• A Model Development of Shariah Principle in E-Payment: The Case of Malaysia.

Mohd Zulkifli M.[1] [0000-0001-9700-454X], Tamrin A.[2], Noormariana M.D.[1], Mohd Fahmi G.[3] and Razman Hafifi R.[1]

[1] Faculty of Entrepreneurship and Business, Universiti Malaysia Kelantan, Kelantan, Malaysia,
zulkifli.m@umk.edu.my; noormariana.md@umk.edu.my;
razmanh@umk.edu.my
[2] Faculty of Computing and Informatics, Universiti Malaysia Sabah, Labuan, Malaysia,
ramdzan_trn@yahoo.com
[3] Faculty of Economics and Management, Universiti Kebangsaan Malaysia, Selangor, Malaysia,
fahmi@ukm.edu.my

Abstract. Issues concerning online transactions, e-payment mode are among the new challenges that Islamic scientists and researchers must face in broadening the reach of the Shariah e-commerce transaction concept. As Malaysia moves towards e-commerce and online shopping, there is no new trend; there are challenges for solutions based on the Shariah principles. This study aims to investigate and suggest the model development for Shariah e-payment system in Malaysia. This study utilizes a qualitative approach. The data employed were drawn from library research. The contents and textual analyses were employed to achieve this purpose. This study found a model consisting of a number of components, namely the Shariah core component, sound technical means, regulatory body and legal provision to enabling e-commerce transactions.

Keywords: e-payment, e-commerce transaction, Shariah principles

1 Introduction

In terms of IT and trade integration, Islamic business and business ethics have become more complicated and the Islamic jurisprudence needs to extend its tools of assessment and interpretation beyond the conventional context. This article seeks and develops an understanding of how to provide an alternative solution for the traditional and unislamic e-commerce transaction, taking into account the legislation and current technical resources in the Shariah's model. In Islam, e-commerce is undeniably permitted provided that e-commerce complies with the criteria laid down in Islamic contract law, namely form, contracting parties and subject matter. The goal is to ensure that the key trade objective in Islam, the protection of interests and the removal of harm by parties engaged in a commercial transaction, can be accomplished successfully [29].

However, an online transaction raised several key issues from the point of view of Shariah that will be addressed here: protection, contract lawfulness, issues of

anonymity, *gharar* (uncertainty) and *riba* (usury or interest). To resolve these aspects, Islamic lawyers and scholars need to discuss both the technicalities of the online transaction and the Shariah rule. Islam places the importance of the trade sector as a source of wealth and its position in the country's and ummah's growth as a whole. The Holy Quran, in this respect, abounds with many references to business and business. The Quranic verses affirm the following statement:

"*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).

"*O man of faith! Do not devour the goods of another with injustice but trade based on mutual agreement and good-will is allowed*" (4:29).

"*O ye who believe; devour not usury, doubled and multiplied; but fear Allah, that ye may prosper*" (3:130).

Islam gave the producers of goods and consumers equal rights to exercise their rights when appropriate. Regardless of the mode of conduct, every Muslim must be faithful and fearful of God. He should make sure that he is in line with the Quran and Sunnah and most importantly, his purpose is for Allah's sake, not just for the earthly benefit [27] [28]. Few studies have tried to develop a suitable model for the existing Islamic financial system. In one research, an eXtensible Access Control Markup Language (XACML) policy management model was developed to demonstrate how an Islamic financial information system could be used to make day-to-day bank decisions. All Islamic banks around the world need such a scheme. Most Islamic banks currently use advisory boards to provide opinions on general activities. Islamic financial information systems are to fill the gap between these high-level general rules and decisions of each client business process [26].

In the meantime, the other suggested that the Intermediate Shariah Transaction Party (ISTP) should be an intermediary until transactions can be concluded for contact between merchant and client. The design facilitates a more efficient and effective e-commerce transaction process that addresses, from the point of view of Shariah, three (3) common shortcomings in e-commerce transactions, namely *riba*, *gharar* and, without compromising on the security aspects of e-commerce transactions [28]. In view of the complexities of how companies and businesses carry out the transaction today, it is very important for the Ummah to establish an entirely new model and methods for a modern Islamic transaction. It is considered necessary to combine many methods, such as IT, e-commerce infrastructure, regulatory system, some adjustment and modification to adhere to the principles of Shariah. This paper is organized as follows. Section 2 reviews the core Shariah requirements for e-payment model. Section 3 describes the sound technological means for this model which includes digital

signature, session key and Financial Process Exchange (FPX). Section 4 elaborates on the regulatory body. Section 5 discusses on legal provision. Finally, Section 6 concludes the paper and recommendations for future research.

2 Core Shariah requirements

According to Islamic jurisprudence law, there is a variety of transactions under *Figh Muamalat* (law of trade) such as *Bai-Murabaha* (contract selling on profit), *Bai-Muqjal* (credit buying and selling) and so on. Depending on the type of the purchase, e-commerce falls under the *Bai-Salam* group. *Bai-Salam* is a type of transaction that always takes place before buying and selling. This involves transactions involving dropships online [33]. The Prophet s.a.w. said, according to *Bai-Salam* "Whoever pays in advance, make sure you have set the measurements and the deadline." The *Bai-Salam* condition can be further listed, as follows [1]:

i. *Ijab* (offer) and *Qabul* (acceptance) prices are set.
ii. Payment in cash or products.
iii. Pay at Majlis (during transaction).
iv. Products must be defined clearly.
v. Date of delivery must be set.

2.1 E-commerce transaction risks

Sections of transaction legality under the conventional viewpoint like halal (allowable) aspects of the commodity or the service itself are often regarded as essential elements in securing the transaction by Islam as confidentiality and honesty. Islam is very concerned about the manner in which e-commerce is offered. It has also brought significant criticism.

2.2 Legality of online contract

Contract formation involves two parties: one proposes the contract, and another accepts the bid. The offer is a proposal that shows its willingness to contract and, in exchange, the other party's subsequent answer to show its willingness to make the offer.

The contract terms and conditions can be easily shared online, but there are concerns concerning the meeting place. In custom, off-line correspondence, where both party's face-to-face anonymity problems are never encountered. The importance of the idea of meeting place can be understood from the tradition attributed to the Prophet Muhammad from the following hadeeth:

"*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" [2]

The above hadeeth covers both the meeting place definition and the time to complete the deal. The concept of position in Islamic commercial law is to extend the validity of the bid to a certain duration in which it must be accepted within a defined time frame. Anonymity issues are minimized apart from offering the option to cancel the sale at any time before separation. If anonymity is not discussed, the protection of the transaction itself will arise.

2.3 E-payment methods

Two most popular e-commerce payments are debit card and credit card. Debit card is considered the best payment option from the Islamic perspective compared with credit card, as there is no room for interest (usury). It just replicates the actual payment on e-commerce transactions from the auto payment system and the payment is transferred almost directly to the merchant's account from the consumer's bank account.

2.4 *Riba* (usury or interest) concerns

On the other hand, a number of problems arise with the credit card. Credit cards are used to buy items online, where the purchase price is charged through transfers to the bank or the card issuing authority is essentially a form of cardholder loans. An issuer is also not eligible to obtain more than the purchase sum. However, in the name of operating costs, the issuer is required to accept a fixed fee and this fee is not incredible due to the rise in the money for buying.

It is certainly *riba* (usury or interest) who sets a percentage on the amount of money used by credit cards, whether that percentage is taken as a charging service and administration costs or as a result of delays in settlement. Both forms are the most usurious loan for non-Islamic *riba* systems.

Riba literally means a rise. It can be defined as usury or the practice of lending money with interest rates, according to the Islamic Jurist. In this respect, the Islamic Fiqh Assembly issued Decision 108(12/2) [3]:

i. It is not allowed to issue or negotiate with exposed credit cards if a condition fixes usurious rises even if the customer plans to pay in a certain free time.
ii. Uncovered credit cards may be issued so long as there is no provision for usurious rises to be made to the debt. Two (2) subpoints are as follows:

(a) It is permissible (for a bank or issuer) to earn a fixed fee as a salary for a service given for issuing or renewing of cards.

(b) It is therefore legal to obtain the customer's sales fee from the trader so long as the sale by card is equal to the sale price in cash.

But how does Islam embrace the credit card idea as an online payment medium? What are the basic concepts of Shariah's credit card functionality? Islamic credit card

is a replacement for standard credit cards based on interest. Islam permits the use of credit cards as long as the factor of interest is not involved. In Malaysia, the *Bay al-Inah* (sale with immediate repurchase) doctrine is accepted and used to validate the transaction by credit card [4].

The contract for *Bay al-Inah* is based on two (2) separate agreements, that is to say, the cash selling in *Bay al-Mutlak* (cash sale) and the postponement sales in *Bay Bi-thaman Ajil* (sale on deferred payment) [5]. The former is the agreement by the bank to sell an object to the client at a price agreed on, and the latter covers the return of the client to the bank at a lower price. The difference is the benefit of the bank on the sale and is a default. No penalty is paid to the consumer and consumers may be reimbursed for the unused financial amount [6].

2.5 *Gharar* (uncertainty) concerns

Gharar literally means fraud and is often linked to risk and insecurity. Both parties must have sufficient information about the values that they wish to exchange to avoid *gharar*; the nature of the commodity, its quantity, quality and attribute are defined and can be delivered properly. In a hadith it is reported that the Prophet (see above) forbade selling *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 [7]. As commented by Islamic jurist, the required to avoid any contracting party deceive the other party and use abusive means dishonestly given on line to his or her ignorance.

Gharar is historically used to describe two forms of transactions: 1) selling the intangible (*bay' al-gha'ib*), including selling crops not yet grown up, or selling fish in the pond, and 2) selling the non-existent (*bay'al-ma'dum*) selling item that was not in existence during the contract. In determining the validity of a transaction with respect to *gharar*, the Islamic jurist is divided. Hanafi think tank claimed that the knowledge of the goods and their attributes as criteria for validating the transaction. Anyway, it is important for enforceability in case the conflict between the contracting parties occurs in the future. On the contrary, the Shafi'is claim that knowing both the essentials and attributes of the counter values is a prerequisite for validity and a sale whereby the buyer fails to see the object is invalid because of excessive *gharar*.

The anonymity of Internet users like traders add to the challenge of describing *gharar* in its new dimension. The subject matter was hidden from the buyer without the buyer knowing its future results exactly. There are also three main issues for *gharar* in online transactions: uncertainties about the goods or the services themselves, uncertainties about cost, delivery and postponement. Certain respondents still have doubts about *riba*, *maysir*, *gharar* and *ikhrah* (duress) free e-commerce. Respondents are questionable as to the free use of e-commerce (*riba*, *maysir*, *gharar* and *ikhrah*). Consumers are also concerned about the fitness of real goods with the photos posted on websites by sellers [31].

The Islamic trade ethics therefore require that sellers clearly identify the goods being offered; for example, the image of the goods with the information, costs, mode of delivery and payment must be clearly shown on the screen. Secondly, all the negotiating parties; sellers and purchasers must be able to communicate with each other in order to achieve compliance with the agreement between them. Furthermore, a supplementary contract such as option (*khiyar*) can be added [30].

E-commerce not only introduces the new dimension to *gharar* 's problems, but also the essence of e-commerce outside territorial borders brings new challenges to its implementation. *Gharar* coping with fraud and dissatisfaction proposes a legislative mechanism to answer the problems in question. While e-commerce is global in nature, laws relating to the protection of e-commerce customers require local compliance. The Consumer Claims Tribunal was formed in Malaysia in 1999 under the Consumer Protection Act for a very long time. Anyway, the Act removes from its scope electronic transactions. In this respect, new legislation to include e-commerce transactions to protect consumers [8] is strongly recommended.

3 Sound technological means

Securing an online transaction must satisfy two key requirements: firstly, how data are secured (confidentiality) and how the credibility of the transaction itself is guaranteed. Confidentiality guarantees that only the approved party's access to and receipt of information travelling online. Secrecy and secrecy are also related to confidentiality. On the other hand, Trusted Network Interpretation defines that the integrity ensures that computerized data are the same as those in source documents; they have not been exposed to accidental or malicious alteration or destruction [9].

In order to ensure transparency in the sense of online communication [10], the data sent should be ensured as follows:

i. Data must be protected against changes in content – including insertion, erasure, translation and modification of the content of a message.
ii. The data must be safe from time shift – delay or replay messages.
iii. Source repudiation – failure of message transmission by source.
iv. Refusal of destination – denial of receipt by destination.

If a person in the middle is able to intercept the message sent to a dealer, he could not actually alter the message (i.e. quantity of order), but repeat the same message to buy the product over a number of times. The process must provide defense against denial of involvement by one of the individuals participating in a conversation. The origin and sender as well as the destination have confirmation that the message has been sent and received. For example, if a customer made a payment online, the merchant does not reject it. Two main ways to meet the above requirements – Encryption and Digital Signature.

Credit card companies realized that most internet transactions only involve credit card details and expiry date, name, and address Information Both Visa and MasterCard developed the "Fixed" or Protected Electronic Transactions protocol involving leading

technology companies including Microsoft, IBM, Netscape, RSA, and VeriSign. As the specification is open and free, anyone can buy or sell online with SET-compliant software [11]. The focus of SET is to ensure confidentiality of information, to ensure the integrity of messages and to authenticate transaction partners. It has been developed to use technology for authenticating the parties involved in payment card transactions on any form of online network and internet that uses Encryption and Digital Signature and Digital Certificates [12].

Transactional threats are another additional security issue. Every company must ensure that every party to the deal is really who they say (authentication), that transactions cannot be transmitted or corrupted (integrity) and that no party can refuse (non-repudiation) participation, and that transaction information remains private (confidentiality). Encryption and digital certificates [13] are the key methods used for transaction authentication, transparency, non-repudiation, and confidentiality. For example, in order to purchase goods via the Internet, users must place an order with a credit card number. Before sending it to the merchant, the credit card number must be encrypted. Encryption is a process in which straightforward data such as a credit card number is transformed into unreadable cypher text accepted in order to decrypt the scramble message into readable form by receiving the data. This ensures that the number of the credit card is not intercepted on the route, but that the data can be interpreted meaninglessly without the interceptor knowing how to scramble it. This prevents unscrupulous people from using the cypher text.

The method of encryption is completely secret from a user. Secure Socket Layer (SSL) is the most widely used technology for automated security. For example, when a URL starts with the https:/ prefix rather than the normal https:/, a browser uses encrypted content when accessing a page [14]. The browser may encrypt a message to keep it secret. Most reputable e-commerce sites are going to use a protected server, where the encryption displays a small lock in the lower right corner of the browser window. The symbol means that when the data is sent the data is encrypted [15].

Current trends have shown some terrific developments in the issue of credit card security. In 2016, Bank Negara Malaysia (BNM) encouraged the cardholders to move to new PIN-based payment cards by the end of the year as the new PIN-enabled infrastructure became operational by 1 January 2017 [25]. The transition takes place at a time when Malaysia is migrating from the existing signature-based transaction method to PIN transactions at point-of - sale (POS) terminals nationally. This decision definitely has strengthened the security system of both type of cards even though this initiative has initially received voluminous comments from the cardholders.

3.1 Digital signature application and certified authority to anonymity resolution

The article suggests that the digital signature be used to overcome anonymity in respect of protection and the authenticity of the Islamic legal system transaction. Although protecting data from the unauthorized party's contact will guarantee confidentiality, the data will not be secured against repudiation. There is an urgent need to protect the mes-

sage from repudiation. Someone sending a message must be responsible and accountable, and he or she can't refuse. On another side, anyone can not falsify a message and say it was another example of repudiation.

Digital signature is an authentication mechanism. It allows the recipient to know a sender of a given electronic document in the same way that the conventional signature enables the recipient to know and cannot be forged the sender of a written document.The digital signature created by the sender's personal key for encrypting information about the document is not simply a scanned version of a traditional signature [14]. Digital Signature seeks to mimic the hand-written signature that marks the signature owner in a special way. The ability to ensure the original signed message is received means the sender cannot deny it later. This process resolves the rejection of the destination where the recipient cannot actually refuse to accept the message. Digital signatures are easy to carry and cannot be replicated or generated by anyone else and can be stamped atomically.

The digital signature supplements the encryption, even though it is not used together. It can be used for any form of message, whether or not it is encrypted. The recipient may simply be confident of the identity of the sender and the message has arrived intact. The presence of two contracting parties must be established and acknowledged before any deal, purchase or deal can be reached in the e-commerce transaction. The use of digital signatures helps Ijab and Qabul to satisfy the requirements for both parties (buyers and sellers) in Bai-Salam.

Also involved in solving any possible conflict regarding authentication and transaction confidentiality is the Certificate Authority (CA). The trusted third party or certificate authority ensures that the message is delivered in a form. The general idea is to trust a certificate authority so that users can delegate the building, issue and acceptance of certificates as well as cancellation of certificates to the authority. [16] cited the following as the relevant actions of the certificate authority:

i. Management of public certificates for the entire life cycle.
ii. Issue certificates by adding a user or device identity with a digital signature to a public key.
iii. Scheduling of certificate expiry dates.

All should check that the certificate is real and that it is issued by the party. Digicert Sdn in Malaysia. Since 1998, Bhd has been the first CA in the country. Digicert Sdn. Digicert. Bhd is a trusted third party that provides both parties with a digital certificate to secure their transaction [17]. Although both the buyer and the merchant are concerned with the payment only, the CA encourages and concentrates on preserving information security and ensuring that the message credibility is maintained and authenticating the parties involved in the transaction.

All the underlying mechanism is performed at a transport level in a protected socket layer in a five-layer Internet protocol. For example, Maybank, the world's leading business bank that implements the 128-bit Verisign Certificate Authority Secure Sockets Layer (SSL) encryption protocol, for all information exchanged over the internet between users as well on its own network and resources [18]. Maybank also adopts

WebTrust Best Practices, an independent company which oversees and tests the facilities to ensure that the highest and most current standards of Internet information security and exchange are maintained.

3.2 Implementation of the session key to overcome time validity period in meeting time and place in Shariah's principle

By using session key, the duration of validity at the meeting site can be overcome by an Authentication Protocol Authorisation and Authorisation Technique. The protocol is usually used to check that the communications partner is not an impostor [12]. The distinction between authentication and authorization is whether a individual interacts with a particular process and whether or not the individual approved for that particular process or operation. For example, the first question arises when two parties enter into an agreement and a contract online, whether the communicating parties "speak" to the trusted parties. The first question is more important to be answered explicitly before the next step starts, where entries in local databases are simply checked in order to verify if the authority to close the deal is granted to him or her.

While the use of the session key is used exclusively for authorization, time validity may be extended. After the conversation is over, the session key can be discarded cheaply [12]. The introduction of the main session therefore addresses issues of meeting place and time in the Islamic transaction of the contracting parties. This is the same situation as the *Bai-Salam* [32], where the payment has to be made in the same Majlis. A trusted third party is involved in order to guarantee and reassure the receiver that the message received is not interrupted.

3.3 Financial Process Exchange (FPX)

FPX is an alternative payment channel for consumers who pay for their consumers on e-market locations such as websites and on-line stores. FPX is a stable internet banking fund that does not require a credit card. However, any transaction needs electronic authorization, and the debits are automatically deducted from the user's account. Transactions are encrypted using the customer's Personal Identification Number (PIN) online account to improve the protection of their user account [19]. For a safe transaction of e-payment, security software 'seller plug-in' is installed on the merchant's web server [20]. In order to ensure that the data transmitted between bank and customer is totally confidential, a 128-bit encryption technology like SSL is adopted.

To ensure a secure transaction, FPX uses authentication and SSL certification. Using both server automation and data encryption, customer access the payment section of online stores or e-commerce website can pick the preferred bank for debiting and SSL is automatically protecting customer details. The protected website with SSL was directly accessible to the website of the bank for user ID / PIN and password (authentication). The sales value was debited from the customer's account and a confirmation of transaction was obtained by the customer and retailer.

In Malaysia, FPX participated banks are Ban Islam, CIMB, Maybank, Public Bank, RHB Bank, Citibank, Deutsche Bank, Hong Leong Islamic Bank, HSBC, OCBC and

Standard Chartered Bank. Each bank has a unique online banking security function and authentication process. All clients were provided by PIN and passwords, with an extra secure system touch button (e.g. HSBC bank), a 6-digit computer-generated transaction authorization (TAC) code which provides a second layer of authentication before a customer can conduct a specific online transaction (e.g. Maybank, CIMB). In addition, when there is no preset operation (i.e. 5 minutes), online banks have an automatic timeout feature to help protect them against unauthorized access.

FPX is run by the Malaysian Electronic Payment System (1997) Sdn Bhd subsidiary, FPX Payment Sdn Bhd [21]. MEPS provides the banks with both a technological and interbank switching and routing infrastructure. MEPS also manages on behalf of banks clearing and settlement. Bank Negara Malaysia now has e-commerce doors open, particularly for businesses (B2B) and commercial payment (B2C), in collaboration with MEPS and all financial institutions in Malaysia. It leverages the participating banks' internet banking services and provides fast, stable, reliable and real-time online payment processing. As funds pass between existing financial institutions, FPX offers full end-to-end corporate transaction details, resourceful payment records, streamlined reconciliation, and reduced risk [22].

4 Regulatory body

4.1 Shariah committee

Bank Negara Malaysia has amended the Central Bank of Malaysia Act of 1958 in order to improve the role and functions of its Islamic Banking and Takaful Shariah Advisory Committee (SAC). At least one proposed member of the Shariah Committee shall have the knowledge, skills, and/or experience required in Islamic jurisprudence (*Usul al-Fiqh*) or Islamic transaction / commercial law (*Fiqh al-Muamalat*) [23].

The Shariah Committee's key roles and obligations are:
i. To guide the Shariah Board in its business activities.
ii. To support Shariah manuals of compliance.
iii. Supporting and validating relevant documents.
iv. To assist related parties in matters concerning Shariah on request.
v. Advising the SAC on matters to be referred.
vi. To have Shariah's written opinion.
vii. To support the SAC in providing guidance.

But it shows that the role and purpose of the Shariah Committee only in Malaysia is focused on financial institutions such as banking and takaful. The role of Shariah advisors in other industries such as e-commerce needs to be established. The SAC of Bank Negara Malaysia will be supplemented by the Shariah Advisory Body, which is to be known as the Shariah Committee.

E-commerce purchases are currently outside the SAC's roles and obligations. As the paper indicates, the Shariah enforcement process needs a systematic approach about the legality of the transaction itself from the Shariah point of view, an efficient technical

approach as well as current regulations and legislation supporting e-commerce. The paper therefore recommends that SAC include the e-commerce transaction in its supervision. The SAC will serve as an advisory board for the Islamic e-commerce transaction on Bank Negara, rather than as a regulatory authority. Extensive research needs to be carried out on how SAC can affect the Islamic online transaction, but the main objective of the incorporation is initially to facilitate the Shariah-based transaction into the e-commerce transaction.

5 Legal provision

5.1 Digital Signature Act (DSA)

The Digital Signature Act 1997 was implemented to meet the global and technical needs of the electronic commerce. Two years after the government initiated the Multimedia Super Corridor Mega project, the Act came into force in 1998. The Act requires a digital signature document to be as legally binding as a conventional signature or an appended thumbprint or any other mark, and that the digital signature produced in compliance with the Act shall be treated as a legally binding signature. The message is also listed as valid, enforceable and effective as if it had been written on paper when it bears a digital signature and the signature is checked according to the procedure laid down in the act [24].

Technological methods to recognize all parties during a transaction cannot be sufficiently persuasive to protect business law. Legal security has been regulated to provide consumers and companies with a complementary solution, apart from the systems of encryption and digital signature. Although this problem is not solved by international treaties, DSA is an essential tool and forum to secure electronic commerce. With respect to global electronic commerce, recognition issues for international parties will always occur.

5.2 The Digital Signature legal binding

As mentioned above, as long as digital signature is produced according to DSA, the effect of the signature is equivalent to any other hand-written signature, thumbprint, or trademark, it is therefore legally mandatory (section 62 DSA). Section 64 DSA allows for the transmission of a digitally signed document as a written document. Copies of a digitally signed document may also be performed as an initial in compliance with Section 65 DSA. In section 67, the presumptions provide an even stronger justification for depending on a digital signature:

A certificate that is digitally signed by a Certification Authority (CA) is provided by the CA, and approved by a subscriber, whether it is either published in a recognized registry, or made publicly available to the CA or subscriber; that the certificate's information is correct:

i. The digital signature is the subscriber's signature.
ii. The subscriber intends to sign the message.

iii. The receiver has no information or warning that the signer has violated a subscriber's obligation or is not the legitimate private keyholder (see discussion below).

The assumption above suggests that the subscriber may violate a subscriber obligation by disclosing a private key to any unlawful group. The criminal group then abuses the key and masks itself as the recipient's actual subscriber. The unlawful party can unlawfully copy or rob the private key and sign the digital certificate with or without the approval of the subscriber. The presumptions require the signatory to prove that the digital signature is not or is not properly attached to it. The practical implications of this will be that the possibility of a fraudulent signature is now the signer (subscriber).

5.3 Duties and liabilities

Subscribers: Subscribers must exercise due caution in section 43 DSA to ensure that their private key is exposed to an unauthorized individual. In section 41 of the DSA, the subscribers should take any loss or damages incurred by false material claims or by non-disclosure in the event of misleading intent or negligence of the representation or no-disclosure.

As the sole owner of a certificate, the subscriber's representation is as follows:

i. The exclusive possession of the subscriber to a third party.
ii. The CA representations and the certificate details are valid.
iii. All statements made to the CA or in the certificate are valid even if not verified by the CA.

Trusted third parties (CA): Section 29 DSA clarifies that the sender CA needs to confirm when it receives an issuance request:

i. The identity of a prospective subscriber the following condition must be given before issuing a certificate CA.
ii. The certificate data are accurate.
iii. The prospective subscriber shall be the legitimate private key holder.
iv. The private key will generate a digital signature.
v. A public key to be identified in the certificate will check the digital signature affixed to the subscriber's private key.

Section 36 DSA requires CA certification of someone who relies fairly on the certificate:

i. The certificate data are accurate.
ii. The reliability of the certificate requires all details foreseeably material.
iii. The certificate has been approved by the subscriber.

Under section 30 of the DSA CA is also required by law to print, upon approval by the subscriber, a signed copy of the certificate, unless the arrangement between the CA

and the subscriber provides otherwise. In compliance with section 35 DSA, the CA is liable to the subscriber to act promptly when the certificate is revoked. CA shall inform the subscriber of any known facts that substantially affect the reliability or validity of the certificate.

6 Conclusions

The article highlighted detailed discussion of e-commerce transactions to conform with the principles of shariah. In addition, a holistic approach to the implementation in a real world is urgently needed. In this article are included all related structures including sound internet infrastructure, lawmaking and law enforcement, SAC and Bank Negara regulators, e-commerce players such as banks and financial institutions and, last but not least, current acts and laws concerning online transactions. In addition, this article may also act as a general e-commerce guide for more than one billion Muslim ummah worldwide.

Like others, we also acknowledge two limitations, which are not really addessed in the current study. First, our discussion on the issue concerned rather on Malaysia without pin pointing broad context of investigations. Future studies, may extend the idea of the present study to capture broad geographies to understand the concept and model between developed and developing Muslim countries to extend the findings. Second, our results obtained are based on library research approach and perhaps may not offer new viewpoint pertinent to Shariah e-payment model. This is considered a drawback since the e-payment system are kept on changing due to the growing digital technology, society and economy. Given this assertion, future studies may consider empirical investigations to produce a more comparable outcome for improved inferences.

References

1. Md Fazlur Rahman A.: Economic doctrines of Islam. Seerah Foundation, UK (2016).
2. Adil, S.: Shahih Muslim: With full commentary by Imam Nawawi. Islamic Foundation, USA (2019).
3. Kazi, M.: Malaysian banks launch first Islamic credit card in Asia, http://www.islam-online.net/English/news/2002-07/25/articles06.shtml, last accessed 2018/08/28.
4. Arsyianti, L. D., & Adelia, A.: Sharia compliance-credit card exposure and utilization in the growing digital economy. Journal of Islamic Monetary Economics and Finance 5(4), 891-918 (2019).
5. Johan, Z. J., Hussain, M. Z., Mohd, R., Kamaruddin, B. H. Muslims and non-Muslims intention to hold Shariah-compliant credit cards: a SmartPLS approach. Journal of Islamic Marketing, (2020).
6. Khir, K., Gupta, L., Shanmugam, B.: Islamic banking: A practical perspective. Pearson, Selangor, Malaysia (2008).
7. Ibn Taymiyyah, T.D.: Nazariyyah al-'aqd. Dar al-Ma'rifah, Beirut, Lebanon (1317 A.H).

8. Kiranjit, K.: Consumers, civic groups, and the internet in Malaysia: A focus on the communications and multimedia consumer forum of Malaysia. In ASEAN Seminar on Social and Cultural Impact of The Internet in ASEAN, Public Relations Academy, Singapore (2003).
9. Boos, P., Lacoste, M.: Networks of trusted execution environments for data protection in cooperative vehicular systems. In Vehicular Ad-hoc Networks for Smart Cities (pp. 99-109). Springer, Singapore (2020).
10. Stallings, W.: Cryptography and network security. 7th edn. Prentice Hall, New Jersey (2016).
11. Lebichot, B., Le Borgne, Y. A., He-Guelton, L., Oblé, F., Bontempi, G. Deep-learning domain adaptation techniques for credit cards fraud detection. In INNS Big Data and Deep Learning Conference, pp. 78-88. Springer, Cham (2019).
12. Tanenbaum, A.S.: Computer networks. 5th edn. New Jersey: Upper Saddle River (2010).
13. Shelly, G.B., Cashman, T.J., Napier, H.A., Judd, P.J., Kaufmann, E.: Discovering the internet: Complete concepts and techniques. Thomson Course Technology, USA (2004).
14. Comer, D. E. The internet book: Everything you need to know about computer networking and how the internet works. 5th edn. Taylor & Francis, USA (2018).
15. Adams, T., Scollard, S.: Internet effectively: A beginner's guide to the world wide web. Pearson/Addison Wesley, USA. (2006).
16. Pfleeger, C., Margulies, J.: Security in computing. 5th edn. Pearson Education, USA (2015).
17. MIMOS, http://www.mimos.com.my, last accessed 2020/08/20.
18. Rakkini, M. J., Geetha, K.: Secure decentralized public key infrastructure with multi-signature in blockchains. In Inventive Communication and Computational Technologies (pp. 451-461). Springer, Singapore (2020).
19. Hassan, M. A., Shukur, Z., Hasan, M. K.: An efficient secure electronic payment system for e-commerce. Computers 9(3), 66 (2020).
20. Nordin, N., Zaidi, M. F. A., Yaacob, N. A., Kosaka, M., Tio, M., Yeoh, S. L.: Value co-creation between stakeholders in Malaysia's automotive aftermarket e-commerce industry: A case study of sparke autoparts. In Business Innovation with New ICT in the Asia-Pacific: Case Studies (pp. 281-303). Springer, Singapore (2020).
21. Ye, S., Zhu, Y., Lu, E.: The innovation of retail banks in the cross-border payment fund transfer system: Take OCBC as an example. Modern Economy 10(05), 1479 (2019).
22. Nurma, E.: Pengaruh model antrian dan waktu menunggu (idle time) terhadap efektivitas pelayanan kepada nasabah tabungan. Almana: Jurnal Manajemen dan Bisnis 3(2), 417-430 (2019).
23. Masruki, R., Hanefah, M. M., Dhar, B. K.: Shariah governance practices of Malaysian islamic banks in the light of Shariah compliance. Asian Journal of Accounting and Governance 13, 91-97 (2020).
24. Khan, S., Khan, N., Tan, O.: Efficiency of legal and regulatory framework in combating cybercrime in Malaysia. In Understanding Digital Industry: Proceedings of the Conference on Managing Digital Industry, Technology and Entrepreneurship (CoMDITE 2019), pp. 333. Routledge, Bandung, Indonesia (2020).
25. Guerar, M., Migliardi, M., Palmieri, F., Verderame, L., Merlo, A.: Securing PIN-based authentication in smartwatches with just two gestures. Concurrency and Computation: Practice and Experience 32(18), e5549 (2020).
26. Izzat, A., Mohammad, Z.: Building an Islamic financial information system based on policy managements. Journal of King Saud University–Computer and Information Sciences 27, 364–375 (2015).
27. Norazlina, Z., Fauziah, O., Siti Hartini, M.: E-Commerce from an Islamic perspective. Electronic Commerce Research and Applications 3, 280–293 (2004).

28. Tamrin, A., Ainnur Hafizah, A.M., Mohd Zulkifli, M., Mohamad Fauzan, N., Roslina, O.: Development method for Shariah compliant e-commerce payment processing. International Journal of Computer Theory and Engineering 7(5), 408-415 (2015).
29. Marjan, M., Muhd Rosydi, M., Mohd Adam, Husnayati H, Mohamed Jalaldeen M.R., Kalthom, A.: Building trust in e-commerce from an Islamic perspective: a literature review. American Academic & Scholarly Research Journal 5(5), 161-168 (2013).
30. Al Arif, M.N.R.: Penjualan on-line berbasis media sosial dalam perspektif ekonomi Islam. Ijtihad: Jurnal Wacana Hukum Islam dan Kemanusiaan 13(1), 33-48 (2013).
31. Muhammad Kholifatul I., Ardiansyarh, Y., Budi, H.: Shari'ah-compliant e-commerce models and consumer trust. Al-Iqtishad: Jurnal Ilmu Ekonomi Syariah (Journal of Islamic Economics) 8(2), 243-254 (2016).
32. Ainnur Hafizah, A.M., Mohd Zulkifli, M., Tamrin, A., Mohd Sarwar, E.A.: Bai as-salam and e-commerce: a comparative analysis from Shariah perspectives. In Proceedings of The 2nd Applied International Business Conference (AIBC2013) pp. 522-529, Labuan (2013).
33. Nor Azah, J., Al-Hasan, A.: Online dropship for business transaction in Malaysia: Views from muslim scholars. International Journal of Islamic Business 1(1), 13-28 (2016).