JFatwa ISSN: 2232-1047 eISSN: 0127-8886
Journal of Fatwa Management and Research
مجلة إدارة وبحوث الفتاوى | Jurnal Pengurusan dan Penyelidikan Fatwa
MAY 2025 | VOL. 30 | NO. 2
ISSN: 2232-1047 eISSN: 0127-8886
www.jfatwa.usim.edu.my

SHARIAH-COMPLIANT E-PAYMENT FRAMEWORK IN MALAYSIA: INTEGRATING FIQH, DIGITAL SECURITY AND REGULATORY GOVERNANCE

Mohd Zulkifli Muhammad[1a], Fatihah Mohd[2b*], Tamrin Amboala[3c], Hanudin Amin[4d], Wan Fatin Fatihah Yahya[5e], Muhammad Khalilur Rahman[6f], Azila Jaini[7g] and Mohammad Salim Al-Rawashdeh[8h]

[a,b,f]Faculty of Entrepreneurship and Business, Universiti Malaysia Kelantan, Kelantan, MALAYSIA
E-mail: zulkifli.m@umk.edu.my[1]
E-mail: fatihah.m@umk.edu.my[2*]
E-mail: khalilur.r@umk.edu.my[6]
[c]Faculty of Computing and Informatics, Universiti Malaysia Sabah, Labuan, MALAYSIA
E-mail: tamrin@ums.edu.my[3]
[d]Labuan Faculty of International Finance, Universiti Malaysia Sabah, Labuan, MALAYSIA
E-mail: hanudin@ums.edu.my[4]
[e]Faculty of Computer Science and Mathematics, Universiti Malaysia Terengganu, MALAYSIA
E-mail: wanfatin@umt.edu.my[5]
[g]Faculty of Business and Management, Universiti Teknologi MARA, Segamat, MALAYSIA
E-mail: azilajaini@uitm.edu.my[7]
[h]International Relations, Al-Balqa Applied University, Princess Alia'a University College, Amman, JORDAN
E-mail: jordanresearch@bau.edu.jo[8]

*Corresponding Author: fatihah.m@umk.edu.my
Received: 20 October 2024 *Accepted: 28 April 2025* *Published: 30 May 2025*
DOI: https://doi.org.10.33102/jfatwa.vol.30no2.638

ABSTRACT

The rapid growth of e-commerce and digital payment systems presents significant challenges for Shariah compliance, particularly concerning riba (usury), gharar (uncertainty), and the validity of online contracts. Despite Malaysia's increasing adoption of e-payment systems, a structured framework ensuring full adherence to Islamic principles remains lacking, leading to uncertainties in contract legitimacy, transactional risks, and regulatory oversight. This study aims to develop a Shariah-compliant solutions for e-payment systems by integrating Islamic legal principles, technological safeguards, and regulatory measures. Using a qualitative approach, the study analyzes Islamic jurisprudence, regulatory guidelines, and technological solutions to identify core Shariah concerns, such as riba in credit-based transactions and the need for a dedicated regulatory body. The proposed solutions includes a Shariah compliance framework, robust encryption and digital signature mechanisms, a specialized Shariah advisory body for e-commerce, and legal provisions to govern online transactions. The findings provide a structured approach for policymakers, financial institutions, and e-commerce stakeholders, contributing to the advancement of Islamic fintech and supporting Malaysia's position as a global leader in Islamic digital finance.

Keywords: *E-payment; e-commerce transaction; shariah-compliant.*

1. INTRODUCTION

The integration of information technology with commerce has introduced increasingly complex layers to Islamic business and commerce ethics, necessitating that Islamic jurisprudents expand their evaluative and analytical tools beyond traditional frameworks. This article adopts a comprehensive approach, incorporating regulatory considerations and existing technological tools within the Shariah solutions, to explore and develop solutions that provide Islamic alternatives to conventional e-commerce transactions.

E-commerce is permissible within Islam, provided it adheres to the stipulations of Islamic contract law, namely: (i) form, (ii) contracting parties, and (iii) subject matter. These requirements are fundamental to ensuring that the primary objective of commerce in Islam—protecting the interests and eliminating harm to the parties involved in commercial transactions—is successfully achieved (Marjan et al., 2013). However, online transactions present significant challenges from a Shariah perspective, including concerns related to security, the legality of contracts, anonymity, riba (usury), and gharar (uncertainty). Addressing these issues necessitates that Islamic jurists and scholars meticulously examine both the technical aspects of online transactions and their legality in terms of Shariah compliance (Sheraz et al., 2021).

Islam places great importance on the trading sector as a source of wealth and a driver of national and communal development. The Quran contains numerous references to trade and commercial activities, underscoring their significance. The following Quranic verses substantiate this perspective:

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

Islam grants equal rights to both producers and consumers, ensuring they can exercise their rights as needed. Regardless of the mode of business, every Muslim is obligated to conduct business with faithfulness and God-consciousness, adhering to the principles of the Quran and Sunnah. Most importantly, their intention should be for the sake of Allah SWT, rather than purely for worldly gains (Abozaid & Khateeb, 2022; Dadach, 2020; Norazlina et al., 2004).

While few studies have aimed to develop solutions suitable for the current Islamic financial system, notable efforts exist. One study proposed a solutions based on eXtensible Access Control Markup Language (XACML) policy management, demonstrating how an Islamic financial information system can assist in day-to-day banking decisions. Such systems are essential for all Islamic banks worldwide, which currently rely on advisory boards to provide opinions on general activities. The gap between these high-level general rules and the specific decisions for each customer's business process can be bridged by Islamic financial information systems (Izzat & Mohammad, 2015). Another study suggested the inclusion of an Intermediate Shariah Transaction Party (ISTP) to act as an intermediary between merchants and customers before transactions are finalized. This design aims to streamline the e-commerce transaction process and address common issues such as riba (usury), gharar (uncertainty), and the validity and legality of e-commerce transactions from a Shariah perspective, without compromising transaction security (Tamrin et al., 2015).

Given the complexity of modern business and commerce transactions, it is crucial to develop new solutions and methods for contemporary Islamic transactions. This necessitates combining various approaches, including information technology, e-commerce infrastructure, and regulatory frameworks, and making adjustments and modifications to ensure they align with Shariah principles.

2. LITERATURE REVIEW

2.1 *Sound Technological Means*

Ensuring secure online transactions involves fulfilling two primary requirements: first, safeguarding data from unauthorized access (confidentiality), and second, ensuring the integrity of the transaction itself. Confidentiality ensures that online data transmission is received and accessed only by authorized parties, and it is often associated with concepts of secrecy and privacy. Conversely, according to the Trusted Network Interpretation, integrity ensures that computerized data remain unchanged from their source documents and are not susceptible to accidental or malicious alteration or destruction. To ensure integrity in the context of online communication, Stallings (2003) suggests that the transmitted data must meet the following criteria:

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 a message by source
iv. Destination repudiation- denial of receipt of the message by destination

If a man-in-the-middle intercepts a message sent to a merchant, they could not only modify the message (e.g., altering the order quantity) but also replay the same message multiple times to repurchase the product. The mechanism must prevent denial by any party involved in a communication, ensuring both the sender and recipient have evidence of message transmission and receipt. For instance, if a customer makes an online payment, the merchant cannot deny receiving it. These requirements can be met through two main methods: encryption and digital signature (Roper, 2023).

Credit card companies recognized that most internet transactions only require entering credit card information such as the card number, expiry date, name, and address. Both Visa and MasterCard developed a protocol called Secure Electronic Transaction (SET) with input from leading technology companies like Microsoft, IBM, Netscape, RSA, and VeriSign. Since the specification developed is open and free, anyone can utilize it or develop SET-compliant software for online buying or selling. SET focuses on maintaining the confidentiality of information, ensuring message integrity, and authenticating the parties involved in transactions. It utilizes technology to authenticate parties involved in payment card purchases on any type of online network or internet using encryption, digital signatures, and digital certificates.

Transactional risks present additional security concerns for businesses. Every company must verify the identities of all parties involved in a transaction (authentication), ensure the integrity of transactions during transmission to prevent interception or corruption (integrity), uphold the participation of all parties in a transaction without denial (non-repudiation), and maintain the privacy of transaction information (confidentiality). Encryption and digital certificates are the primary tools used to achieve transaction authentication, integrity, non-repudiation, and confidentiality (Wang & Ren, 2024).

For instance, when purchasing goods over the Internet, a user must submit an order accompanied by a credit card number. Before sending the credit card number to the merchant, it must be encrypted. Encryption involves transforming plain data, such as a credit card number, into unreadable ciphertext, which can only be decrypted by the receiving end. This ensures that even if the data is intercepted en-route, it remains meaningless to the interceptor without knowledge of the decryption method, thereby preventing misuse by unscrupulous individuals.

The encryption process is transparent to the user, with the Secure Socket Layer (SSL) being the most widely used technology for automated security. SSL enables a browser to encrypt messages, ensuring the content remains private. For example, when a URL begins with "https://" instead of "http://," the browser automatically uses encryption when accessing the page. Reputable e-commerce sites typically use a secure server with encryption, indicated by a small lock icon in the browser window, signifying encrypted data transmission.

Recent developments in credit card security have seen significant advancements. In 2016, Bank Negara Malaysia (BNM) encouraged credit and debit cardholders to transition to new PIN-based payment cards by the end of the year, as the new PIN-enabled infrastructure became effective on January 1, 2017. This move coincided with Malaysia's migration to PIN-based transactions at Point-of-Sale (POS) terminals nationwide, replacing the existing signature-based transaction system. Although this initiative initially received extensive feedback from cardholders, it has undoubtedly strengthened the security of both types of cards.

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

The article suggests the use of Digital Signatures to address anonymity concerns related to the security and validity of transactions within the framework of Islamic legal systems. While ensuring data security against unauthorized disclosure ensures confidentiality, it does not safeguard against repudiation. Messages must be protected against repudiation, meaning that the sender cannot deny sending a message or falsify a message and claim it came from someone else.

Digital signatures serve as a mechanism for authentication. They enable a receiver to verify the sender of an electronic document, similar to how a conventional signature verifies the sender of a written document, and cannot be forged. Digital signatures are created by encrypting information about the document using the sender's private key and are not simply a scanned version of a conventional signature (Comer, 2007; Esayas, 2024). Digital Signatures aim to replicate handwritten signatures, uniquely identifying the signature owner. Ensuring that the original signed message arrives intact means that the sender cannot easily deny it later, thereby resolving issues of repudiation by the recipient. Digital signatures are portable and immune to copying or fabrication by unauthorized parties, and they can be automatically time-stamped.

While digital signatures complement encryption, they are not necessarily used together. They can be applied to any type of message, whether encrypted or not, providing the receiver with assurance of the sender's identity and the integrity of the message. In e-commerce transactions, prior to any deal, purchase, or agreement, the existence of both contracting parties must be established. The application of digital signatures facilitates the fulfilment of the conditions of Ijab and Qabul for both parties (buyers and sellers) in Bay al-Salam transactions.

Certificate Authorities (CAs) are also involved to address potential conflicts regarding authentication and transaction confidentiality. Acting as trusted third parties, CAs ensure that received messages remain in the same form as when they were sent. The underlying principle is that users trust the certificate authority, allowing them to delegate the construction, issuance, acceptance, and revocation of certificates to the authority. (Pfleeger & Pfleeger, 2015) 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 the authenticity of the certificate and its issuer. In Malaysia, Digicert Sdn. Bhd has been the country's first Certification Authority (CA) since 1998. Serving as a trusted third party, Digicert Sdn. Bhd issues digital certificates for both parties involved in transactions to enhance security (MIMOS, 2009). While buyers and merchants focus on payment and the delivery of products or services, the CA ensures confidentiality, and message integrity, and authenticates the parties involved in the transaction. These processes occur within a Secure Socket Layer (SSL) at the transport level of a five-layer Internet protocol. For example, Maybank, a leading commercial bank in the country, implements the 128-bit SSL encryption protocol from Verisign Certificate Authority for all information transmitted over the Internet among users and within their own network and resources (Azni et al., 2024). Maybank also adopts Best Practices Maybank from WebTrust, an independent corporation that monitors and tests facilities to ensure the highest standards of Internet information security and exchange.

2.3 *The Application of Session Key to Resolve Time Validity Period in Meeting Time and Place in Shariah's Principle*

The validity period concerning the meeting place can be addressed through an authentication and authorization technique in Authentication Protocols, utilizing a session key. Generally, this protocol verifies that the communication partner is not an impostor (Tanenbaum & Wetherall, 2010; Wang & Ren, 2024). The distinction between authentication and authorization lies in determining whether a person is communicating with a specific process versus whether they are permitted to carry out a specific process or activity. For example, when two parties engage in a deal or contract online, the initial concern is whether they are communicating with trusted entities. This primary question must be definitively answered before proceeding to the next step, which involves simply checking entries in local databases to ascertain the level of authority granted to close the deal.

Although the session key application is primarily utilized for authorization, it can also be extended to validate time validity. Once the communication ends, the session key can be easily discarded (Tanenbaum & Wetherall, 2010; Wang & Ren, 2024). The application of the session key thus resolves issues related to the meeting place and time for contracting parties in Islamic transactions. This aligns with the conditions required in Bay al-Salam transactions (Ainnur Hafizah et al., 2013), where payment must be settled in the same Majlis. To ensure and reassure the receiving party that the message received has not been tampered with, the involvement of a trusted third party is necessary.

2.4 *Financial Process Exchange (FPX)*

FPX serves as an alternative payment channel allowing customers to make payments at e-marketplaces such as websites and online stores, and enabling corporations to collect payments from their customers. It offers a secure Internet banking fund transfer method, eliminating the need for a credit card for transactions. Each transaction requires electronic authorization, with debits instantly deducted from the user's account. To enhance account security, FPX employs the customer's online account personal identification number (PIN) authentication system.

For secure e-payment transactions, merchants install 'seller plug-in' security software on their web servers (Roper, 2023). Utilizing 128-bit encryption technology like SSL ensures that data transmitted between the bank and the customer remains fully confidential, as the data is sent in encrypted format. FPX employs authentication and SSL certification to ensure secure transactions. When customers access the payment section of online stores or e-commerce

websites, they can select their preferred bank for debiting, with SSL automatically protecting customer information through server authentication and data encryption. Upon accessing the secured site with SSL, customers are directed to the bank's Internet banking website to log in using their User ID/PIN and Password for authentication. The purchase value is then debited from the customer's account, with both the customer and merchant receiving a notification confirming the transaction.

Participating banks in FPX in Malaysia include Bank Islam, CIMB, Maybank, Public Bank, RHB Bank, Citibank, Deutsche Bank, Hong Leong Islamic Bank, HSBC, OCBC, and Standard Chartered Bank. Each bank offers unique security features and authentication processes for online banking. Customers are provided with a PIN and password, along with additional security measures such as a secure touch button device (e.g., HSBC bank) or a Transaction Authorization Code (TAC) with a 6-digit computer-generated code (e.g., Maybank, CIMB), adding an extra layer of authentication before specific transactions can be performed online. Online banks also incorporate automatic timeout features, terminating sessions after a preset period of inactivity (e.g., 5 minutes), to safeguard against unauthorized access.

FPX is operated by FPX Payment Sdn. Bhd, a subsidiary of Malaysian Electronic Payment System (1997) Sdn. Bhd. (Aliha et al., 2019). MEPS provides technical support and interbank switching and routing infrastructure for banks, as well as managing clearing and settlement on their behalf. Through collaboration with Bank Negara Malaysia, MEPS, and all financial institutions in the country, e-commerce, particularly business-to-business (B2B) and business-to-commerce (B2C) payments, have been facilitated. FPX leverages the Internet banking services of participating banks, offering fast, secure, reliable, and real-time online payment processing. It provides comprehensive end-to-end business transactions, efficient payment records, simplified reconciliation, and reduced risks, as fund movements occur between established financial institutions.

3. METHODOLOGY

This study employs a qualitative research methodology to develop a Shariah-compliant solutions for e-payment systems, integrating Islamic jurisprudence, financial regulations, and technological solutions. The research methodology consists of the following key components:

3.1 *Research Approach*

The study follows a doctrinal and analytical approach, focusing on

Islamic legal texts, financial regulations, and e-payment system frameworks. It involves a detailed examination of primary sources such as the Quran, Hadith, and classical Fiqh literature, as well as contemporary Shariah rulings and fatwas on e-commerce and digital transactions.

3.2 *Data Collection Methods*

The study conducts an extensive review on existing Islamic financial principles, e-payment mechanisms, and regulatory frameworks. Scholarly works, journal articles, conference papers, and institutional reports from Bank Negara Malaysia (BNM), the Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI), and the Islamic Financial Services Board (IFSB) are analyzed. In addition, a qualitative content analysis is performed on Shariah rulings, regulatory guidelines, and technological reports to identify key compliance challenges and potential solutions for e-payment systems. The study also compares conventional and Islamic e-payment frameworks, highlighting differences in contractual elements, risk mitigation strategies, and regulatory structures.

3.3 *Analytical Framework*

The study applies the Maqasid al-Shariah (objectives of Islamic law) framework to evaluate the ethical and legal aspects of e-payment transactions. It assesses the compliance of digital payment solutions with Shariah principles such as the prohibition of riba (usury), gharar (uncertainty), and maysir (gambling). Additionally, the study incorporates risk analysis to examine potential security vulnerabilities in e-payment systems and their implications for Islamic finance. This research methodology ensures a comprehensive, multi-disciplinary approach in addressing the challenges of e-payment systems within the context of Islamic finance.

4. RESULTS AND DISCUSSION

4.1 *Core Shariah Requirements*

Islamic jurisprudence, particularly Fiqh Muamalat (law of commerce), outlines several types of transactions, including Murabahah (cost-plus sale) and Bay al-Mu'ajjal (deferred payment sale), among others. E-commerce, by its nature, falls under the category of Bay al-Salam. Bay al-Salam is a type of transaction where buying and selling occur in advance, such as in online drop shipping transactions (Nor Azah & Al-Hasan, 2016). Regarding Bay al-Salam, the Prophet Muhammad SAW said, 'Whoever pays in advance, make sure you fix the measurement and time limit.' Bay al-Salam is a contract in Islamic

finance where payment is made in advance for a specified product to be delivered later. This transaction structure ensures certainty and fairness in trade. However, in the context of e-commerce, several challenges arise in fulfilling the conditions of Bay al-Salam, which present a significant research problem requiring further examination (Fajriyyah et al., 2023; Md Fazlur Rahman, 1980).

Firstly, price fixation with Ijab (offer) and Qabul (acceptance) is a fundamental requirement, ensuring mutual consent between the buyer and seller. In conventional e-commerce platforms, price fluctuations, hidden fees, and dynamic pricing models challenge this principle. Additionally, automated transactions using artificial intelligence may alter prices dynamically, raising concerns about whether genuine ijab and qabul occur with full transparency. Secondly, the requirement to pay in cash or goods becomes complex in online transactions. Most e-commerce platforms rely on credit-based systems, deferred payments, or installment plans, which may involve riba (usury). Furthermore, the widespread use of digital wallets and third-party payment processors raises concerns about whether the payment is made in a Shariah-compliant manner, especially when interest-bearing accounts are involved.

Thirdly, the condition that payment must be made in the same Majlis (session) is difficult to maintain in e-commerce, where buyers and sellers interact asynchronously. Unlike traditional face-to-face transactions where acceptance and payment occur simultaneously, online purchases often involve delays in processing orders, confirmation emails, and third-party payment gateways. This time lag raises questions about the validity of ijab and qabul in online transactions. Fourthly, product identification and clarity are crucial in Bay al-Salam to avoid gharar (uncertainty). However, e-commerce platforms often display misleading product descriptions, altered images, or vague specifications. Customers may not have full knowledge of the product's exact condition, quality, or existence at the time of purchase, leading to potential disputes. The absence of physical inspection further complicates compliance with this requirement.

Finally, fixing a delivery date is a necessary condition in Bay al-Salam to ensure transactional certainty. In e-commerce, logistical challenges, supply chain disruptions, and vendor inconsistencies often lead to delays in product delivery. Some online sellers operate on a pre-order basis without guaranteeing a specific delivery timeline, which contradicts the Islamic principle that the delivery date must be clearly determined at the time of contract formation. Addressing these challenges requires a robust framework integrating Shariah principles with modern technological solutions. Smart contracts, blockchain technology, and regulatory oversight could play a crucial role in mitigating

these issues while maintaining compliance with Islamic jurisprudence. Further research is needed to explore how digital transactions can be structured to fulfill the conditions of Bay al-Salam without compromising Shariah integrity.

4.2 *E-commerce Transactional Risks*

In addition to ensuring the halal (permissible) nature of the product or service from a traditional perspective, Islam also emphasizes the importance of confidentiality and integrity in securing transactions (Akhlaq & Asif, 2024; Arif & Elfadel, 2024). The mode of transaction used in e-commerce is of significant concern in Islam, attracting considerable critical attention.

4.3 *Legality of Online Contract*

The formation of a contract requires two parties: one who makes an offer and another who accepts it. The offer represents a proposal indicating the offeror's willingness to form a contract, while the acceptance reflects the offeree's agreement to the terms. While the terms and conditions of a contract can be easily communicated online, issues arise regarding the meeting place. In traditional offline transactions, where both parties meet face-to-face, anonymity is not a concern. The importance of the concept of a meeting place in Islamic tradition is emphasized in the following hadith attributed to the Prophet SAW:

> *"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"* (Siddiqi, 2000).

The above hadith addresses both the concept of a meeting place and the time required to conclude an offer. In the Islamic commercial legal system, specifying a meeting place is necessary to extend the validity of an offer for a certain period, during which acceptance must occur. Additionally, by allowing for the annulment of the sale at any time before separation, the meeting place helps mitigate concerns of anonymity. Failing to address anonymity issues can compromise the security of the transaction itself.

4.4 *E-Payment Methods and Related Pertinent Sharia Issues*

Debit cards and credit cards are the two most common payment methods in e-commerce (Zhou, 2024). From an Islamic perspective, debit cards are

preferred over credit cards because they do not involve interest (usury) (Mohd Dali, 2014). Debit card transactions mirror real-time ATM withdrawals, transferring funds almost instantly from the consumer's bank account to the merchant's account.

4.4.1 *Issues of Riba*

On the other hand, credit cards raise several issues. Using credit cards to purchase goods online and then paying for those goods in instalments to the bank or issuing authority constitutes a form of loan to the cardholder. Therefore, the issuer should not receive more than the amount used for the purchase. However, the issuer is allowed to charge a fixed fee for administrative expenses, provided this fee does not increase with the amount of money used for purchases. Imposing a percentage fee on the amount of money used via credit cards constitutes riba (usury and interest), whether this percentage is labelled as a service charge, administrative expense, or a penalty for delayed payments. Both scenarios represent an usurious loan, which is a well-known form of riba in non-Islamic financial systems.

Literally, riba means an increase or growth. According to Islamic jurists, it is defined as usury or the practice of lending money at interest rates. In this concern, Islamic Fiqh Assembly issued its decision No. 108 (12/2) stating (Abozaid & Khateeb, 2022):

a. 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.
b. It is permitted to issue uncovered credit cards as long as no condition fixes usurious increases to be added to the 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 view the concept of credit cards as a medium for online payments? What Shariah principles are required for the functionality of a credit card? The Islamic credit card is an alternative to conventional interest-based credit cards. Islam permits the use of credit cards as long as they do not involve interest. In Malaysia, the doctrine of Bay al-Inah is recognized and used to validate credit card transactions (Sheraz et al., 2021).

The Bay al-Inah contract operates based on two separate agreements: Bay al-Mutlak (cash sale) and Bay Bithaman Ajil (deferred sale) (Husni, 2023). In the first agreement, the bank sells an item to the customer at an agreed price. In the second agreement, the customer sells the item back to the bank at a lower price. The difference between the two prices is the bank's profit, which is a predetermined amount. There is no penalty charged to the customer, and the customer is eligible for a rebate on the unutilized financing amount (Alhusban et al., 2021).

4.4.2 *Issues of Gharar*

Gharar, literally meaning fraud, is often associated with risk and uncertainty. To avoid gharar, both buyers and sellers must possess adequate information about the values they intend to exchange, including the existence, obtainability, quantity, quality, and attributes of the object, ensuring it can be duly delivered.

It is reported in a Hadith that the Prophet SAW prohibited transactions involving gharar. Commenting on this Hadith, Ibn Taymiyyah wrote that a gharar sale involves risk-taking and unlawfully consuming the property of others (Ibn Taymiyyah, 1317). According to Islamic jurists, it is necessary to prevent any contracting party from misleading the other party and using abusive means dishonestly, especially online, due to ignorance. Traditionally, gharar is used to describe two types of transactions: 1) sale of the unseen (bay al-gha'ib), such as the sale of crops not yet grown to maturity or fish in a pond, and 2) sale of the non-existent (bay al-ma'dum), where the sale object did not exist at the time of the contract.

Islamic jurists are divided in determining the validity of transactions with reference to gharar. The Hanafi school of thought asserts that knowledge of the products and their attributes is a prerequisite to validate the transaction. However, it is required for enforceability in case of disputes between the contracting parties. Conversely, 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, contributes to the complexity of defining gharar in its new dimension. In online transactions, major concerns regarding gharar include uncertainties over the products or services themselves, pricing and delivery uncertainties, and deferment (Muhammad Kholifatul et al., 2016).

Despite the doubts of some respondents, e-commerce is not entirely free from major prohibitions such as usury, gambling, fraud, and coercion. To address these concerns, sellers must clearly define the products offered, display clear images with detailed specifications, and provide pricing, delivery, and payment details. Additionally, both sellers and buyers must be able to exchange messages to achieve agreement, and sellers may include additional contracts such as options (khiyar) (Al-Arif, 2013).

E-commerce not only brings new dimensions to gharar issues but also poses new challenges due to its global nature. Given that gharar deals with fraud and deception, a regulatory framework is proposed to address these issues. Although e-commerce is global, legislation pertaining to consumer protection in e-commerce requires local enforcement. In Malaysia, the Consumer Claims Tribunal, established under the Consumer Protection Act in 1999, excludes electronic transactions from its scope. Therefore, it is strongly recommended that new legislation be enacted to include e-commerce transactions for consumer protection (Zeno, 2022).

4.5 *Roles of Regulatory Bodies on E-commerce Transactions*

4.5.1 *Shariah Committee*

Bank Negara Malaysia has revised the Central Bank of Malaysia Act 1958 to strengthen the responsibilities and functions of its Shariah Advisory Council (SAC) for Islamic Banking and Takaful. Any potential member of the Shariah Committee must possess either formal qualifications or sufficient knowledge, expertise, or experience in Islamic jurisprudence (Usul al-Fiqh) or Islamic transaction/commercial law (fiqh al-muamalat) (BNM, 2010).

The main duties and responsibilities of the Shariah Committee are:

i. To advise the board on Shariah matters in its business operation;
ii. To endorse Shariah compliance manuals;
iii. To endorse and validate relevant documentations;
iv. To assist related parties on Shariah matters for advice upon request;
v. To advise on matters to be referred to the SAC;
vi. To provide written Shariah opinion;
vii. To assist the SAC on reference for advice.

BNM has issued guidelines regarding the governance of Shariah Committees, primarily focusing on financial institutions such as banking and Takaful. However, there is a pressing need to delineate the roles of Shariah advisors in other sectors, particularly in e-commerce. Establishing a Shariah body within

industries, referred to as a Shariah Committee, would serve as a complementary entity to BNM's Shariah Advisory Council (SAC).

Presently, e-commerce transactions fall outside the purview of the duties and responsibilities of the SAC. This paper suggests that a comprehensive framework for Shariah compliance is imperative, encompassing the legality of transactions from a Shariah perspective, robust technological approaches, and relevant enactments and laws supporting e-commerce. Consequently, the paper proposes that the SAC extend its supervision to include e-commerce transactions. Rather than serving as a regulatory body, the SAC could function as an advisory council for Islamic e-commerce transactions under Bank Negara. Extensive research is required to explore how the SAC can influence Islamic online transactions, with the primary objective being the promotion of Shariah-based transactions within e-commerce.

4.6 *Legal Provision on E-Commerce Transactions*

4.6.1 *Digital Signature Act (DSA)*

In response to the global and technological demands of electronic commerce, the Digital Signature Act 1997 was enacted. The Act came into effect in 1998, following the launch of the Multimedia Super Corridor mega project by the government two years prior. According to the act, a document accompanied by a digital signature is deemed legally binding, equivalent to a traditional signature, thumbprint, or any other mark. A digital signature created in compliance with the act holds the same legal validity as a traditional signature. Moreover, a message containing a digital signature is considered valid, enforceable, and effective if it entirely bears the digital signature and the signature is verified in accordance with the procedures outlined in the act (Chandrashekhara et al., 2021).

While technological solutions for identifying parties involved in transactions may not fully satisfy the legal protection needs of businesses, the Digital Signature Act provides an additional layer of legal protection for both customers and businesses, supplementing the Encryption and Digital Signature mechanisms. Although no international treaties specifically address this issue, the Digital Signature Act is regarded as a crucial tool and platform for securing electronic commerce. However, challenges related to identification may persist, particularly when dealing with foreign parties in the context of global electronic trade.

4.6.2 *The Legal Binding of a Digital Signature*

As previously mentioned, a digital signature, when created in accordance with the Digital Signature Act (DSA), carries the same legal weight as any handwritten signature, thumbprint, or mark, thus rendering it legally binding (as stated in section 62 of the DSA). Section 64 of the DSA stipulates that a digitally signed document is to be treated as equivalent to a written document. Additionally, copies of digitally signed documents are recognized as enforceable originals under section 65 of the DSA.

Section 67 further strengthens reliance on digital signatures by introducing certain presumptions:

i. A certificate digitally signed by a Certification Authority (CA) is considered valid and accepted by the subscriber if it is either published in a recognized repository or provided by the CA or subscriber.
ii. The information contained in the certificate is deemed accurate.
iii. Verification of the digital signature using the public key listed in the certificate confirms:
    a. The digital signature belongs to the subscriber.
    b. The subscriber intended to sign the message.
    c. The recipient does not know or notice that the signer breached any duty as a subscriber or is not the rightful holder of the private key.

These presumptions imply that a subscriber may breach their duty by disclosing the private key to an unauthorized party, who could then misuse it to impersonate the subscriber to the recipient. The unauthorized party may unlawfully obtain or misuse the private key to sign a digital certificate, with or without the subscriber's consent. The presumptions place the burden on the signer (subscriber) to prove that the digital signature was not theirs or was improperly attached in any way, shifting the risk of forgery or false signature to the signer.

4.6.3 *Duties and Liabilities*

Subscribers: According to section 43 of the DSA, subscribers are obligated to exercise reasonable care to prevent the disclosure of their private key to unauthorized individuals.

Under section 41 of the DSA, subscribers are liable for any loss or damage resulting from false material representations or non-disclosures, provided that such representations or non-disclosures were made with deceitful intent or negligence. As the exclusive owner of a certificate, subscribers are implicitly

making the following representations:

i. The subscriber asserts sole ownership to third parties.
ii. Representations made to the Certification Authority (CA) and the information contained in the certificate are accurate.
iii. Even if not explicitly confirmed by the CA, all representations made to the CA or included in the certificate are truthful.

Trusted third parties (CA): According to section 29 of the DSA, when a request for issuance is received, the CA must confirm the following before issuing a certificate:

i. The identity of the prospective subscriber;
ii. The accuracy of the data to be included in the certificate;
iii. The prospective subscriber's rightful ownership of the private key;
iv. The capability of the private key to create a digital signature;
v. The capability of the public key listed in the certificate to verify a digital signature generated by the subscriber's private key.

Section 36 of the DSA mandates that the CA certifies to all those who reasonably rely on the certificate:

i. The accuracy of the data contained in the certificate;
ii. Inclusion of all information material to the reliability of the certificate;
iii. Acceptance of the certificate by the subscriber.

Under section 30 of the DSA, the CA is legislatively obliged to publish a signed copy of the certificate upon acceptance by the subscriber, unless otherwise specified in a contract between the CA and the subscriber. Section 35 of the DSA mandates the CA to promptly revoke a certificate when necessary and to notify the subscriber of any facts known that significantly affect the reliability or validity of the certificate.

5. CONCLUSION

The increasing adoption of e-payment systems and e-commerce presents both opportunities and challenges in ensuring compliance with Shariah principles. This study has identified key concerns, including riba (usury) in conventional payment structures, gharar (uncertainty) in online transactions, and the legal complexities surrounding the validity of digital contracts. To address these issues, this paper proposes a Shariah-compliant e-payment solutions that integrates Islamic jurisprudence with technological solutions, regulatory oversight, and legal provisions. The solution emphasizes secure

May 2025 | Vol. 30 No.2 | ISSN: 2232-1047 | eISSN: 0127-8886

payment mechanisms, the role of a dedicated Shariah advisory body, and the application of digital signatures to enhance transactional integrity. By aligning e-commerce practices with Islamic commercial law, this study provides a foundation for policymakers, financial institutions, and e-commerce stakeholders to develop more ethical and compliant digital financial ecosystems. Future research should explore the practical implementation of these solutions, particularly in integrating smart contracts and blockchain technology for enhanced Shariah governance in online transactions.

6. REFERENCES

Abozaid, A., & Khateeb, S. H. (2022). A critical shariah and maqasid appraisal of Islamic credit cards. *European Journal of Islamic Finance, 9*(3), 14-20.

Ainnur Hafizah, A.M., Mohd Zulkifli, M., Tamrin, A., & Mohd Sarwar, E.A. (2013). Bai as-salam and e-commerce: A comparative analysis from shariah perspectives. *Proceedings of The 2nd Applied International Business Conference (AIBC2013)*, Labuan, Malaysia, 522-529.

Akhlaq, M., & Asif, M. (2024). The importance of sharia compliance in Islamic finance. *Tanazur*, *5*(1), 196-212.

Alhusban, A. A. A., Massadeh, A. A. M., & Haloush, H. (2021). The Islamic credit card as an electronic payment method: The technical trick in the installment payment contract as a financial product. *International Journal of Law and Management, 63*(6), 599-628.

Aliha, P. M., Sarmidi, T., & Said, F. F. (2019). Comparing the forecasts of the demand for money in Malaysia with the inclusion of financial innovation using different estimation methods. *Regional Science Inquiry, 11*(3), 163-194.

Arif, S., & Elfadel, M. (2024). An introduction to Islamic perspective in fintech security. *International Journal on Islamic Applications in Computer Science And Technology*, *12*(3).

Azni, A. H., Ridzuan, F., Pitchay, S. A., MohdAlwi, N. H., Ishak, M., & Radzali, R. (2024, December 11-12). Certificate authority capacity and digital signature market demand in promoting interoperability in Malaysia [Conference presentation]. *1st International Conference on Advances in Machine Intelligence, and Cybersecurity Technologies (AMICT2023)*, Sabah, Malaysia.

BNM (2010). *Guideline on the governance of Shariah committee.* http://www.bnm.gov.my

Chandrashekhara, J., Anu, V. B., Prabhavathi, H., & Ramya, B. R. (2021). A comprehensive study on digital signature. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST), 9*(3), 43-47.

Comer, D. E. (2007). *The internet book: Everything you need to know about computer networking and how the internet works.* Pearson Prentice Hall.

Dadach, Z. E. (2020). Charity: The divine science of Allah (SWT). *Journal of Islam and Science, 7*(1), 39-48.

Esayas, S. Y. (2024). *Data privacy and competition law in the age of big data: Unpacking the interface through complexity science.* Oxford University Press.

Fajriyyah, L., Arif, B., Hidayah, N., Sujoko, I., & Asmawi, A. (2023). Recent practice of bay'al-salam hadiths: A study of e-commerce system. *Proceedings of the 5th International Graduate Conference in Islam and Interdisciplinary Studies (IGCIIS 2022)*, Lombok, Indonesia.

Husni, A. (2023). Sharia issues in Islamic credit card based on Indonesia practice. *JISRAH: Jurnal Integrasi Ilmu Syariah, 4*(2), 223-231.

Ibn Taymiyyah, T. D. (1317). *Nazariyyah al-'aqd*. Dar al-Ma'rifah.

Izzat, A. & Mohammad, Z. (2015) Building an Islamic financial information system based on policy managements. *Journal of King Saud University-Computer and Information Sciences, 27*, 364–375.

Marjan, M., Muhd Rosydi, M., Mohd Adam, Husnayati H, Mohamed Jalaldeen M.R., Kalthom, A. (2013) Building trust in e-commerce from an Islamic perspective: A literature review. *American Academic & Scholarly Research Journal, 5*(5), 161-168.

Md Fazlur Rahman, A. (1980). *Economic doctrines of Islam.* Islamic Publications Ltd.

MIMOS (2009). *Digicert to provide validation service soon.* https://www.mimos.my/main/digicert-to-provide-validation-service-soon-2/.

Mohd Dali, N. R. (2014). *Islamic credit card users' satisfaction: a comparative study* (Doctoral dissertation, Cardiff University).

Muhammad Kholifatul I., Ardiansyarh, Y. & Budi, H. (2016) Shari'ah-compliant e-commerce models and consumer trust. *Al-Iqtishad: Jurnal Ilmu Ekonomi Syariah (Journal of Islamic Economics), 8*(2), 243-254.

Nor Azah, J., & Al-Hasan, A. (2016) Online dropship for business transaction in Malaysia: Views from muslim scholars. *International Journal of Islamic Business, 1*(1), 13-28.

Norazlina, Z., Fauziah, O. & Siti Hartini, M. (2004). E-Commerce from an Islamic perspective. *Electronic Commerce Research and Applications, 3,* 280–293.

Pfleeger, C. & Pfleeger, S. (2015). *Security in computing.* Pearson.

Roper, J. (2023). *The rise of e-commerce: From dot to dominance.* Pen and Sword History.

Sheraz, M., Ullah, A., Ullah, S., & Irfan Khadim, M. (2021). Islamic credit card: A new version of sharia compliant credit card. *International Journal of Information, Business and Management, 13*(4), 174-181.

Siddiqi, A. H. (2000). *Shahih muslim.* Kitab Bhavan.

Stallings, W. (2003). *Cryptography and network security.* Prentice Hall.

Tamrin, A., Ainnur Hafizah, A.M., Mohd Zulkifli, M., Mohamad Fauzan, N., & Roslina, O. (2015). Development method for shariah compliant e-commerce payment processing. *International Journal of Computer Theory and Engineering, 7*(5), 408-415.

Tanenbaum, A.S. & Wetherall, D. J. (2010). *Computer networks.* Prentice Hall.

Wang, J. L. & Ren, S. Y. (2024). *Dynamical behaviors of multiweighted complex network systems.* Wiley-IEEE Press.

Zeno, J. (2022). Information in consumer contracts: Reforming consumer protection law in Malaysia. *Asian Journal of Comparative Law, 17*(2), 242-267.

Zhou, Y. (2024). The impact of payment methods on consumer behaviour in the e-commerce environment. *International Journal of Web Based Communities*, *20*(3-4), 298-310.