ISSUES OF SECURITY, CHALLENGES AND IMPLEMENTATION OF *SHARIA'* PRINCIPLE IN E-COMMERCE TRANSACTION

Tamrin Amboala[ψ], Mohd Zulkifli Muhammad and Mohd Rushdan Yasoa

Universiti Malaysia Sabah, Malaysia

Abstract
There are growing concerns among e-commerce customers particularly Muslims in Malaysia regarding on-line transaction both from security aspects and *Sharia'* perspective. There are two main issues arise concerning purchasing on-line using credit cards. First is the medium of transaction via on-line or Internet itself and secondly, the mode of payment being used to purchase online in which using credit card in this case. As Malaysia is heading towards e-commerce and purchasing on-line via credit cards has no longer a new trend; the challenges arise for solution which compliance with *Sharia'* principles. This paper will address and highlight several challenges and issues and present recommendations based on the existing technology without overlooking legal provision provided in this country to solve the above concerns.

Keywords: E-commerce transaction; *Sharia'* principles; Credit card.

JEL Classification Codes: M15; Z12.

1. Introduction

The advents of IT and e-commerce have brought more complex levels of Islamic business and commerce ethics that require the Islamic jurisprudents to expand their tools of evaluation and analysis beyond the traditional context. With a comprehensive approach that taking into account regulations and the existing technological tools brought into the *Sharia's* perspective, this article seeks and develops an understanding how to provide alternative solution to the conventional and unislamic e-commerce transaction.

There are several main challenges of on-line transaction from the perspective of *Sharia'* which will be discussed here namely the security, legality of the contract, issues of anonymity, *gharar and riba.* Addressing these aspects require Islamic jurist and scholars to scrutinize both the technicalities of the on-line transaction and the legalities in terms of *Sharia'*.

2. Challenges from perspective of *Sharia'*

Islam accords the importance to the trading sector as source of wealth and the roles its play to the development of the country and the *ummah* as a whole. In this regard, the holy *Quran* abounds with many references to the trade and commercial activities. The *Quranic ayats* supports this statement as below:

> "O you who believe! Eat not up your property among yourselves unjustly except it be a trade amongst you, by mutual consent. And do not kill yourselves (nor kill one another). Surely, Allah is Most Merciful to you' (4:29)
>
> "Woe to *Al-Mutaffifin* [those who give less measure and weight (decrease the rights of others)]" (83:1).

Parts from legality of transaction from the traditional perspective such as *halal* (permissible) aspects of the product or the service itself, Islam also recognize the confidentiality and the integrity as important elements to secure the transaction. Islam is very much concerns on the mode of transaction offered by the e-commerce. Thus, it has brought considerable critical attention.

[ψ] Corresponding author. Tamrin Amboala. Labuan School of Informatic Science, Universiti Malaysia Sabah, 87000 Labuan Federal Territory, Malaysia. Corresponding author E-mail: tamrin@ums.edu.my

What is known as "Trading Data Management" can be traced dated backward since fourteen centuries ago where the religion broken it into four major legalistic sections – *Fiqh al-Muamalat* (Islamic Business Transaction).

3. On-Line transaction

Securing transaction online must fulfill two main requirements, first concerning how to protect the data from the unauthorized parties (confidentiality) and how to guarantee the integrity of the transaction itself. Confidentiality ensures that the data travels on-line only be received and access by the authorized party(s). Confidentiality sometimes is associated with secrecy and privacy. On the other hand, Trusted Network Interpretation defines that the integrity ensures that computerised data are the same as those in source documents; they have not been exposed to accidental or malicious alteration or destruction (National Comp Sec Center, 1987).

In order to guarantee the integrity in the context of communication on line, Stalling (2003) suggested that the data sent must ensure the following:

i. The data must be protected against content modification – it includes changes to the contents of a message, including insertion, deletion, transposition and modification
ii. The data must be protected against timing modification – delay or replay messages
iii. Source repudiation –denial of transmission of message by source
iv. Destination repudiation – denial of receipt of message by destination

If man-in-the-middle is able to intercept the message sent to a merchant, he might not just modify the message (i.e. the order quantity), yet able to replay the same message to re-purchase the product several time.

The mechanism must provide protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. Both the origin or sender and destination have proof that message was sent and received. For instance, if a customer has made a payment on line there is no way that the merchandiser denies it. The above requirements can be achieved by two main ways - Encryption and Digital Signature.

Credit card companies realized that most transactions over the internet require just keying in information on credit card number, expiry date of card, name and address. Both Visa and MasterCard have designed a protocol called "SET" or Secure Electronic Transaction with participation from leading technology companies, including Microsoft, IBM, Netscape, RSA and VeriSign. As the specification developed is open and free, anyone can use it or develop any SET-compliant software for buying or selling on line (www.visa.com).

SET focuses on maintaining confidentiality of information, ensuring the message integrity and authenticating the parties involved in transactions. It has been designed to utilize technology for authenticating the parties involved in payment card purchases on any type of online network and internet that uses Encryption and Digital Signature and Digital Certificates.

3.1 Encryption

To buy goods over the Internet, one need to place an order accompanied by a credit card number. The credit-card number must be encrypted before sending it to the merchandiser. Encryption is a process in which the plain data such as a credit card number is transformed into a cipher text unreadable accept for by receiving end who then decrypts the scramble message into a readable form. This will ensure that the credit card number will not be intercepted en-route, though if they are capable the interpretation of the data is meaningless without the interceptor knowing how the scrambling was done. This will prevent the cipher text be used by the unscrupulous individuals.

3.2 Legality of on-line Contract: Perspective of Sharia'

The formation of contract requires two parties: one offers the contract then another party who will accept the offer. The offer is the proposal which is made to show his or her willingness to form a contract and in turn, the later response from the other party to prove his or her willingness to the offer.

The terms and conditions of the contract can be easily communicated on line but issues arise pertaining to the meeting place. Traditionally with off-line communication where both parties met face-to-face issues of anonymity is never arise.

From the tradition attributed to the Prophet emphasized the importance of the concept of meeting place can be understood from the following *hadith*:

> *"When two persons enter into a transaction, each of them has the right to annul it so long as they are not separated and are together (at the place of transaction); or if one gives the other the right to annul the transaction. But if one gives the other the option, the transaction is made on this condition it becomes binding. And if they are separated after they have made the bargain and none of them annulled it, even the transaction is binding"* (Shahih Muslim)

The above *hadith* covers both the concept of meeting place and time to conclude the offer. The idea of setting place in Islamic commercial legal system is required to extend the validity of the offer over a certain period of time in which the acceptance must be made within the designated period. A part from giving option for annulling the sale at any time before separation the meeting place alleviate anonymity concern. Failure in addressing the issue of anonymity will bring in issues of security of the transaction itself.

3.3 The Application of Session Key to Resolve Time Validity Period in Meeting Place

The validity period in meeting place can be resolved with an authorization and authorization technique in Authentication Protocols by using session key. Generally the protocol is used to verify that the communication partner who is supposed to be not an impostor (Tanenbaum, 2003). The difference between authentication and authorization is deal with whether you are communicating with a specific process whilst whether or not you permitted to do the specific process or activity. For instance when two parties initiate a deal or contract on line the first question arise are the communicating parties are "talking" to the trusted ones. The first question is more important to be answered unambiguously before the next process begin in which is just a matter of looking up entries in local databases to check out level of authority be given to him or her to close the deal.

Though the application of session key is mainly used for authorization it can be expanded to validate time validity. Once the communication is terminated the session key can be cheaply discarded.

3.4 The Application of Digital Signature and Certified Authority to Resolve Anonymity Concern

This article seeks to present and clarify the mechanism to resolve the above concerns pertaining to anonymity in relation with the security and the validity of the transaction from Islamic legal system. By applying both the technological and legal solution in e-commerce transaction will provide a comprehensive approach towards the above concerns.

3.4.1 Digital Signature

Though securing data from disclosure by the unauthorized party will ensure confidentiality it will not protect the data from repudiation. There is a compelling need that for the message to be protected from repudiation. Someone who sends a message must be accountable and responsible and there is no way he or she to deny. In another hand someone cannot falsify a message and claim that it was from someone else is another example of repudiation.

A digital signature provides a mechanism in which the identity of the sender of a message or the signer of a document to ensure that the original content of the message or document that has been sent is not tampered or changed.

Digital Signature tries to replicate traditional signature that uniquely identifies the owner of the signature. The ability to guarantee that the original signed message arrived means that the sender cannot easily deny it later. Digital signatures are easily transportable and cannot be copied or fabricated by someone else and can be atomically time-stamped.

Digital signature complements the encryption though it is not necessarily be used together. It can be used with any kind of message, whether it is encrypted or not. The receiver simply can be sure of the sender's identity and the message arrived intact.

3.4.2 Trusted third Party – Certificate Authority (CA)
In order to guarantee and convince the receiving party that the message received is not tampered a trusted third party is involved. The Trusted Third Party and sometimes interchangeably called Certificate Authority (CA) to resolve any possible conflict concerning the authentication and the confidentiality of the transaction. The trusted third party or the certificate authority will ensure that the message received in a form when it was sent. The general idea is that a certificate authority is trusted, so users can delegate the construction, issuance, and acceptances as well as revocation of certificates to the authority.

Pfleeger (2006) cited that the specific actions of a certificate authority include the following:

i. Managing public key certificates for their whole life cycle
ii. Issuing certificates by binding a user's or system's identity to a public key with a digital signature
iii. Scheduling expiration dates for certificates.

Anyone can verify that the certificate is real and from the party who issue it. In Malaysia, Digicert Sdn. Bhd is the first Certification Authority (CA) in the country since 1998. Digicert Sdn. Bhd serves as a trusted third party which issues digital certificate for both parties to secure their transaction (www.mimos.com.my). Whilst the buyer and the merchandise will only concern about the payment and the product or service to be delivered the CA facilitate and focus on maintaining the confidentiality of the information, ensuring the message integrity, and authenticating the parties involved in the transaction.

All the underlying process takes place in a Secure Socket layer in a transport level in a five-layer Internet protocol. For instance, Maybank, a leading commercial bank in this country implementing 128-bit Secure Sockets Layer (SSL) encryption protocol from Verisign Certificate Authority for all information transmitted over the Internet among users as well as within their own network and resources (www.thefigh.org). At the same time, Maybank to adopt Best Practices Maybank from WebTrust – an independent corporation that monitors and tests the facilities to assure that it maintains the highest and most current standards in Internet information security and exchange.

4. Digital signature act (DSA) in Malaysia
To cope up with global and technological need of electronic commerce the Digital Signature Act 1997 was introduced. The Act came into force in 1998 two years after the government launches the Multimedia Super Corridor mega project.

The Act requires that a document attached with a digital signature shall be as legally binding as a traditional signature, an affixed thumbprint or any other mark and that digital signature created in accordance with the Act shall be deemed to be a legally binding signature. It is also mentioned that a message shall be as valid, enforceable and effective as if had been written on paper if it bears in its entirely a digital signature and the signature is verified in accordance with the procedure laid out in the act (The Credit Risk Data Management, 2007).

Technological solutions to identify both parties during transaction might not be convincing enough in order to meet the business legal protection. Legal protection has been regulated to provide a complementary approach for customers and businesses apart from what have been provided by Encryption and Digital Signature mechanisms.

Though there are no international treaties dealing with this issue DSA is considered an important tools and platform in securing electronic commerce. In terms of global electronic trade, problems regarding identification will still arise with regards to foreign parties

4.1 The Legal Binding of a Digital Signature
As stated above the effect of the signature is the same as any other handwritten signature, thumbprint or mark as long as the digital signature is created in accordance with the DSA it is therefore as legally binding (section 62 DSA).

Section 64 DSA provides that a digitally signed document will be treated as a written document. The copies of a digitally signed document are also enforceable as an original under section 65 DSA. In section 67, provides an even stronger foundation for reliance on a digital signature with the presumptions as follows:

that a certificate digitally signed by a Certification Authority (CA) is issued by the CA and accepted by the subscriber if it is either published in the recognized repository or made available by the CA or the subscriber;

that information in the certificate is accurate; where the digital signature is verified by the public key listed in the certificate:

i. the digital signature is that of the subscriber;
ii. there is intention by the subscriber to sign the message; and
iii. the recipient has no knowledge or notice that the signer has breached a duty as a subscriber (see discussion below) or is not the rightful holder of the private key; and

The above presumption indicates that the subscriber may breach a duty as subscriber by revealing the private key awarded to them to any illegitimate party. The illegitimate party then misuses the key and masquerading themselves as the real subscriber to the recipient.

The illegitimate party may illegally copy or steal the private key and sign the digital certificate with or without the subscriber's acknowledgement.

The presumptions require the signer to prove that the digital signature was either not his or not attached by him or not proper in any way.

The practical impact of this would be that the risk of a forged or false signature now lies with the signer (subscriber).

4.2 Duties and Liabilities
Subscribers: In section 43 DSA the subscribers are required to exercise reasonable care to ensure the private key from disclose to any unauthorized person.

In section 41 DSA the subscribers should shoulder any lose or damage caused by a false material representations or non-disclosure of where the representation or non-disclosure was made with a deceitful intent or negligence

As the sole owner of a certificate the representations by the subscriber are implied as followed:

i. The subscriber sole ownership of the private key
ii. Representations made to the CA and information contained in the certificate are true
iii. Though not confirmed by the CA all representations made to the CA or in the certificate are true.

Trusted third parties (CA): Section 29 DSA clarifies that upon receiving a request for issuance from the sender CA need to confirm:

i. the identity of the prospective subscriber Before issuing a certificate CA must come up with the following prerequisite
ii. the data to be on the certificate is accurate
iii. the prospective subscriber is the rightful holder of the private key
iv. the private key is capable of creating a digital signature
v. the public key to be listed in the certificate is capable of verifying a digital signature affixed by the private key held by the subscriber.

Section 36 DSA requires CA certifies to all who reasonably rely on the certificate that

i. the data in the certificate is accurate;
ii. all information foreseeably material to the reliability of the certificate is included;
iii. the subscriber has accepted the certificate.

Under section 30 DSA the CA is also legislatively required to publish a signed copy of the certificate upon acceptance by the subscriber unless otherwise stipulated in a contract between the CA and the subscriber.

Under section 35 DSA the CA has a legislative responsibility to the subscriber to act promptly when revoking a certificate. CA is required to notify the subscriber of any facts known which significantly affect the reliability or validity of the certificate.

5. Payment using credit card – Based on Islamic principle

Payment using credit card is presented here due to its convenience and served as one of if not the most common in online transaction in Malaysia. The question on how to provide credit card that conforms to the *Sharia'* principles have become a central issue for Islamic on-line transaction.

The use of credit cards for purchasing goods online and then paying the price of purchase by installments to the bank or authorities that issue the cards is, in fact, a form of loan to card-bearer. So, an issuer is not entitled to receive more than the amount taken to purchase. But, the issuer is permitted to take a fixed charge under the name of administrative expenses, and such a charge is not increasable due to an increase of money used for purchase.

For sure, imposing a percentage on the amount of money used by credit cards is *Riba* (usury and interest) in itself, whether such a percentage is taken as a charge service and administrative expense or due to delay in settlement. Both forms are a usurious loan and the most well-known form of *Riba* of non-Islamic systems.

Literally *riba* means an increase or increase. According to Islamic Jurist it can be defined as usury or a practice of lending money with interest rates. In this concern, Islamic Fiqh Assembly issued its decision No. 108 (12/2) stating (Al-Faqih, 2002):

i. It is not permitted to issue uncovered credit cards or to deal in them if there is a condition that fixes usurious increase even if a user intends to pay up within a given free period.
ii. It is permitted to issue uncovered credit cards as long as there is no condition that fixes usurious increases to be added to debt. Here are two (2) sub points:
    i) It is lawful (for the bank or issuer) to receive a fixed charge for the issue or renewal of such cards as a wage for service rendered.
    ii) It is also lawful to receive commission from the trader for purchase, by the customer provided that selling by card is equal in price to selling in cash.

However, how does Islam accept the concept of credit card as a medium of on-line payment? What are the underlying principles required by *Sharia'* in the functionality of credit card? Islamic credit card is the substitute for conventional interest-based credit cards. Islam allows the use of credit card as long as it does

not involve the element of interest. In Malaysia, the doctrine of *Bay al-Inah* is recognized and used to validate the credit card transaction (Kazi, 2002).

The *Bay al-Inah* contract works on the basis of two (2) separate agreements, namely *Bay al-Mutlak* (cash sale) and *Bay Bithaman Ajil* (deferred sale) (Darwish, 2003). The former is the bank's agreement to sell an item to the customer at an agreed price, while the latter agreement covers the customer selling back to the bank at a lower price. The difference is the bank's profit on the transaction and is a predetermined amount. There is no penalty charged to the customer and for the unutilized financing amount the customer is legible for rebate (Khir *et al*, 2008).

But the doctrine of *Bay al-Inah* is not recognized by some scholars from Middle-East. Their reasoning is that the contract is ethically flimsy when applied in this manner, the sale transacted is a fake sale and thus just a means of masking *Riba*. They decided that the solution to *Riba* avoidance was to exercise the acceptable right of charging for the provision of a financial guarantee called the guarantee system (Darwish, 2003).

Regarding the above issue, *Murabahah* System is proposed by Ustaz Mustafa Omar of Islamic International University (Zainul, *et. al*, 2004). *Murabahah* is generally defined as a sale with Mark-up or a cost plus profit sale. It is sale of product for the price at which the bank in this case has purchased it, with the addition of stated profit. Islamic banks use it as a credit vehicle to finance the buyer against a predetermined profit without bearing any risk.

6. *Gharar*

Literally *gharar means* fraud and has often been associated with risk and uncertainty. To avoid from *gharar* both parties; buyers and sellers are required to have adequate information of values they intend to exchange, the existence of the object, obtainable, its quantity, quality and attributes are identified and it can duly be delivered.

It is reported in a *Hadith* that the Prophet (s.a.w), prohibited the sale of *gharar.* While commenting on this hadith, Ibn Taymiyyah wrote that *gharar sale* is a sale which partakes in risk taking (*mukhatarah*) and in unlawful devouring the property of others (Taqi al-Din Ibn Taymiyyah, 1317 A.H). As commented by Islamic jurist the necessary to avoid any contracting party mislead the other party and use abusive means dishonestly provided on line to his or her ignorance.

Traditionally *gharar* is used describe two types transactions – 1) sale of the unseen (*bay' al-gha'ib*) such as sale of crops not yet grown to maturity, or sale of fish in the pond and 2) sale of the non-existent (*bay' al-ma'dum*) which is the sale object was non-existent at the time of contract.

Islamic jurist are divided in determining the validity of transaction with reference to *gharar.* Hanafi school of thought stated that the knowledge of the products and its attributes as perquisites to validate the transaction. Anyway it is required for enforceability in case the dispute arise in the future between the contracting parties. On the other hand the Shafi'is maintain, that knowledge of both the essence and attributes of the counter values is a precondition of validity and a sale in which the buyer has not seen the object is invalid due to excessive *gharar* .

The anonymity of Internet users including traders contribute to the complexity of defining *gharar* in its new dimension. It used to happen in which the subject matter is concealed from the buyer without he or she knowing exactly its future result. In the sense of on-line transactions there are also three major concerns pertaining to *gharar;* the uncertainties over the products or the services itself, uncertainties over pricing and delivery and deferment.

Islamic business and commerce ethics require the sellers to clearly define the products offered, for instance the image of the products must be displayed clearly on the screen with their detailed specifications, the prices, the mode of delivery and payments. Secondly both contracting parties; sellers and buyers must able to exchange the message in order to achieve conformity in the agreement that bind them together.

7. Conclusion

The discussion presented here might have answered the major concern among Muslims regarding the security, legality and against *gharar, riba* and related issues from the perspective of *Sharia* particularly in Malaysia. A part from a comprehensive approach, this article is also meant to provide a general guidance for e-commerce players.

References

Al-Faqih, A. (2002), *Credit Card Transactions*. [On-Line]. Available: http://www.islamweb.net/ver2/Fatwa/ShowFatwa.php?lang=E&Id=3399&Option=Fatwald

Darwish, A. F. (2003). *Can a credit card ever be halal?* [On-line]. Available: http://www.baankerme.com/bme/2003/mar/islamic_banking.asp.

http://www.mimos.com.my accessed on June 20, 2007.

http://www.thefigh.org accessed on October 29, 2007.

http://www.visa.com/cgi-bin/vee/nt/ecomm/set/main.html/ accessed on June 20, 2007.

Kazi, M. (2002). *Malaysian banks launch first Islamic credit card in Asia*. [On-line]. Available:http://www.islam-online.net/English/news/2002-07/25/articles06.shtml.

Khir, K., Gupta, L & Shanmugam, B. *(*2008). *Islamic Banking: A Practical Perspective*. Selangor: Pearson.

National Comp Sec Center (1987) *Trusted Network Interpretation,* National Computer Security Centre, NCSC-TG-005-VER1.

Pfleeger, C. P. (2006) *Security in Computing* 4th Edition. New Jersey: Prentice Hall.

Siddiqi, A. H. (2000) *Shahih Muslim*, tradition no. 3658, Kitab Bhavan, 971.

Stallings, W. (2003) *Cryptography and Network Security*. New Jersey: Prentice Hall.

Tanenbaum, A.S. (2003) *Computer Networks,* 4th Edition. New Jersey: Upper Saddle River.

Taqi al-Din Ibn Taymiyyah, (1317 A.H) *Nazariyyah al-'Aqd*. Beirut: Dar al-Ma'rifah, pp. 225.

The Credit Risk Data Management (2007) [Online, available at http: http://www.bakerinfo.com/apec/malayapec_main.htm accessed on June 28, 2007.]

Zainul, N. et al. (2004) E-Commerce from an Islamic perspective. *Electronic Commerce Research and Application*, 3, 280-293.