connect its users across a wide range of available funding sources. PayPal hence embodies a high degree of interoperability, having integrated the most prevalent payment types (direct debit, credit card, credit transfer, prepaid card, invoice, et al).
- **Innovation:** PayPal actively promotes innovation in a number of ways. PayPal has already launched several mobile payment products and solutions. PayPal supports the success of innovative start-ups, acting as a trust factor and thus opening wider markets. PayPal also operates x-commerce, an open platform for developers and innovators, which provides an effective launch pad for viable innovative business ideas.
- **Business development:** PayPal is an effective business enabler, especially for small businesses and startups.
- **loop Closed-:** As an account based, 3-party system, PayPal has control over both ends of a transaction, i.e. can trace both sender and recipient of a payment, and builds a quasi customer relationship with its users. Together with highly sophisticated risk management practices and effective anti-fraud technologies practices, this closed loop allows PayPal to identify suspicious behavior.
- **Data protection:** Consumer privacy and especially consumers' financial information must be protected. PayPal never discloses financial information between the payer and the payee. Only the payment and contact information is transmitted, while all financial information is safely held by PayPal only. This also relieves the merchants, as they do not have the extra burden of safeguarding that financial information.

- **Buyer and seller protection:** Consumers must know that any problems with their transactions will be addressed quickly and fairly in a dispute resolution process. It is important to note here that most transaction issues are the result of honest mistakes or poor communication, not fraud. The provision of a protection scheme and dispute resolution procedures not only benefits individual buyers, but in particular also small businesses.

4.9.3. Paypal and QR code:

There's news today on the PayPal front. The company is working on some new QR features, and one of those features will have some PayPal users excited. Soon, PayPal users will be able to use a PayPal QR code to check out at various retail locations. Interested? Here are the details.

How the QR Codes Will Work:

Basically, PayPal will provide the site's users with special QR codes that are directly linked to PayPal accounts. From there, those codes can be scanned by participating retailers. The money required will then be withdrawn directly from a PayPal account.

Here's a better example:

You walk into a store armed with your smartphone. You access your PayPal screen A participating retailer scans the QR code on your screen You pay for your item and leave the store.

All of this can be done with your smartphone, and none of this takes more than a few minutes to complete. You do have to have funds in your PayPal account, but that is something that's becoming more and more commonplace.

Other Ways to Pay

In order for a merchant to accept PayPal QR codes, that merchant must have updated PayPal software. But, if that update isn't in place, PayPal will also provide users with a four-digit code that can be entered into payment platforms easily.

Another example:

You walk into a retail store with your smartphone The retailer doesn't have updated PayPal software You ask PayPal to generate a four-digit code instead The merchant adds the four-digit number to a system Your item is paid for via your PayPal account You still only need your smartphone to pay for items using this alternate PayPal method. But, there are a few restrictions with the first one being that you have to live within the United States in order to use PayPal's newest payment methods. Another obvious restriction is that merchants must use PayPal in order for this payment system to work.

Availability - Or, When Can You Test it Out?

Dying to try PayPal's latest payment features? PayPal won't be rolling out the new feature until later next year. That's a long time to wait, right? Well, PayPal wants to make sure that the systems are all set up and running smoothly before they are implemented (no glitches).

PayPal has told press that many merchants across the United States will be using the PayPal system. Plus, PayPal is the number one online payment option for many online users, and that means that tons of people will be setting up PayPal apps. If only PayPal would spread to other parts of the globe, this payment system could really take off - and compete with the likes of, say, Square. Of course, there's huge marketing potential here too. PayPal will be working with retailers to implement deals and ads into QR codes. So, you may just get a discount with that latte. It res, right? [43]

4.10. Why QR Code in our model?

The asked Question her is why we will use QR code in our model not NFC nor barcode?

4.10.1. What is NFC code?

NFC (near-field communication) allows two devices placed within a few centimeters of each other to exchange data. In order for this to work, both devices must be equipped with an NFC chip.

In the real world, there are a essentially two ways this works.

Two-way communication: This involves two devices that can both read and write to each other. For example, using NFC, you can touch two Android devices together to transfer data like contacts, links, or photos.

One-way communication: Here, a powered device (like a phone, credit card reader, or commuter card terminal) reads and writes to an NFC chip. So, when you tap your commuter card on the terminal, the NFC-powered terminal subtracts money from the balance written to the card.

4.10.2. NFC and e-payments:

One day, we'll all be paying for things with our phones. In light of the many recent credit card data breaches, now is an especially good time to present a solution that finally shields our wallets from theft and fraud.

The biggest concern around NFC payments is security, but the mobile payment structure is so complex, any hacking or intercepting would be very difficult. To understand why, here's how it works.

After launching the payment application on your phone, the phone is tapped on the credit card terminal and a connection is made using NFC. At this point, you may be asked to scan your finger or enter a passcode to approve the transaction. The transaction is then validated with a separate chip called the secure element (SE), which relays that authorization back to the NFC modem. From there, the payment finishes processing the same way it would in a traditional credit card swipe transaction[51].

4.10.3. NFC and QR code :

Near Field Communication (NFC) is a short-range wireless connectivity technology that enables data transfer through a simple touch of devices, allowing compatible devices within a few centimeters of each other to communicate with each

other. Most people in the London will have used the technology with their London Oyster transport card which uses NFC chips. Quick Response (QR) technology (2D Data matrix barcodes) is a type barcode that can be read by any smart-phone through the phone's camera and a generic, free app that decodes the barcode into data.
In the past 6 months a debate has been growing over whether NFC technology will kill QR codes. NFC offers a more user-friendly interaction with simpler and fewer user steps for interaction (just touch two things together). A comparison of the two technologies makes sense because they both offer a way to trigger interactive content on mobile phones.

Journalists and bloggers word wide are joining in the NFC/QR debate but many often miss the crucial arguments in the debate. In this blog, I'll take a look over the pro's and con's of NFC over QR and argue why I think NFC is a complimentary technology, not a replacement. I'll take a logical look to the industry and predictions within it[52].

4.10.4. NFC Vs QR code Technology

Table 6.1 below compare between NFC and QR code[52]:

Table (4.1)NFC vs QR code[52]

	NFC tag	QR code
Infrastructure	requires special "initiator" hardware that creates an NFC field searching for a "target", a NFC chip that holds data for the device to pick up..	QR codes use the camera already in the phone and only need a small "QR reader" app to enable the device to support the technology.
Production and implementation	To implement NFC a publisher must embed a NFC chip into every target (thing that someone should interact with). For things like Point of Sale	Generating QR codes is simple once you have a generator (a library of code that generates the image from text you enter

	displays and Travel Information Points, NFC will become a logical solution to implement. For direct-mail/business card type applications, where many items are handed out at a low cost, NFC will add a significant cost	) .QR codes can then be printed from free ,quickly and easily .the barriers to adding QR codes are really very low.
Scanning	Difficult to scan as discussed above	much easier to scan. Smart phones will have better cameras (which are the factor holding back fast QR scanning on the older phones). QR reading software will be built into the phone's camera software, meaning no special app is required

4.10.5. QR code VS barcode

What is a barcode?

Barcodes are—simply put—machine-readable fonts. Their "letters" consists of binary symbols that can be read opto-electronically.

There are different barcode standards. Just as a person can read a foreign text as soon as they learned the alphabet and language, a barcode scanner or its software can read a barcode as long as the underlying standard is "understood" (= implemented).

In general, barcodes are used as optical machine-readable labels on objects, containing information about the object on which they are glued. The most popular barcode type is used on the product packaging and can be viewed at every grocery store where they make the Universal Product Code machine readable. Because of

their omnipresence, the terms “barcode” is often used synonymously for this UPC-A barcode symbol, although there are many other barcode types.[19]

Table 4.2 compare between QR code and Barcode

Table (4.2) comparison between QR code and barcode

	QR code	Barcode
Data types	two dimensional codes, capable of storing data horizontally and vertically. Therefore, the QR codes can hold up to 7100 characters of data, rather than the much lower number which barcodes hold. Additionally, the QR codes hold characters, numbers, symbols, text, and control codes. Due to the fact that the codes are horizontal and vertical, they store the same exact amount as the barcode can, but in only 1/10 of the space the barcode requires	one dimensional numeric codes, and they are capable of up to 20 characters. This is simple for keeping track of inventory that leaves and enters a store,
data restoration	can still be scanned. Additionally, when damaged, the QR code can still recover from 30 to 35% of the damaged data, words, or symbols, making the QR code far superior in the capabilities or restoring data, or	When the barcodes are damaged, they are not capable or reading any data, and they cannot be used to scan.

	recovering information	
Scanning data	from anywhere, any distance, and any position. Due to the three positions and the detection patterns on the QR codes (which are located in the three corners of the code), they are going to be read no matter where they are scanned.	the exact position has to be perfect, otherwise they will not scan; this slows down the speed of clerks at busy stores, and in some cases, requires them to manually input the codes, if the code is extremely wet, or may be dirty due to where the product was located in the store.
speed and precision	far superior to the traditional barcodes	**Slow**
structured appended feature	the information can be segmented, in up to 16 smaller sized squares. In turn, the QR codes allow any information to be stretched out on to an object, allowing the QR code to be printed out on smaller, and narrower areas	data cannot be broken up by the reader

As appear to you from the above discussion and comparison that the QR code is the code for this generation it give the customer the security , speed, simplicity with ,minimum cost, so our choice was the best and our model will be very successful to use

Chapter Five

QRG e-payment Model

5.1. Introduction:

The smartphone is the fastest growing device in the world today, connecting consumers to online resources anytime, anywhere. The growth of mobile is creating a new channel for customers to complete the critical financial transactions that drive business. The growth of this channel is a great opportunity to encourage more customers to use e-billing and e-payment programs. Because e-payers pay earlier and more consistently, the more customers that transition to e-payment the more you will enjoy faster collection, reduced payment processing time and fewer late collections. And your customers will thank you for allowing them to pay in a way that is most convenient for them--hassle free, right from the palm of their hand. But how can mobile be integrated with the printed billing process? One convenient and immediate answer is by using Quick Response (QR) codes--barcodes that when read by smartphones take users to online content.

In this chapter we will introduce a new model _QRG e-payment model_ that use e-payment technique with gateway technique together with QR code to simplify e-payment process.

5.2. e- payment processing network:

- **Merchant bank "acquiring bank":** provides internet merchants accounts to enable online credit card or bank account authorization and payment processing.

- **Authorization:** the process by which a customer's credit card or bank account is verified as active and that they have the credit available to make a transaction.
- **Customer:** the holder of the payment instrument such as credit card , debit card, e-check, or bank account .
- **Customer bank:** a financial institution that provides a customer with bank account or any other payment instrument.

The elements involved in the e-payment systems is:

- **Merchant:** someone who owns company that sells product or services.
- **Payment processing service:** a service that provides connectivity among merchants, customers and financial networks to process authorization and payments.
- **Processor:** a large data center that process transaction and settle funds to merchants site on behalf of merchant bank.
- **Settlement:** the process by which transactions with authorization codes are sent to the processor for payment to the merchant.

5.3. The e-payment model with QR code (QRG e-payment model)

5.3.1. Preliminaries:

- **QR code scanner:** Special scanner of QR code of products or you can use your smart phone camera to scan the QR code.
- **Online customer:** a customer is an entity who will buy products by making payment in timely manner.
- **Merchants:** a merchant is a seller who will receive payments made by customer.
- **Banks:** two banks are involved (client bank , and merchant bank).
- Client bank : holds client's bank account and validate customer during account registration.

- **Merchant bank:** merchant bank holds merchant bank account. it is responsible of management.
- **Payment gateway:** a payment gateway is connected to all customers, merchants and banks through internet and responsible for the speed , reliability and security of all transactions that take place in this model.

A Payment Gateway is an e-commerce application service provider that provides tools to process a payment between a customer, merchant and banks over the World Wide Web . It helps secure a purchase and a customer's payment information in a transaction. A payment gateway protects payment information by encrypting sensitive information, such as credit/debit card details, to ensure that information is passed securely between a customer and, the payment processor. Besides encrypting the payment information, a payment gateway also helps in authorizing payments and protect against financial frauds. Many online merchants use payment gateways for its security, reliability and immediate authorization of payment.

You can see the proposed QRG e-payment model on figure (5.1)

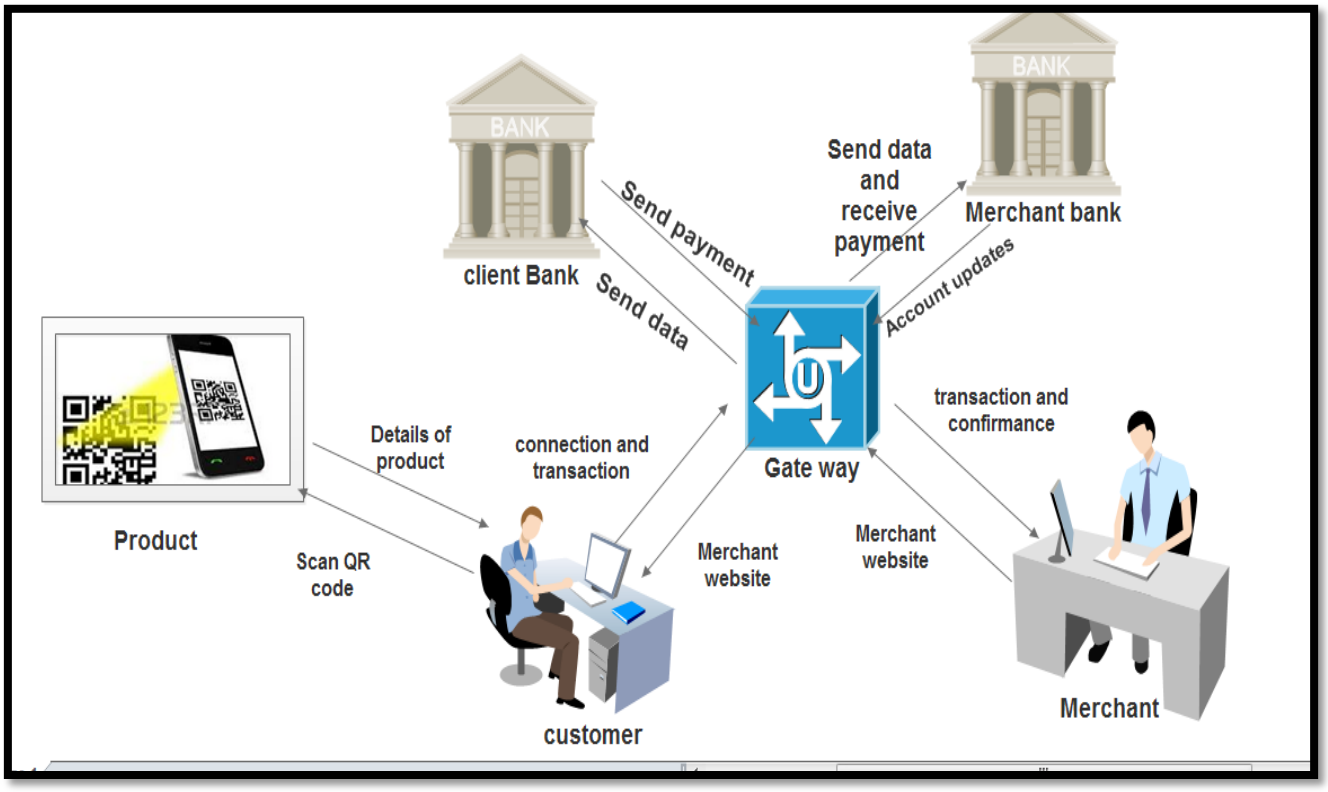


Fig (5.1): QRG e-payment model flow diagram

5.3.2. Framework overview:

As you can see in figure (5.1) ,

There are five interfaces:

- Customer interface.
- Server interface "e- payment gateway".
- Client bank interface.
- Merchant bank interface.
- Merchant interface.

5.3.3. QRG e-payment model algorithms:

1. client algorithm:

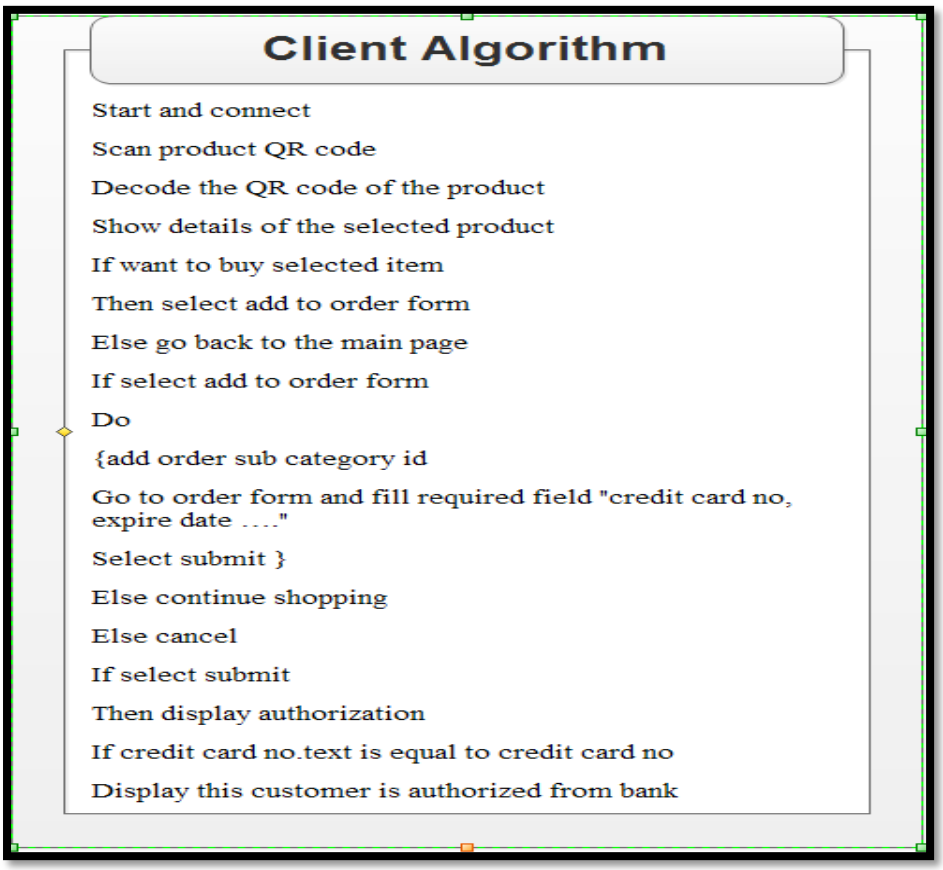


Fig 5.2: QRG e-payment client algorithm

2. Gateway algorithm

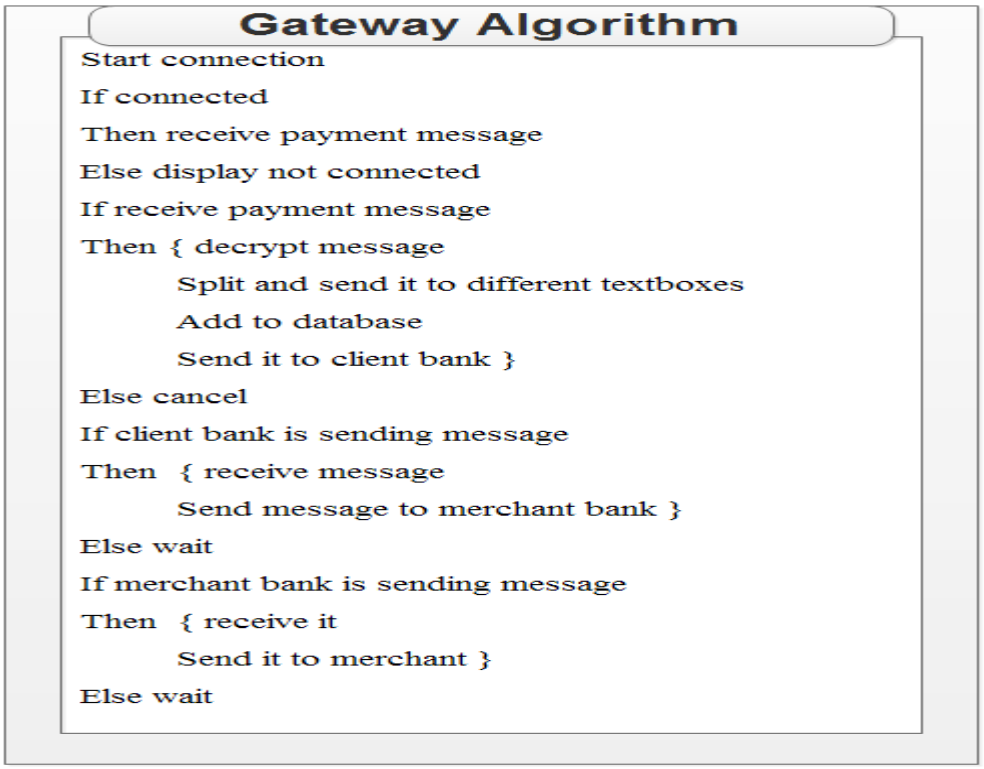


Fig (5.3): QRG e-payment gateway algorithm

4. Client bank algorithm

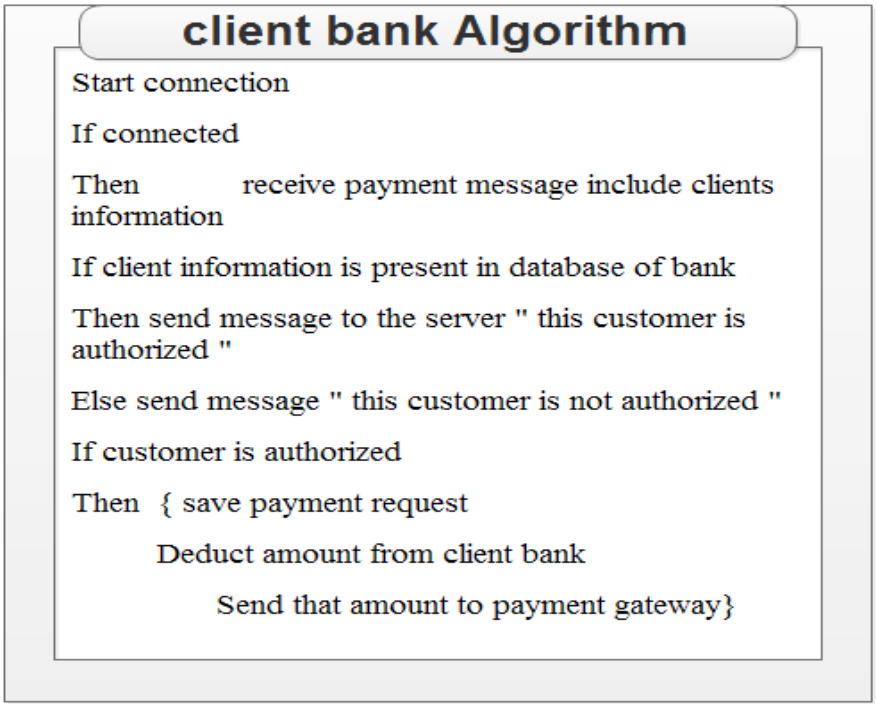


Fig (5.4): QRG e-payment client bank algorithm

5. Merchant bank algorithm

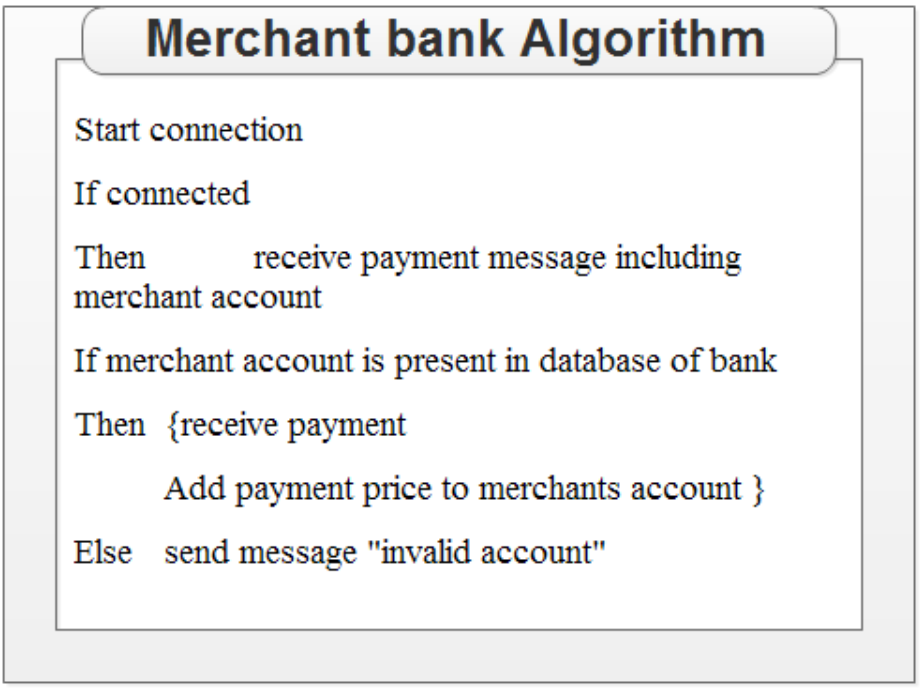


Fig (5.5): QRG e-payment merchant bank algorithm

6. Merchant algorithm

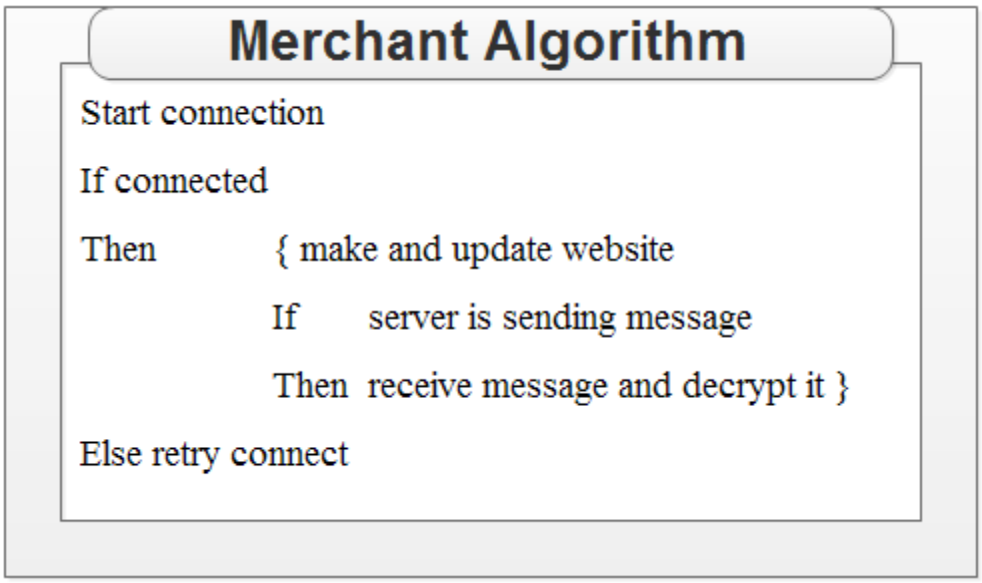


Fig (5.6): QRG e-payment merchant algorithm

This algorithm will appear in flow chart below step by step as in fig (5.7)

5.3.3. flowchart diagram:

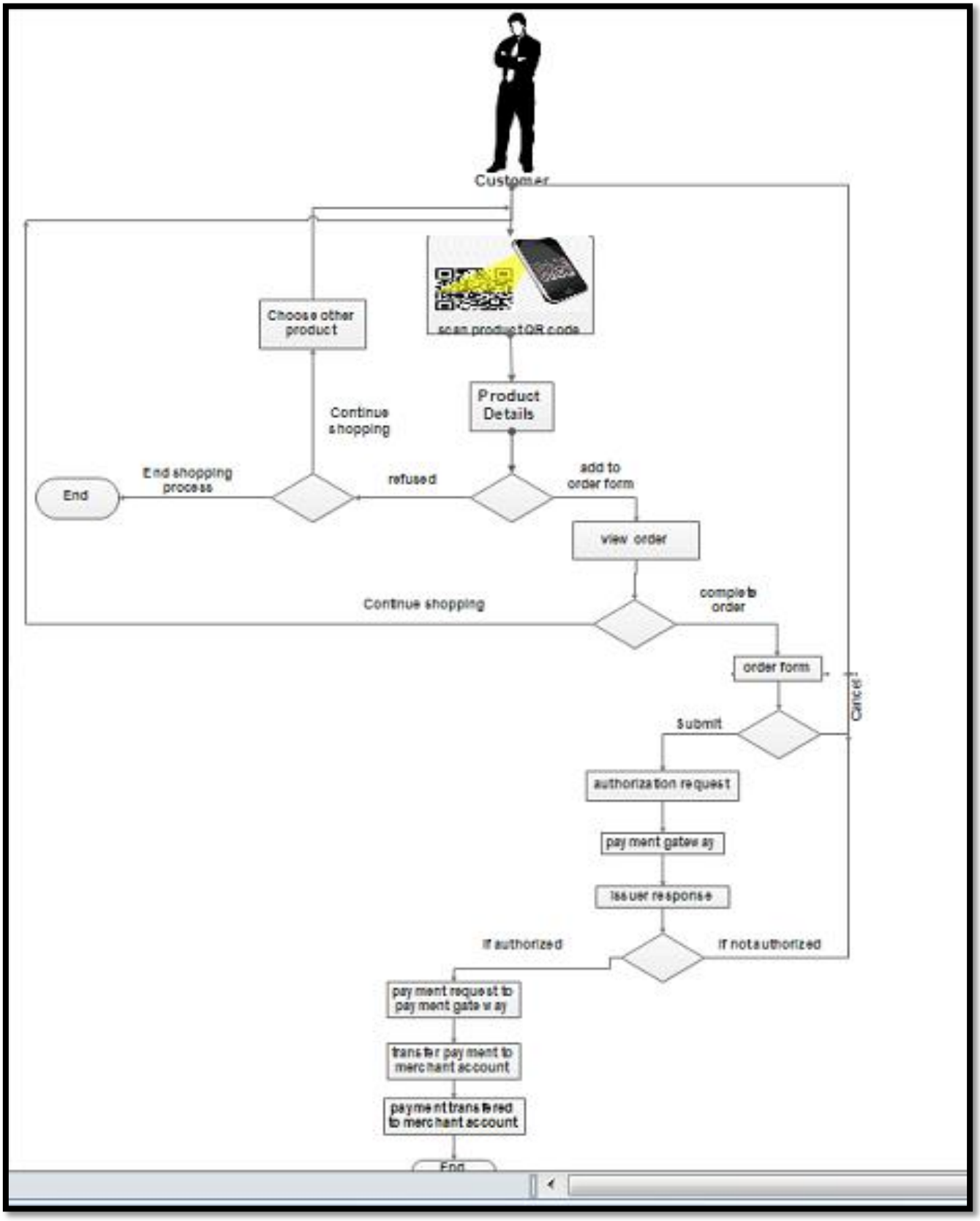


Fig 5.7:QRG e-payment model flow chart

5.3.5. How QRG e-payment model work ?

Payment processing in the proposed QRG model can be divided into three major phases: QR code scanning, authorization and settlement.

5.3.5.1. QR code scanning phase:

Decoding a QR code requires using a QR code scanner. besides commercial scanners including hi-resolution, dedicated devices and hand held scanners, smart phones that have a camera and include a code reader software application can function as a scanner. code reader software applications are freely available for most devices. when application is downloaded, the phones camera toward the code and scan it, the reader application software decodes the code, converts it in to readable text. fig 5.8- visualizes how QR code works.

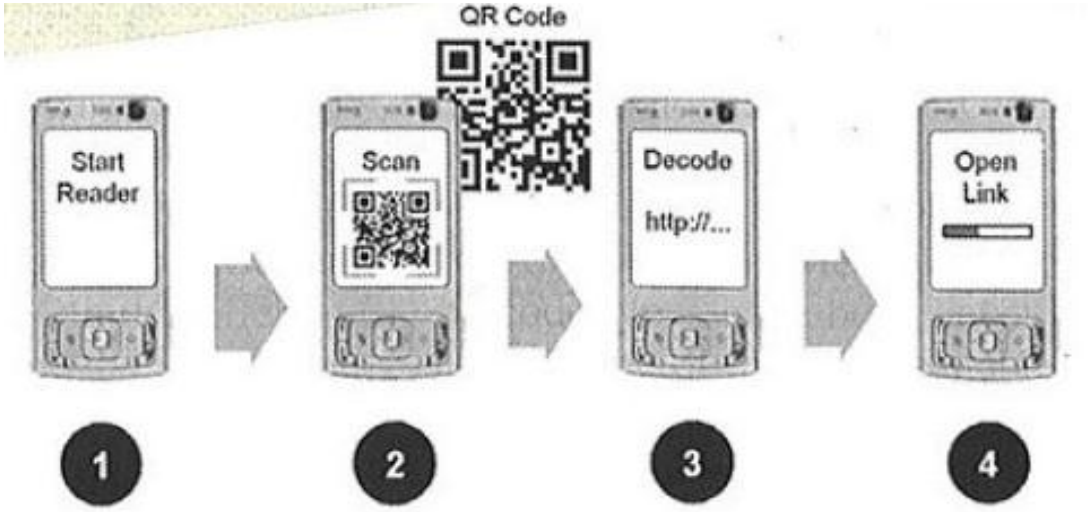


Fig 5.8:QRG scanning phase

In payment scanning phase the customer uses the scanner to scan the QR code of required product the reader of QR code application will decode this QR code to show you the details of this product and you can accept or deny buy this product.

5.3.5.2. Payment Processing-Authorization phase:

1. Customer decides to make a purchase product on Merchant's market by choose product and scan its QR code by scanner or mobile phone camera, and make authorization by inputs credit card information or bank account ….

2. Merchant swipes card and transfers transaction information to a point of sale terminal.

3. Point of sale terminal routes information to the Processor via dial -up connection

4. Processor sends information to the Issuing Bank of the Customer's credit card, or bank account.

5. Issuing Bank sends transaction result (authorization or decline) to the Processor.

6. Processor routes transaction result to the point of sale terminal.

7. Point of sale terminal shows Merchant whether the transaction was approved or declined.

8.Merchant tells the Customer the outcome of the transaction. If approved, Merchant has the Customer sign the credit card receipt and gives the item (s) to the Customer.

5.3.5.3. Payment processing settlement phase:

The settlement process transfers authorized funds for a transaction from the customer's bank account to the merchant's bank account. The process is basically the same whether the transaction is conducted online or offline.

As shown in figure (5.9)

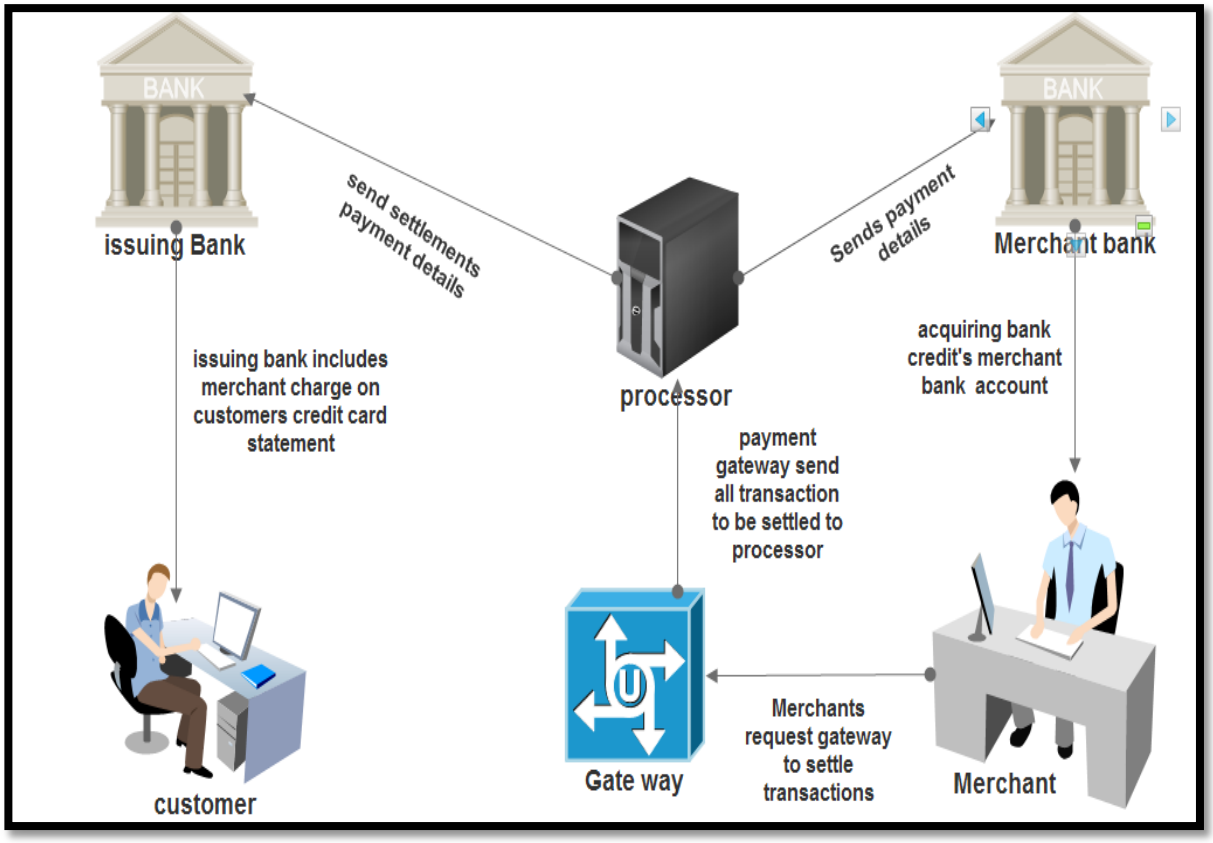


Fig (5.9) QRG e-payment settlement phase

5.4. Why not send payment information to merchants?

The development of e-commerce demonstrated a greater need for payment system to secure customers' financial data when sending it over the Internet. Since then, various payment systems have been developed. But, with the advancement in cyberspace and technology, protecting customers' financial data is not the only issue. Financial frauds reported over the years due to hackers, spammers, fraud merchants and network breaches have become a major concern. To address these problems, current online payment systems follow an approach where customers' payment information is first sent to merchants and then the merchants redirect it to payment gateways. This approach in conjunction with other technologies works well as merchants and payment gateways communicate directly with each other and are aware of customers, purchases and payments .But independently, this approach does not facilitate in protecting customers' financial data from fraud merchants. Instead it makes the entire system susceptible to infringement/ intrusion.

When customers send their payment information (hashed/encrypted) to merchants, they are not aware how that information travels over the Internet and is processed by a merchant. Merchants can save the encrypted/hashed financial information of customers and later decrypt it. It might also be possible that a merchant's server is being compromised and he is completely unaware of it. On the other hand, most banks rely on password-based access and encryption methods to secure customers' data. A bank, however, cannot guarantee that a customer's financial information has not been compromised if that information has travelled through a merchant's server before reaching a payment gateway/bank.

Taking these factors into consideration, we infer that sending customers' financial information to payment gateways via merchants exposes it to additional networks susceptible to information leaks and attacks. Hence, to avoid this vulnerability, we develop a different approach for payment systems in which customers directly send their payment information to payment gateways. This way a merchant gets paid for his sold items without receiving a customer's payment information, not even in encrypted/hashed form.

5.4.1. Design issues when payment information is not sent to merchant

When customers' payment information is sent to a payment gateway via merchants, certain information of the customers along with their purchase and payment details are retained by merchants. The current approach to a payment system allows merchants to store some information related to customers' purchases including some parts of payment information (like credit/debit card type or issuer). This is done so that merchants can prove a transaction's validity or existence in case of dispute and charge backs. When merchants do not obtain any payment information from customers because, customers provide their payment information directly to a payment gateway, several challenges as listed below need to be addressed.

1. For sending a payment, the payment gateway should be able to identify the merchant and ensure his authenticity;

2. validity of a purchase should be determined by a payment gateway before authorizing its payment to merchants;

3. when sending a payment, the payment gateway should ensure that only the rightful merchant receives payment;

4. And most importantly, merchants should be able to obtain purchase information when required and prove the legitimacy of its payment in case of dispute/charge back.

5.5. QRG Model Security:

In our system online transaction system will work with the payment gateway with SSL/TLS"secure Socket layer (SSL) / Transport Layer Security (TLS)". Payment gateway act as a bridge between merchant application host server to bank server and data transferred from merchant application host server to bank server is in encrypted format by using SSL According to Ved Prakash Gulati[45], when an online transaction takes place these functions come in the picture Authorizing, Clearing and Reporting. As firstly when customer wants to buy a product so customer will scan this product QR code and after see the details of this product then will click to buy. If merchant website has SSL certificate then there visitor get know that entering their personal information over the website will be safe and transactions will also be secure. It can be identified by an https prefix (display in browser address bar) which ensures website is protected. The SSL certificate will be issued to encrypt data transfers like customer bank details and to identify that merchant website has matching information on file with the CA. The encrypted data send via payment gateway to bank server where data is decrypted and authenticate (customer detail with bank) transaction details and then bank will give response after validating and depending upon the credit limit, bank will reject or accept the transaction. After this payment gateway then transmits the receipt of bank to the merchant website as report.

Our system will use the e – payment and According to Holly Lynne McKinley[46], Existing Online Payment transaction communication is secured by

using SSL/TLS protocol in order to protect the connection between the customer and the server. However, SSL/TLS protocol is vulnerable to different attacks.

SSL communication follows following steps:

Step 1. Establish Secure Communication:

Customer send https request, the SSL layer initiates a communication handshake channel.

Step 2. The SSL Handshake Channel:

a. The customer's web browser sends the Bank website server its methods of encrypting data with other information like encryption type and other SSL related data.

b. The Server provide its own data like SSL certificate with public key, it is used for encryption as well as other secure sockets layer information.

c. The customer's browser checks the received information like certificate expiration date and valid certificate authority.

Step 3. Completing the SSL Handshake:

a. Now browser creates a "premaster secret" that will be used to encrypt the data for entire session. “Premaster Secret” is a random key that it encrypts using the agreed upon encryption method combined with the server's public key string that it received and sends the new encrypted secret string back to the server.

b. With the new "premaster secret" string, the browser and the web site server create a new "master secret" string and use it to create session keys (long characters strings)that their encryption programs use for the rest of the session to encrypt/decrypt all transmissions . Using Master secret key browser and server both are able to verify that the data did not change in network transmission.

c. Now browser sends a message as start secure communication by using new session key.

d. The web server send back ok response to browser as start secure communication by using new session key.

e. The web server (encrypted communication) verifies to the browser that it is finished securing its part of the session.

The browser and the web server use the session keys to encrypt and decrypt the data they send to each other Existing online transaction systems assume that above SSL steps provide online security for online transaction .But According to Peter Burkholder [3], this secured communication channel has also vulnerability of attacks.

5.5 .1. Security Analysis

The sending of a customer's payment information directly to a payment gateway prevents a merchant from obtaining a customer's sensitive financial information .This protects a customer's payment information from risks of data theft and data infringement on the merchant's side. In this section we show that our approach for online payment is secure and protects both a customer's payment and payment information through security claims in the following ways.

1. Only a registered merchant can obtain an identity token from an Identity Provider and initiate the payment process
   Each merchant in our payment system is required to register with an Identity Provider (IP). A merchant cannot request and receive payment from a customer without an identity token. This is done to secure a customer's payment information and insure that the transaction is being implemented by a registered merchant

2. Only the rightful merchant can verify a transaction and obtain its payment

When a payment gateway receives a request for payment from a customer, it does not authorize the customer's payment immediately to a merchant. It sends the transaction's identity attribute by the merchant to the payment gateway validates the correctness of the transaction. The other reason why a payment gateway verifies a transaction from a merchant is to confirm that a customer's order details and transaction id have not been manipulated and match with the merchant's record.

Let us assume that an attacker captures the transaction check message sent by a payment gateway to a merchant for the verification of a transaction. Since the transaction check message is encrypted with the merchant's public key, it can be decrypted only by the merchant's private key. This prevents an attacker from obtaining the information within the transaction check message. However, even if we assume that an attacker knows the merchant's private key, decryption of the transaction check message does not provide an attacker with any information related to the transaction.

3. A customer's payment information is protected

The main objective of our proposed payment approach is to protect a customer's payment information from being stolen or misused. To achieve this, unlike the current payment approaches, we do not send a customer's payment information to a payment gateway through a merchant. We send a customer's financial information directly to a payment gateway and prevent a merchant from obtaining a customer's financial information even in encrypted form. When a customer shops online, he is exposed to various risks on the Internet. To avoid these risks, a customer provides his payment information to a payment gateway directly on a payment gateway's server. Payment gateways are more secure and trustworthy. They also communicate with banks for authorizing and issuing payments.

Hence, providing a customer's payment information directly onto a payment gateway's server will protect a customer's payment information from being tampered

4. Merchants can prove the validity of their transactions in case of dispute/charge backs.

When Current payment approaches allow a merchant to store some details of a customer's debit/credit card to prove the validity of a transaction. Our payment approach, however, restricts a merchant from obtaining any part of a customer's payment information.

In security analysis 1) and 2) we proved that a fraudulent merchant cannot initiate a transaction and obtain a customer's payment. Likewise, a merchant does not obtain any financial information of a customer which makes it very unlikely for a customer's payment information to be compromised from the merchant's side. Therefore, the only dispute a customer would have in our payment system is regarding a transaction's order details and payment amount.

Therefore, to avoid disputes and charge backs, our proposed payment system validates all required information before sending a customer's payment to a merchant. However, in case of a dispute, a merchant provides all purchase details of a transaction to a payment gateway for re-verifying them with the information provided by a customer. This also proves that the merchant does not require a customer's payment information to prove the genuineness of a transaction in case of dispute.

5.6. Conclusion:

As you can see from our model the use of QR code in e-payment or marketing will enable the customer to make Direct Marking, The QR Code's high degree of readability under low-contrast conditions allows printing, laser etching or dot-pin marking (DPM) of a symbol directly onto a part or product.

And the use of Electronic Payment Gateway will make the process more secure. At first it's checked if the customer is authorized one or not then the whole transaction takes place. The electronic payment gateway is made secure enough that any authorized customer can easily trust on it and fearlessly or confidently make payments over the Internet.

Chapter Six

Evaluation and remarks:

The proposed QRG (e-payment model with QR code) will be very simple, secure and fast technique that can be used in e-payment process.

, In this chapter we will evaluate our proposed algorithm and comparing it with other techniques that can be used in the same field side.

And to evaluate our system we use GNS3 program to simulate our model and then take the result from GNS3 simulator and draw and simulate it using Mat lab program.

6.1. GNS3 program:

GNS3[63] is a Graphical Network Simulator that allows emulation of complex networks. You may be familiar with VMW are or Virtual PC that are used to emulate various operating systems in a virtual environment. These programs allow you to run operating systems such as Windows XP Professional or Ubuntu Linux in a virtual environment on your computer. GNS3 allows the same type of emulation using Cisco Internetwork Operating Systems. It allows you to run a Cisco IOS in a virtual environment on your computer. GNS3 is a graphical front end to a product called Dynagen. Dynamips is the core program that allows IOS emulation. Dynagen runs on top of Dynamips to create a more user friendly, text-based environment. A user may create network topologies using simple Windows ini-type files with Dynagen running on top of Dynamips. GNS3 takes this a step further by providing a graphical environment.

6.1.1. Run and configure GNS3:

The first time GNS3 is run, the setup wizard shown in fig (6.1) will be displayed. This can be used to perform initial configuration of the simulator.

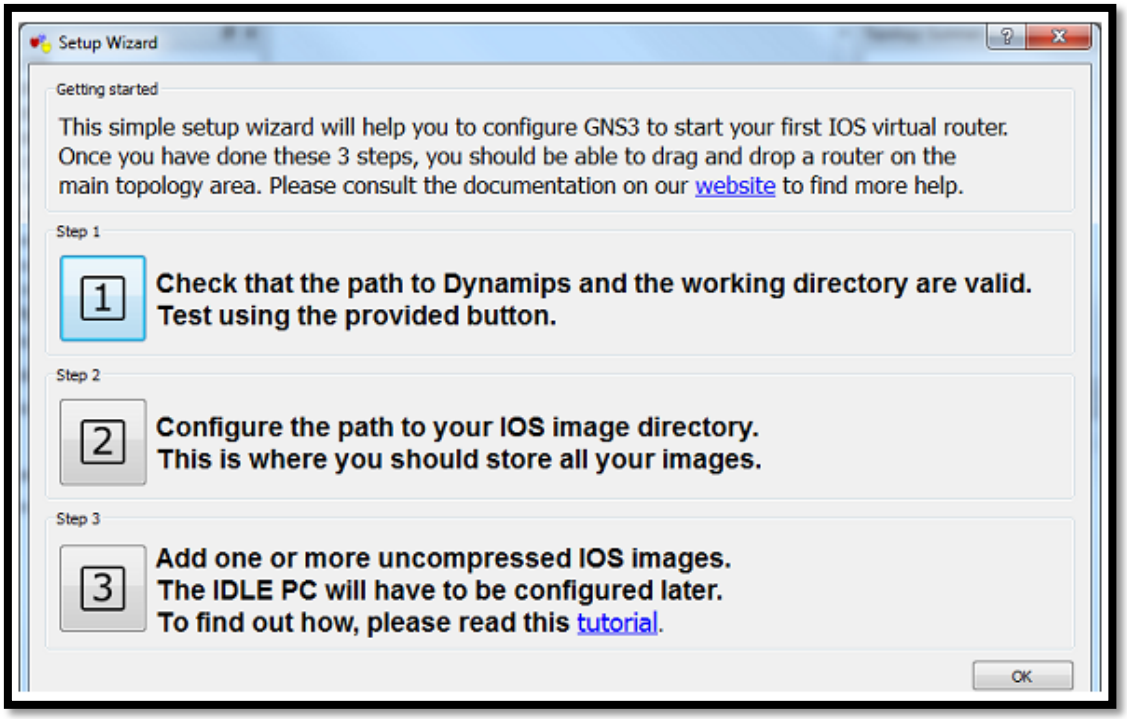


Fig (6.1):GNS3 setup wizard

- **Step 1 – Setup Dynamips :**

To configure Dynamips we use the Preferences Dialog>Dynamips Page, shown in fig (6.2) .

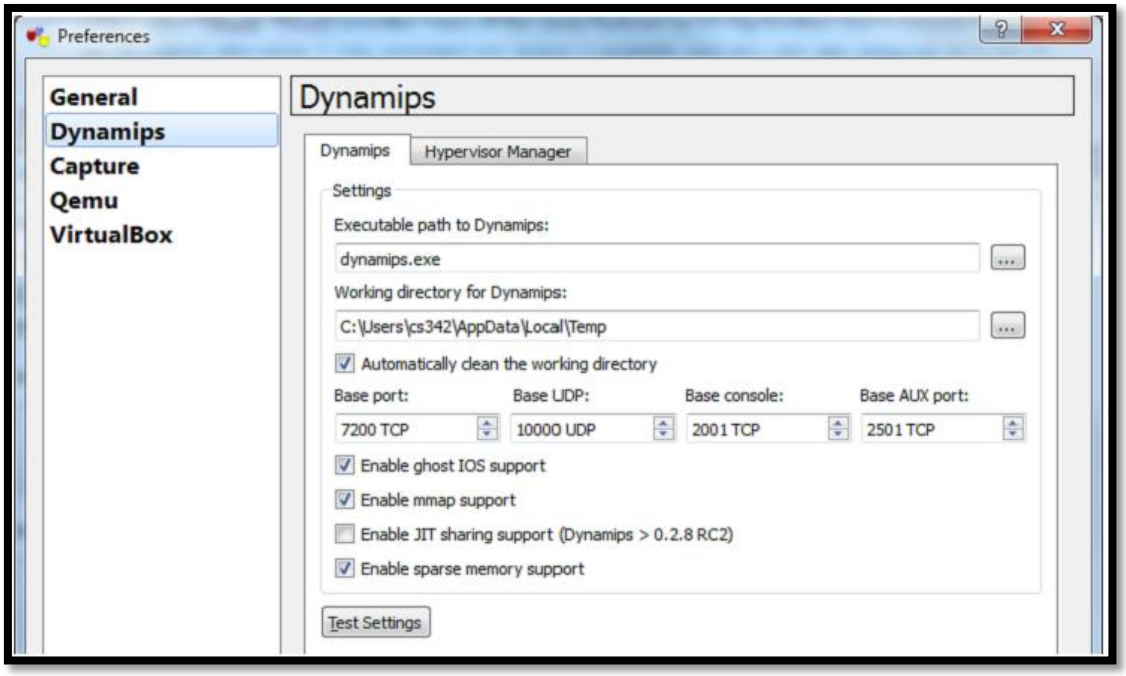


Fig (6.2) :GNS3 preferences configuration

The Dynamips test should be successful, as shown in Fig (6.3)

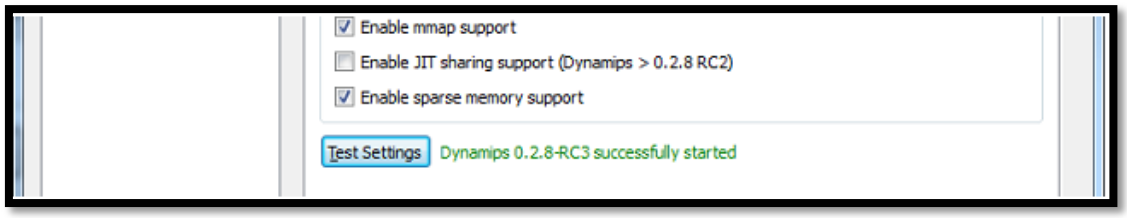
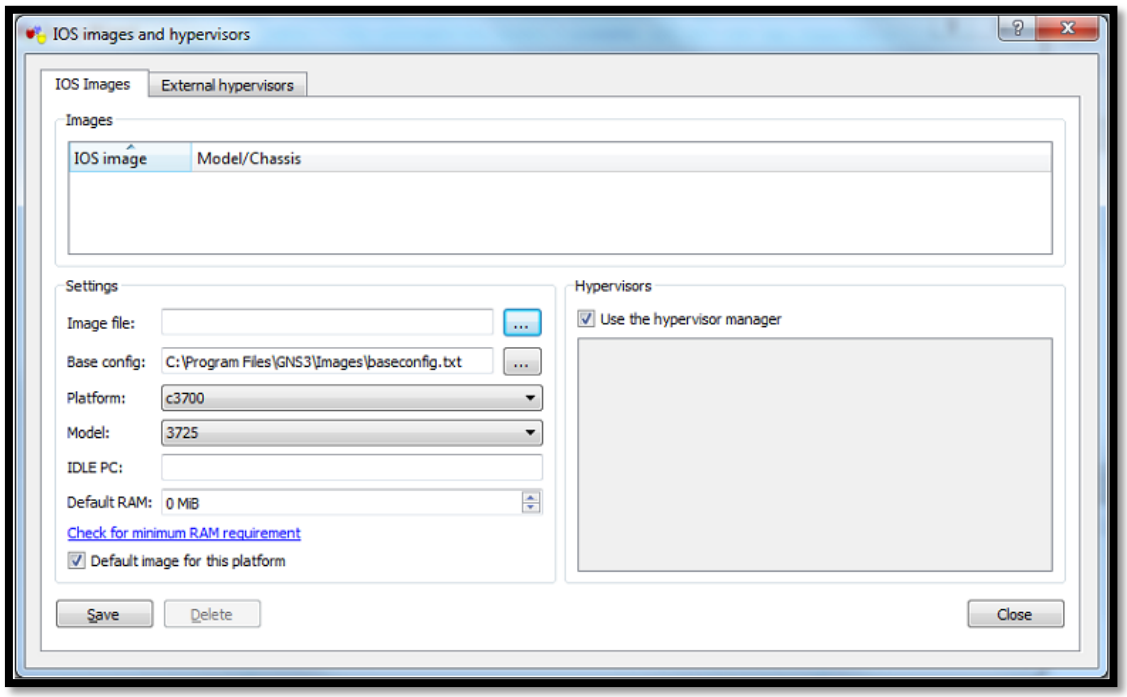


Fig (6.3) Testing Dynamips

- **Step 2: Configure IOS images :**

  Go to the IOS Images Dialog, This can be reached via Edit>IOS Images and Hypervisors. The IOS images appear in fig (6.4)

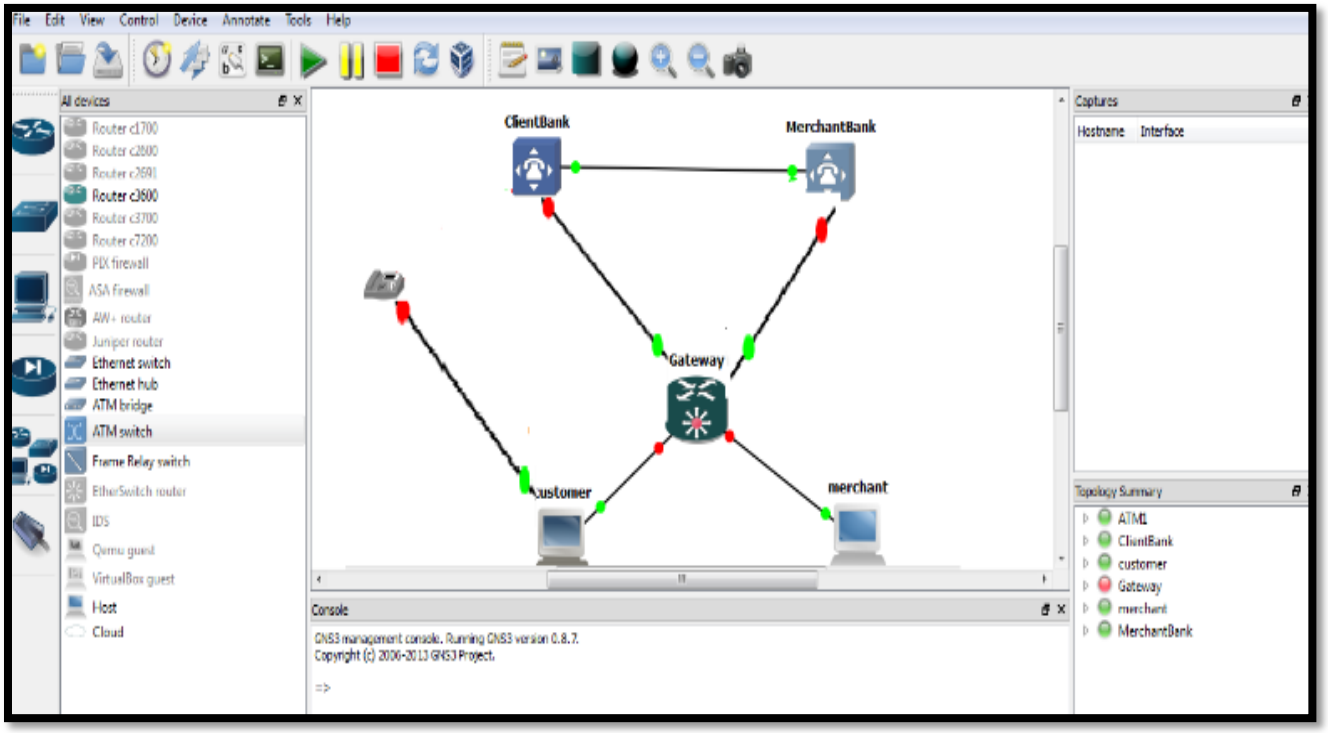


Fig(6.4) IOS images configuration

Now GNS3 simulator is ready to simulate the proposed QRG e-payment model ,

6.2. Evaluation and simulation of the proposed QRG e_payment model with GNS3:

To use GNS3 program to simulate the proposed model ,we first draw the proposed model on the GNS3 simulator screen .in the graph below fig (6.5) our model appear in GNS3 program



Fig(6.5):QRG E_payment model with GNS3 program

After run the proposed model then the console result of security and speed will appear in fig(6.6) give us the security and speed of our QRG e-payment model as a function of time

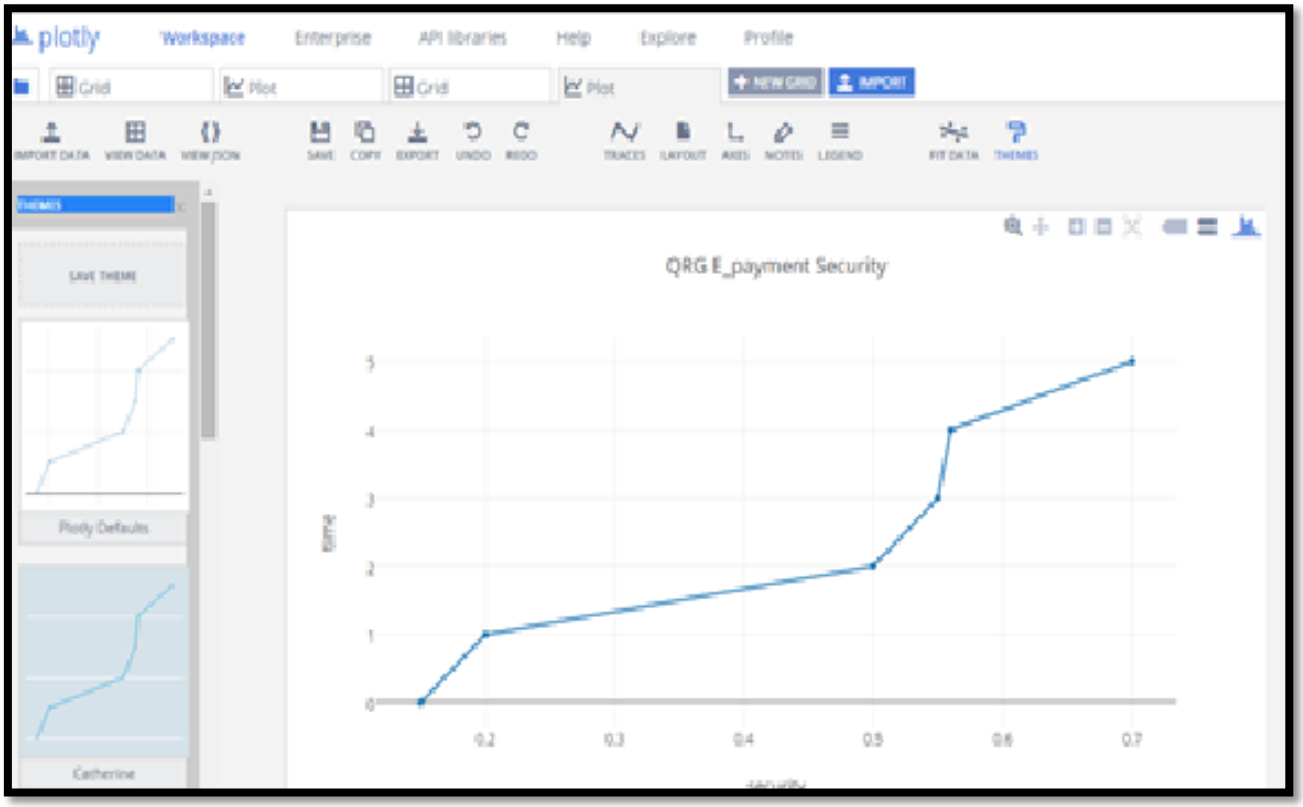
```
  active           Report on active interfaces only
  backbonefast     Show spanning tree backbonefast status
  blockedports     Show blocked ports
  bridge           Status and configuration of this bridge
  brief            Brief summary of interface information
  inconsistentports Show inconsistent ports
  interface        Spanning Tree interface status and configuration
  root             Status and configuration of the root bridge
  summary          Summary of port states
  uplinkfast       Show spanning tree uplinkfast status
  vlan             VLAN Switch Spanning Trees
  |                Output modifiers
  <cr>

Haven#show spanning-tree

 Bridge group 1 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address c203.1672.0000
  Configured hello time 2, max age 20, forward delay 15
  We are the root of the spanning tree
  Topology change flag set, detected flag set
  Number of topology changes 1 last change occurred 00:00:20 ago
          from FastEthernet0/0
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 1, topology change 16, notification 0, aging 15

 Port 4 (FastEthernet0/0) of Bridge group 1 is forwarding
```

Fig(6.6):security of QRG e_payment model

6.2.1. Security and speed evaluation and simulation:

After running the proposed QRG e-payment model on GNS3 then we will take the result of speed and security from GNS3 program console–fig(6.6)- and simulate it with Matlab program:

- **Security Simulation (with Matlab)**



Fig(6.7): QRG e_payment model security

You can see from fig(6.7) that the security of the proposed QRG e_payment system increases rapidly with increasing time .The code of the Matlab security simulation will be :

```
data:[ {
x:[".15",".20",".50",".55",".56",".7"],
y:["0","1",2","3","4","5"],
name:"time",   type:"scatter", xsrc:":b3edb9",        ysrc:":3aa393",
        uid:"a94691"
}],      layout:{
```

yaxis:{
title:"time", type:"linear",
range:[-0.35554311310190373,5.355543113101904,autorange:true},
xaxis:{title:"security",type:"linear",range:[0.11581033935934029,0.7341896606406
96],
autorange:true},
height:486,width:869,autosize:true,showlegend:false,title:"QRGE_payment
Security"}

- **Speed evaluation and simulation (with Matlab)**

Fig (6.8).QRG E_payment model Speed

You can see from fig(6.8) that by using QRG model the e_payment process will be more fast ,

The code of the Matlab speed simulation will be:

data:[{
x:["0","1","2","3","4","5"],

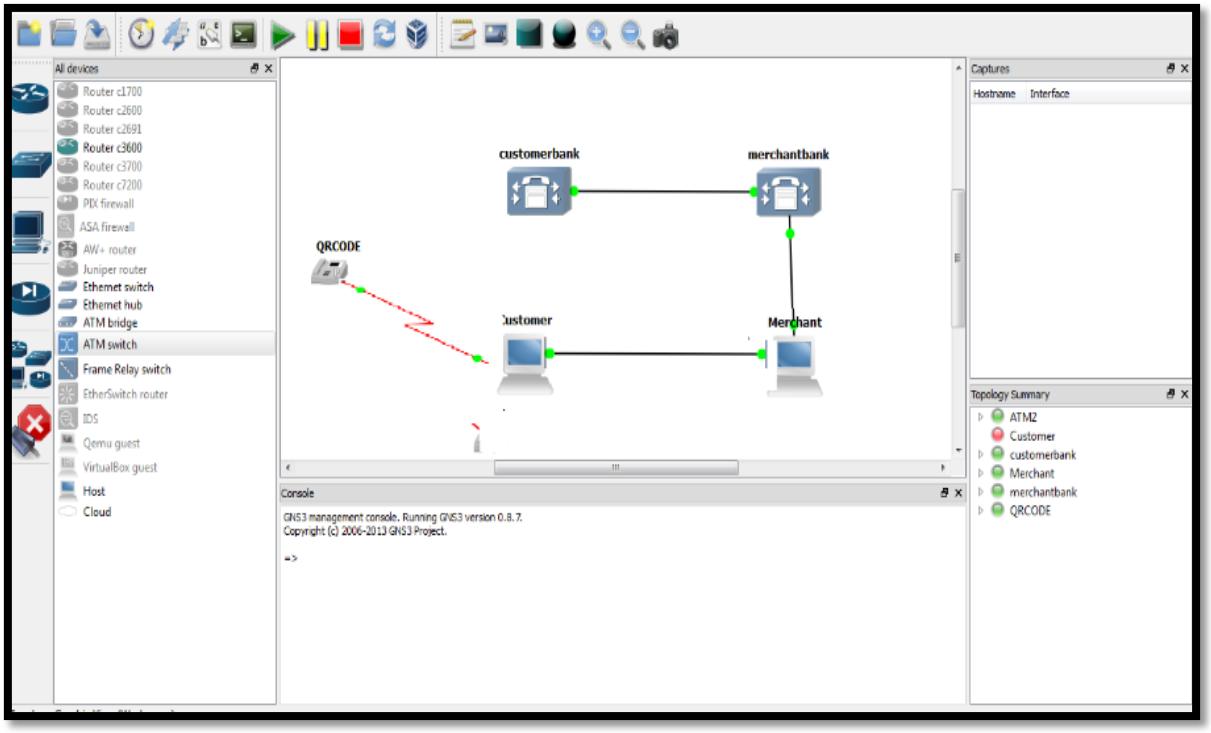
y:["12","15","15.5","18","50","50.1"],
name:"speed",
type:"scatter",
fill:"tonexty",
mode:"lines",
xsrc:":ff31df",
ysrc:":dfc145",uid:"55893"
} layout:{
yaxis:{title:"speed",type:"linear",range:[0,52.73684210526316],
utorange:true},
xaxis:{title:"time",type:"linear",range:[0,5],
autorange:true},
height:486, width:869, autosize:true, showlegend:false,
title:"QRG E_payment system speed"}

6.3.Comparison between QRG e_payment model and other models

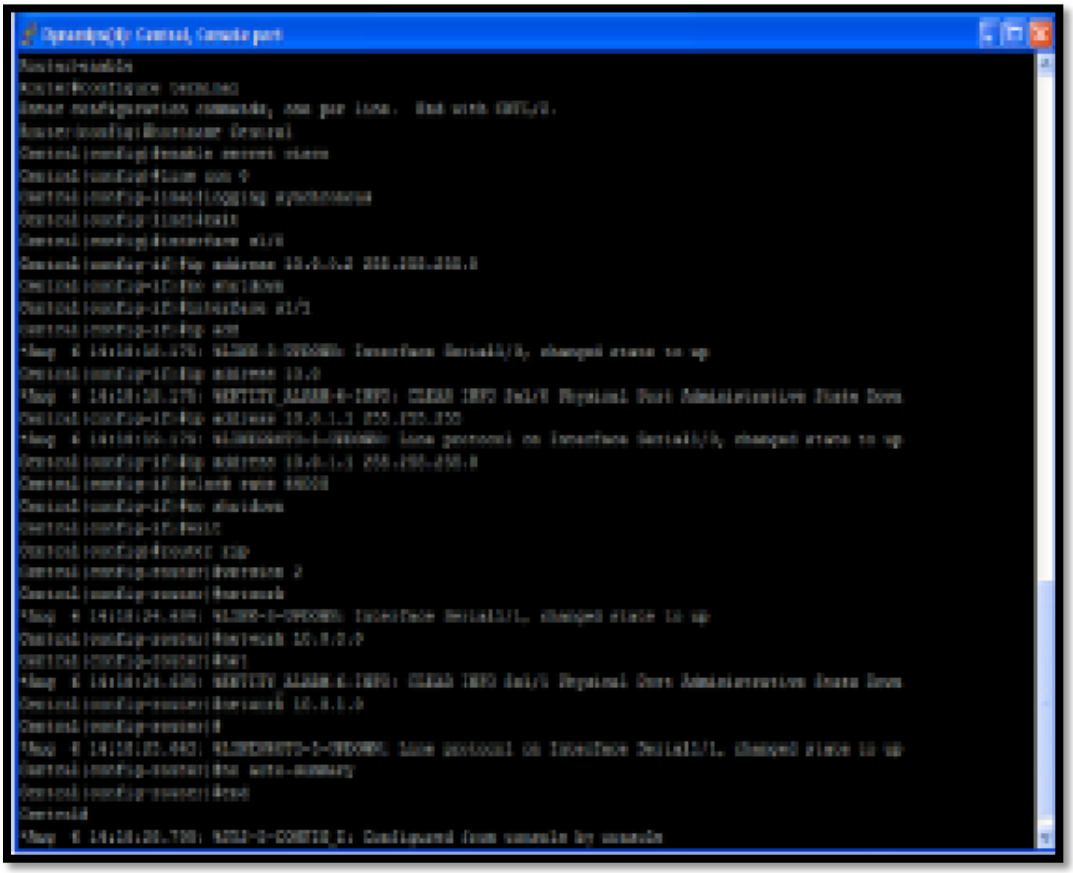
Now to evaluate our model we will compare it with other models that don't use the gateway technique and don't use QR code

- **QRG e_payment model Vs Models without gateway :**

We use the GNS3 program to simulate the models without gateway technique this model appear in fig (6.9) , then the result of this model security from fig (6.10) will be taken to Matlab simulation and compare it with the security of QRG model , the comparison result will be as in fig (6.11)



Fig(6.9) :E_payment model without gate way with GNS3 program



Fig(6.10) :E_payment model without gate way security and speed GNS3 simulation

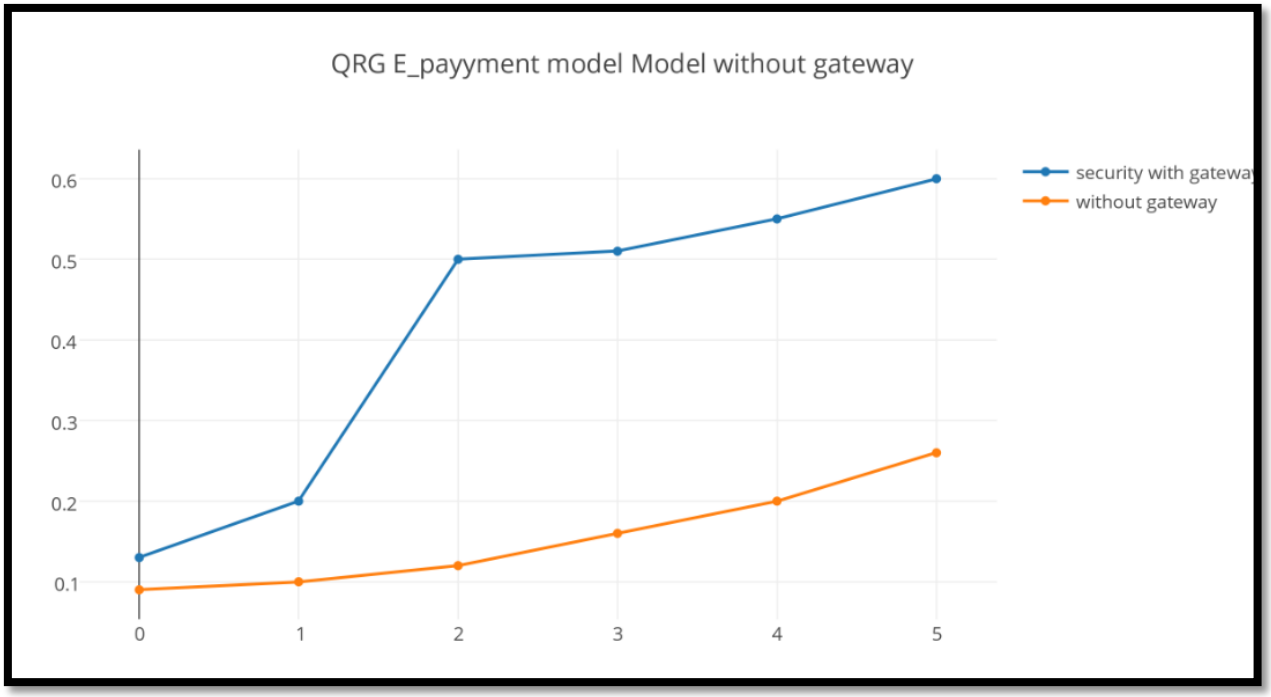


Fig (6.11):QRG Vs models without gateway security simulation

You can see from fig (6.11) that proposed QRG e_payment model with gateway will be more secure than other models that don't use gateway technique, so our model will increase the security of used models

The code of fig (6.11) Matlab simulation will be :

```
data:[{
x:["0","1","2","3","4","5"],          y:[".13",".2",".5",".51",".55",".6"],
name:"security with gateway",
type:"scatter",
xsrc:":8d50eb",
ysrc:":b52773",
uid:"9073e7"},
{ x:["0","1","2","3","4","5"],        y:[".09",".1",".12",".16",".2",".26"],
name:"without gateway",
type:"scatter",
xsrc:":8d50eb",
ysrc:":1370e9",
```

uid:"979607"],
layout:{
yaxis:{type:"linear",range:[0.05373460246360581,0.6362653975363941],
utorange:true},
xaxis:{type:"linear",range:[-0.37648866692278155,5.376488666922781],
autorange:true},
height:486, width:869, autosize:true, showlegend:true,
title:"QRG E_payyment model Model without gateway"

- **QRG e_payment model Vs models without QR code**

You know before that the proposed model use QR code , and using QR code will add to e_payment more security and more speed in comparison with other models that use other techniques like barcode, NFC ….

In the comparison using Matlab simulation results in fig (6.12) you can see that the proposed model with QR code will be more faster than other models and this speed will increase rapidly in time

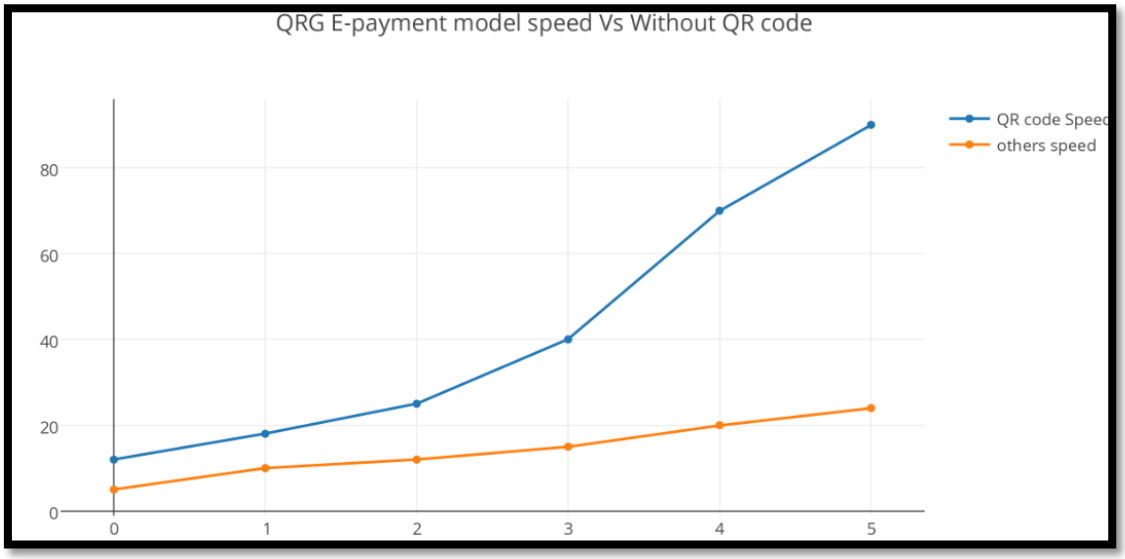


Fig (6.12) QRG model speed Vs Speed of models without QR code

The code of the Matlab simulation in fig (6.8) will be :

data:[{

```
x:["0","1","2","3","4","5"],
y:["12","18","25","40","70","90"       ],
name:"QR code Speed",
type:"scatter",
xsrc:":55a04f",
ysrc:":66303f",
uid:"927248"},{
x:["0","1","2","3","4","5"],
y:["5","10","12","15","20",24"],
name:"others speed",
ype:"scatter",
xsrc:":55a04f",
            ysrc:":6c0c64",
uid:"4abd61"
}],
layout:{
yaxis:{
type:"linear",
range:[-1.0442329227323635,96.04423292273236],
autorange:true},
xaxis:{
type:"linear",
range:[-0.31477535073699175,5.3147753507369915],
autorange:true
```

```
},
heght:486, width:869,
autosize:true,
showlegend:true,
title:"QRG E-payment model speed Vs Without QR code"
}
```

6.4.Conclusion :

From the result we found out that there are areas today when you have to use cash because card payment is not accepted or available there is a gap that could be filled with mobile payments.

The majority of the participants in our research could consider paying for the ability to use the mobile phone as a payment instrument. This means that the mobile payment provider does not need to promote their mobile payment services as free to the consumers if the consumers can see the benefits that follow. This in turn leads to, that the provider does not need to only charge the merchants and thus leads to a farer cost for the merchants.

When it comes to the question of preferable technologies in mobile payments two conclusions can be drawn(QR code and NFC). And as we discussed before QR code is more secure reliable and fast to be used in e_payment .

Also when it comes the question of what's better for e- payment (with gateway or without gate way) the simulation result above will answer to you and tell you that using gateway is more and more secure to be applied in e_payment process .

Everyone except one participant in our study could consider using the mobile phone as a payment instrument in the future which is a very high degree of acceptance and shows that mobile payment is a technology that creates value for the consumers.

In the field of diffusion theory mobile payment seems to have a bright future since most of the innovation attributes for diffusion are fulfilled from the consumers' perspective. It seems as it is the social barriers that needs to be penetrated and that

some people take the roles as early adopter in order to fuel the diffusion and get the process started.

And when we speak about the best technique to be applied in smart phone on e_payment process QRG will be the best .

Chapter Seven

Conclusion:

As you can see from the thesis study, QR Code are an upcoming and fast-growing technology that is used in many different fields. QR Codes offer a range of benefits that stakeholders from different fields are exploring and adopting to fulfill their requirements. Even though advertising is the area where QR Codes mostly used, new services like payment using QR Codes have been introduced over the last years. Along with this development security with high speed and flexibility concerns arise. This thesis examines a specific security issue, which is attacking e payment with QR Codes. Our empirical study is mainly focused on e-payment system and the QR code (definition , security , types , benefits ,…..).

And to make the e payment process more secure, fast, flexible with less cost We developed a new model with algorithms using QR code .

In the current payment systems, a customer's payment information is sent to a payment gateway via a merchant. This makes the payment system vulnerable to intrusions and information leaks, causing customer data theft, identity theft and fraudulent transactions.

To protect a customer's financial information from being compromised, we developed an approach for online payment systems in which a customer's payment information is directly provided to a payment gateway rather than sent through

a merchant. This approach, however, introduced some design issues .Hence, we show that our proposed payment system is secure and protects a customer's payment information and payment against network intruders or attackers.

Also our model use the QR code technique to make the above e payment system more and more flexible.

"QR code" is the trademark for a two-dimensional barcode first designed for the automotive industry. It can be read by an imaging device (such as a camera), and the required data extracted from patterns present in both horizontal and vertical components of the image. The QR Code system has become popular due to its fast readability and greater storage capacity compared to standard UPC barcodes.

They enable consumers to pay directly from their smartphone by allowing the merchant to scan the QR code (generated by a QR payment app) on the customer's phone to obtain payment information.

QR code is processed over the existing payment networks so it inherits all the existing legacy payment features with the strong security and flexibility ,more speed, less cost and time .also With the use of QR code in our module you can use mobile payment "use your smart phone to scan the QR code"

Also we use Edrawmax [44] program to draw all the graphs and flow charts in our thesis .Edraw Max is an all-in-one diagram software that makes it simple to create professional -looking flowcharts, organizational charts, network diagrams, business presentations, building plans, mind maps, science illustration, fashion designs, UML diagrams, workflows, program structures, web design

diagrams, electrical engineering diagrams, directional maps, database diagrams and more.

References

[1] Arpita gopal,chandrani singh , "E-Banking " , "E-world emerging trends in information technology", information technology book , Vol 337 ,2009

[2] Shristi Pant, " asecure online payment system" computer science , Vol 56,DSTI/ICCP/IE(2004)18/REV1

[3] David pinter meastre "QRP an improved secure authentication process",Vol 11, June 8, 2012

[4] Brad C.Johnson, Jonathan G.Gossels & Donald T.Davis,"The SSL Handshake" ,aperspective on practical security ,2004.

[5]www.epayment.com ,10-01-2015

[6] Singh sumanjeet , "Emergence of payment systems in the age of electronic commerce : the state of art " , *Asia Pacific Journal of Finance and Banking Research. 2009*

[7]http://www.smartcardbasics.com/smart-card-security_2.html, *Jan,2015*

[8] http://www.smartcardbasics.com/smart-card-types.html, "smart card basics",Feb 2015

[9] Mohammad Al-Fayoumi,, Sattar Aboud,and Mustafa Al-Fayoumi ,"practical e-payment scheme",IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 7, May 2010

[10] Jonerry Gao Ph.D., "electronic cash payment protocol", Journal of Networks, Vol 5, No 8, 937-941 ,May 2000

[11]Hossrein Bidgoli ,e;ectronic commerce principles and practices,secure socket layer ,page 208

[12] Houssam El Ismaili, , Hanane Houmani, , Hicham Madroumi ,"A secure electronic transaction payment protocol ,design and implementation",(IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 5, No. 5, 2014

[13]A.koponen, " E-commerce , Electronic payment " . Magazine Communications of the ACM CACM Homepage archive Volume 22 Issue,2006

[14] vlad petre,"3D secure protocol" , Computing in the Global Information Technology, 2012. ICCGI ’08. The Third International Multi-Conference .

[15] Ciprian Stanică-Ezeanu,"Comparative Study of Internet Payment Security Protocols Based on Credit Cards ", informatics Security Master ,2008

[16]Mustafa Ally ,Mark Tolman , " Aframe work for assessing payment security mechanisms and security information on e- commerce web sites " , Vol. LX ,No. 2/2008

[17] http://www.nahb.org/payment_check.aspx, "electronic check", 27 Feb,2015

[18] A. R. Dani, V. Visweswar, Ashutosh Saxena, P. Radha Krishna and V. P. Gulati,"E-CHECK CLEARING & SETTLEMENT SYSTEM FOR INDIAN BANKS",2004

[19]"http://goqr.me/ ",august,2014

[20] http://www.qrcodesinmarketing.net/history-of-qr-codes.html, oct,2014

[21]QRStuff. What’s a QR Code?, 2011. http://www.qrstuff.com/qr_codes.html. Accessed 25 Jan 2013.

[22]Steeman, J. QR code data capacity, 2004. QR4 QR Codes blog: http://blog.qr4.nl/page/QR-Code-Data-Capacity.aspx. Accessed 3 Feb 2013.

[23] P. Kieseberg, M. Leithner, M. Mulazzani, L. Munroe, S. Schrittwieser, M. Sinha,E. Weippl. Qr code security. In *Proceedings of the 8th International Conference onAdvances in Mobile Computing and Multimedia, MoMM ’10* (2010), pp. 430–435.

[24] Russ Cox. QArt Codes, 2012. http://research.swtch.com/qart. Accessed 05 Mar 2013

[25] Thonky.com. QR Code Tutorial, 2012. http://www.thonky.com/qr-code-tutorial/.Accessed 10 Feb 2013.

[26] Esponse. Innovative QR Code campaigns (About QR codes), 2013. http://www.esponce.com/about-qr-codes. Accessed 23 Mar 2013.

[27] Loannis Kapsalis,"Security of QR code " , Master thesis in security and mobile computing ,Vol 92, June 2013

[28] P. Kieseberg, M. Leithner, M. Mulazzani, L. Munroe, S. Schrittwieser, M. Sinha,E. Weippl. Qr code security. In *Proceedings of the 8th International Conference on Advances inMobile Computing and Multimedia, MoMM '10* (2010), pp. 430–435.

[29] I. Reed and G. Solomon. Polynomial Codes Over Certain Finite Fields. *Journal of the Society for Industrial and Applied Mathematics 8*, 2 (1960), 300–304.

[30] C. Dow, Y. Lee, H. Yang, W. Koo, J. Liao . A location-based mobile advertisement publishing system for vendors. In *Eighth International Conference on Information Technology: New Generations* (2011), pp. 24–29.

[31] M. Ebling, R. Cres. Bar Codes Everywhere You Look. *PERVASIVE computing,IEEE 9*, 2 (2010), 4–5.

[32] J. Gao, V. Kulkarni, H. Ranavat, Lee Chang Hsing Mei. A 2D barcode-based mobile payment system. In *Third International Conference on Multimedia and Ubiquitous Engineering* (2009), pp. 320–329.

[33] Y. Kao, G. Luo, H. Lin, Y. Huang, S. Yuani. Physical access control based on QR code. In *International Conference on Cyber-Enabled Distributed Computingand Knowledge Discovery* (2011), pp. 285–288.

[34] D. Lorenzi, B Shafiq, J. Vaidya, G. Nabi, S. Chun, V. Atluri. Using QR codes for enhancing the scope of digital government services. In *Proceedings of the 13th Annual International Conference on Digital Government Research* (2012), pp. 21–29.

[35] D. Pirrone, S. Andolina, A. Santangelo, A. Gentile, M. Takizava. Platforms for human-human interaction in large social events. In *Seventh International Conference on Broadband, Wireless Computing, Communication and Applications.*

[36] J. Rouillard, M. Laroussi. Perzoovasive: contextual pervasive QR codes as tool to provide an adaptive learning support. In *Proceedings of the 5th international conference on Soft computing as transdisciplinary science and technology, CSTST '08* (2008), pp. 542–548.(2012), pp. 545–551.

[37] Ugo B. Ceipidor, Carlo M. Medaglia, A. Perrone, M. De Marsico, G. Di Romano. A museum mobile game for children using QR-codes. In *Proceedings of the 8th International Conference on Interaction Design and Children, IDC '09* (2009), pp. 282–283.

[38] Gia M. Agusta, K. Hulliyah, Arini, R. B. Bahaweres. QR code augmented reality tracking with merging on conventional marker based backpropagation neural network. In *International Conference on Advanced Computer Science and Information Systems (ICACSIS)* (2012), pp. 245–248.

[39] "QR code essentials " , Denso invertor of QR code ,2015 http:\www.denso-adc.com.18 ,Feb 2015

[40] http://www.createqrcodes.org/qr-codes-in-marketing.html oct,2014 "

[41] Pual Dungy , http://www.socialmediatoday.com/content/9-reasons-qr-codes-are-bad-your-brand , 18Feb 2015

[42] http://faculty.ist.psu.edu/bagby/432Fall07/T7/howWorks.html

http://www.dummies.com/how-to/content/finding-out-how-paypal-works.html ,28 Feb 2015

[43]http://paypal-qr-payments.articles.r-tt.com/,05Jan,2015

[44]http://paypal-qr-payments.articles.r-tt.com/,15 Jan,2015

[45] Ved Prakash Gulati And Shilpa Srivastava – "The Empowered Internet Payment Gateway"

[46]Holly Lynne McKinley,"SSL and TLS: A Beginners", SANS Institute 2003,Guide-,GSEC Practical v.1.4b

[47] Peter Burkholder, "SSL Man-in-the-Middle Attacks", SANS Institute,February 1, 2002 (v2.0)

[48]James ACAndrews, 'the automated claering house system : moving toward electronic payment "

[49] http://www.achnetwork.com/overallbenefits.html 22-02-2015

[50] https://www.paypalobjects.com/en_US/vhelp/paypalmanager_help/, about_ach_payments.htm,feb 2015

[51]http://www.cnet.com/how-to/how-nfc-works-and-mobile-payments/28,Feb 2015

[52] http://www.zdnet.com/article/you-dont-need-nfc-in-your-phone-to-pay-for-things-without-a-wallet/ 28Feb 2015

[53]Jethendra Dara,"credit card security and e-payment" ,master thesis in computer system and science ,Vol 52, 2006:23.

[54] Shristi Pant,"A SECURE ONLINE P AYMENT SYSTEM",Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09),Nanchang,P.R. China, May22-24,2009, pp. 046-050

[55] David Pintor Maestre,"QRP: An improved secure ,authentication method using QR codes" . The First International Workshop on Application of Arti- ficial Intelligence for Email Management (AAIEM 2011) in London (UK), June 2012.

[56] Dominik Schrank,"Trustful Payment System for Virtual Worlds,Design and Implementation of a Payment System for Virtual Worlds ",2009

[57] http://www.ehow.com/info_8612622_importance-epayment-systems.html, Feb,2015

[58] G. Dhillon, J. Ohri, Optimizing Security in E-commerce through Implementation of Hybrid Technologies, CSECS'06 Proceedings of the 5th WSEAS International Conference on Circuits, Systems, Electronics, Control & Signal Processing, Pages 165 – 170.

[59]A.A. Slamy, E-Commerce security, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, May 2008

[60]B. Lee, T.Lee, An ASEP (Advanced Secure Electronic Payment) Protocol Design Using 3BC and ECC(F2m) Algorithm, e-Technology, e-Commerce and e-Service, 2004. EEE '04. 2004 IEEE International Conference on, pages 341 – 346

[61] Houssam El Ismaili, Hanane Houmani, , Hicham Madroumi,"A Secure Electronic Transaction Payment Protocol Design and Implementation", (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 5, No. 5, 2014

[62]Thair Al-Dala'in, Peter Summons and Suhuai Luo ,"A Prototype Design for Enhancing Customer Trust in Online Payments",Journal of Computer Science 5 (12): 1034-1041, 2009

[63] http://www.gns3.com/.May ,2015