

IoT-Driven Payment Gateways in Fintech: Towards a *Shari'ah*-Compliant Digital Future

Abdullah Shakir

PhD Islamic Banking and Finance Scholar, School of Islamic Banking and Finance, International Institute of Islamic Economics, International Islamic University, Islamabad Sector H-10, abdullahshakir@live.com

Malik Muhammad

Associate Professor, International Institute of Islamic Economics, International Islamic University, Islamabad, Sector H-10. malikmuhammad@iiu.edu.pk

Ihsan Ullah Chishti

Lecturer, Islamic Research Institute, International Islamic University, Islamabad.
Ihsanullah.chishti@iiu.edu.pk

Abstract

The growing integration of the Internet of Things (IoT) within financial technology is giving rise to a new generation of payment gateways capable of executing autonomous transactions with unprecedented speed and accuracy. These IoT-driven systems, ranging from wearable payment devices to smart appliances, are reshaping digital finance; however, this rapid expansion raises significant concerns regarding compliance with Sharī'ah. This study investigates the design and operation of IoT-based payment gateways through the lens of Islamic jurisprudence, aiming to outline a pathway towards a Sharī'ah-compliant digital payment gateway future. It examines how these technologies can be aligned with fundamental Islamic legal requirements, including the clarity of contractual terms, the validity of consent, transparency, and the avoidance of unjust enrichment, etc. A critical theme in this evaluation is the pressing need for Islamic states to establish institutional mechanisms capable of defining contemporary Maṣlaḥah in the governance of IoT systems. Without such bodies, the application of Sharī'ah to emerging innovations remains fragmented. Drawing from classical legal theory as well as contemporary fatwā literature, the study proposes a conceptual framework that integrates Islamic moral values with technological innovation. It presents practical guidance to Fintech developers, Islamic financial institutions, Sharī'ah jurists, and regulators. By addressing both the operational functionality of IoT payment systems and their conformity with Sharī'ah principles, this research contributes to the development of an IoT-enabled financial infrastructure that is not only efficient and future-oriented but also rooted in justice, trust, and moral accountability.

Keywords: Internet of Things, Fintech, payment gateways, Real-time digital transactions, Shariah Compliance.

Introduction

The incorporation of Internet of Things (IoT) technology into the Fintech ecosystem has initiated a structural transformation of digital payment gateways. Instead of relying solely on browser-based or mobile platforms, contemporary gateways are now leveraging IoT-enabled tools, such as QR code scanning, near-field communication (NFC), and digital tokenization enhance transactional efficiency, voice-command devices and embedded automotive systems. These autonomously initiate, authenticate, and complete financial transactions. This shift has enhanced the transaction speed and user convenience as well as it has enabled real-time, sensor-based payment execution across multiple environments. These inter-connected automotive interfaces have become integral to executing personalized, immediate, and secure financial transactions (Gilchrist, 2016). They have not only strengthened the infrastructural capacity of digital finance but also enhanced capabilities in fraud prevention, behavioral analytics, and user-specific financial profiling (Udeh et al., 2024). This facilitates autonomous interactions between networked devices, has

**IoT-Driven Payment Gateways in Fintech:
Towards a *Shari'ah*-Compliant Digital Future**

enabled a continuous data exchange and real-time decision-making without the need for human oversight (Kang, 2022). These IoT-based gateways are evolving to handle automated micro-payments, deploy biometric identity verification, and trigger payments through machine-to-machine (M2M) communication, making a critical departure from conventional digital infrastructure. Stripe and PayPal, serve as digital intermediaries, managing encrypted data flows among users, merchants, and financial institutions. Their recent integration with mobile applications and IoT-enabled devices has enabled real-time transaction authorization, currency conversion, and layered encryption protocols across diverse platforms (Zou, 2025).

Despite the operational advantages of IoT-based financial technologies, challenges still exist with respect to cybersecurity vulnerabilities, data ownership, and ethically unmonitored automation particularly within Islamic financial frameworks governed by *Shari'ah* law (Khando, et al., 2023). These IoT-driven Fintech solutions increasingly bypass conventional banking structures, ensuring that these innovations operate within ethically sound and legally valid parameters remains a foundational requirement for Islamic finance. Within the Islamic finance framework, such advancements raise intricate *Shari'ah* concerns particularly around the prohibition of *Ribā* (usury), *Gharar* (excessive ambiguity), the application of *Bai Al Saraf* and engagement with non-ethical or exploitative transaction models. Evaluating the *Shari'ah* legitimacy of these gateways necessitates a critical examination of the underlying contractual structures, data integrity, and the automation of consent mechanisms inherent in IoT-based financial operations, as well as their indirect associations with interest-bearing accounts (Oseni, 2019).

In a recent development by AAOIFI, it issued the Governance Standard No. 17 (GS-17) and the draft standard on the *Shari'ah* compliance function (2024–25), which underscores the growing emphasis on institutional ethical oversight in Islamic finance. These standards, though primarily focused on *Sukūk* and centralized governance structures, provide a foundational framework that can be extended to IoT-based payment gateways. The integration of these governance principles into IoT-enabled financial ecosystems is essential to ensure transparency, accountability, and *Shari'ah* compliance particularly in automation and decentralized decision-making.

Islamic finance has traditionally approached technological innovation with measured practicality, the accelerating digitization of financial systems through IoT-driven infrastructures demands a more deliberate *Shari'ah* response e.g. an active collaboration among technologists, *Shari'ah* scholars, and financial regulators to design payment gateways that uphold Islamic legal principles without undermining functional efficiency. In light of this, there arises an urgent need to scrutinize how IoT-based payment mechanisms can be architected to meet both performance benchmarks and the jurisprudential conditions of contract clarity, risk mitigation, contractual clarity, and transactional fairness, the exclusion of exploitative elements such as *Ribā*, *Gharar*, and unjust enrichment. Unlike conventional platforms, *Shari'ah*-compliant financial services are obligated to reject speculative instruments, vague contractual terms, and automation models that bypass conscious consent. Ensuring compliance, therefore, entails more than technological integration it requires sustained moral scrutiny rooted in fiqh-based accountability. This study thus positions itself at the intersection of IoT and Fintech, offering a *Shari'ah*-informed framework aimed at cultivating a digitally secure, morally sound, and legally compliant financial ecosystem.

Literature Review

The intersection of Islamic finance and Fintech has witnessed growing scholarly and practical interest during recent years. Considerable research has explored *Shari'ah*-compliant financial technologies but the specific attention to **IoT-driven payment gateways** remained limited. This section reviews important contributions while identifying critical gaps related to the ethical, legal, and operational dimensions of IoT-based financial systems within the Islamic framework.

Oseni and Ali (2019) have investigated the implications of emerging technologies particularly smart contracts and AI in Islamic finance. In this work the authors have focused on consent, ownership, and risk. The study touches on automation, however only briefly acknowledges the role of IoT in financial transactions. The study stresses the potential erosion of *Shari'ah* safeguards in automated systems and call

for dedicated frameworks that uphold ethical and legal integrity in technology-enabled payments.

Hasan (2020) examines Fintech's promise in promoting financial inclusion among unbanked Muslim populations through mobile and blockchain applications. Nevertheless, the study does not engage with IoT-driven payment models, leaving unaddressed the *Sharī'ah* implications of device-initiated or sensor-triggered transactions. This underscores a missed opportunity to link IoT applications with Islamic legal principles.

Dawood et al. (2022) have conducted a systematic review of Islamic Fintech literature. According to them the most research centres on funding and lending mechanisms, giving less attention to IoT. Although the study emphasises the need to avoid *Ribā* and ensure compliance, it does not examine how IoT-based transactions may involve *Sharī'ah* prohibitions such as Gharar or unjust enrichment, etc.

Aysan et al. (2022) have reported a general flow in the adoption of technologies such as AI, DLT, and IoT among Islamic banks. While their analysis is less jurisprudential. It highlights the institutional inertia that has delayed serious discussion on IoT compliance mechanisms within *Sharī'ah*-based financial systems.

Kurt et al. (2022) introduce LNGate2, a protocol enabling IoT devices to perform Bitcoin micropayments with minimum memory load. The protocol is technically sophisticated, but is entirely silent on *Sharī'ah* concerns like whether automated, trust-minimized payments conforms Islamic legal standards, which reveals a lack of ethical and jurisprudential scrutiny.

Amila et al. (2022) give a comprehensive overview of blockchain-enabled micropayment solutions for IoT. The study addresses technical issues like scalability and automation, however it fails to assess key Islamic legal principles such as Gharar, *Ribā*, or transparency limiting its relevance for *Sharī'ah*-compliance.

Aysan and Al-Ansari (2022) emphasize the integration of blockchain, CBDCs, and IoT in Islamic banking, proposing BIoT (Blockchain-IoT) models in order to enhance security. Despite acknowledging IoT's potential, the authors have not evaluated the *Sharī'ah* permissibility of these solutions or analyze contractual elements—such as clarity, mutual consent, and prohibition of unjust enrichment in any such digital transactions.

Asmadi Naim et al. (2023) evaluated Malaysian e-wallets from a *Sharī'ah* perspective, proposing valid Islamic contracts such as *Wakālah* and *Wadi'ah* to govern digital funds. However, the study stops short of exploring how these contract types could be applied in IoT interfaces where human involvement is almost absent, neglecting a crucial dimension of automated payment gateways.

Aulia et al. (2024) provide a bibliometric overview of Islamic Fintech, highlighting recurring themes such as Islamic ethics and emerging technologies, including IoT. The study acknowledges IoT's potential in enabling real-time payments; however, it doesn't evaluate how specific IoT-driven payment models comply with *Sharī'ah* standards or avoid *Sharī'ah* prohibitions.

Sulartipurkar (2024) presents the use of IoT and blockchain in Takaful as tools for improving efficiency and *Sharī'ah*-compliant monitoring. However, it lacks a detailed analysis of how IoT payment triggers or automated claims would fit within Islamic contractual norms.

Amin and Hamid (2025) emphasise the ethical foundations of Islamic Fintech such as transparency, trust, and the avoidance of *Ribā* and Gharar. Nevertheless, their analysis is largely theoretical and does not interrogate the specific features of IoT such as automated triggers, sensor data reliability, etc.

The reviewed literature discusses the emerging technologies in Islamic finance, including smart contracts, artificial intelligence, blockchain, and the Internet of Things (IoT), with varying degrees of depth. These studies explore foundational *Sharī'ah* concerns such as consent, ownership, and risk in the context of automated systems and evaluate Fintech models. Despite technical innovations such as blockchain-based micropayment protocols and mobile financial tools aimed at promoting inclusion, the adoption of such advancements within Islamic Financial areas is still limited. *Sharī'ah*-compliant contracts in digital wallets and broader ethical themes such as transparency, trust, the avoidance of *Ribā*, and the elimination of Gharar, yet to be discussed in more depth. While blockchain applications and digital finance tools are often analysed, juristic scrutiny of IoT-enabled transactions is usually absent. Some essential legal concerns,

**IoT-Driven Payment Gateways in Fintech:
Towards a *Shari'ah*-Compliant Digital Future**

such as informed consent, the prohibition of *Ribā*, and the presence of *Gharar*—are rarely evaluated in the context of device-triggered or sensor-based payments. They have also neglected the *Shari'ah* assessment of IoT micropayments while addressing the nuances of autonomous financial activity. The minimal use of IoT in Islamic financial institutions further reflects the lack of institutional readiness of these technologies to manage *Shari'ah* compliance in this emerging domain.

Shari'ah Compliance in IoT Payment Gateways

In *Shari'ah*, prohibitions are not monolithic; some are rooted in manifest injustice, such as *Ribā* and *Dharar*, while others are prohibited not due to inherent harm, but because of their potential to lead to future injustice (*Jahalah*) or uncertainty (*Gharar*). A third category exists wherein the rationale for prohibition remains unknown or controversial, falling under divine wisdom beyond human grasp, e.g. the conditions Shariah imposed in exchange of certain goods and currencies. In such cases, Islamic legal scholars often assess permissibility through the lens of *Maqāṣid al-Shari'ah*, the higher objectives of Islamic law and the collective welfare (*maṣlaḥah*) of the Ummah. Within Islamic finance, consideration of these distinctions is significant when evaluating novel technologies. The emergence of the Internet of Things (IoT) in payment systems introduces autonomous, device-led financial interactions that challenge conventional fiqh categories of agency, consent, and contractual validity. As such, determining *Shari'ah* compliance in IoT-based payment gateways requires a layered approach balancing clear prohibitions, inferred legal wisdom, and public interest. It is not sufficient to apply static legal rulings; rather, it demands a dynamic jurisprudential inquiry that aligns with both the ethical spirit and structural foundations of Islamic finance.

Islamic jurisprudence rests on the foundational values of justice, fairness, transparency, and accountability. These principles shape financial ethics in Islam, where the prohibition of *Ribā* (interest), *Gharar* (excessive uncertainty), and *Maysir* (gambling) ensures that economic dealings are equitable and free from exploitation (Hassan, M.K, 2021). Mutual consent, protection of public welfare, and contractual clarity are essential pillars in Islamic financial transactions (Al-Amine, 2023). In the evolving domain of IoT, preserving *Shari'ah* principles has become both more difficult and more urgent.

IoT transactions often operate through pre-programmed logic and automated triggers. In any IoT-based payment systems, where transactions are initiated without the user's direct involvement, raises *Shari'ah* concerns around informed consent and contract validity. To assure *Shari'ah* compliance, such systems must be built on pre-agreed digital contracts, with mechanisms that verify mutual agreement and ensure transparency at every stage (Dusuki et al., 2021). *Ribā* also poses a real threat in IoT, not just in conventional interest-bearing models but through hidden fees, delayed settlements, and conditional pricing structures embedded in digital platforms (ISRA, 2022). The use of platforms such as Apple Pay, Google Pay, or Stripe must be carefully evaluated as they are backed by processes involve interest-based gateways or service providers (Pereira et al., 2019; Hahn, 2020). Similarly, systems like Easypaisa, despite playing a role in financial inclusion in Pakistan, face criticism for links to services that charge or accumulate interest (Rehman & Shahid, 2020). In the IoT, these risks multiply as users are mostly not fully aware of the financial implications triggered by their connected devices.

Another critical concern is the issue of *milkīyyah* (ownership). As alluded to before, for a transaction to be valid in Islamic law, the transfer of ownership must be clear, immediate, and unconditional. In automated payments, such as a smart fridge reordering groceries or a vehicle paying toll fees, ownership transfer happens without direct user confirmation. This necessitates rigorous system design to ensure that ownership rights are honored and that users are not unknowingly parting with property or funds (AAOIFI, 2022). It is also arguable that automation can erode human dignity (*ḥifẓ al-karāmah*). Transactions that occur without user awareness or consent can compromise *Shari'ah* values of accountability and free will. To preserve dignity, developers must design IoT systems that protect user agency, embed *Shari'ah* safeguards, and offer clear, accessible terms. *Shari'ah* compliance in Fintech must go beyond technical checklists to embrace a value-driven approach rooted in justice and public benefit

(Abdullah & Oseni, 2021). Beyond rule-based analysis, *Maqāṣid al-Sharī'ah* gives a broader lens for assessing the *Sharī'ah* dimensions of IoT in finance. The protection of wealth (*ḥifẓ al-māl*), one of the five key objectives, requires a mechanisms that guard users against loss, fraud, or unauthorized deductions (Dusuki, 2023).

***Maqāṣid al-Sharī'ah*, State Authority, and the Ethical Boundaries of IoT-Driven Payment Gateways**

The evaluation of financial transactions within the Islamic Financial framework is not limited to a checklist of prohibitions such as *Ribā*, *Gharar*, and *Maysir* rather it is deeply rooted in the higher objectives of *Sharī'ah* (*Maqāṣid al-Sharī'ah*). Mere absence of apparent violations does not suffice to declare a financial system *Sharī'ah*-compliant. Islamic jurisprudence demands a deeper inquiry: Does the system serve the public good (*maṣlaḥah 'āmmah*)? And crucially, **who determines this *maṣlaḥah*?** In classical Islamic governance, the role of determining *maṣlaḥah* in complex or novel situations was not delegated to individual entities. Instead, it is the prerogative of the Islamic state, acting through qualified institutions, to issue decisions based on the prevailing needs of the *Ummah*. This principle is especially relevant in the era of Fintech and IoT-based payment systems, where technologies often originate outside Islamic legal traditions and evolve faster than juristic consensus can form or even faster than it becomes clear to many jurists. If a payment gateway appears formally sound, containing no interest, no uncertainty, and no gambling but its underlying logic, infrastructure, or socio-economic consequences disrupt communal justice or increase dependency on unethical systems, then it cannot be treated as ***Sharī'ah* compliant**. Hence, **the determination of compliance cannot rest solely with individual scholars or consumers; it must be institutionalized under the legitimate authority of the Islamic state**, which bears responsibility for preserving the collective welfare over fragmented interests of individuals as well as overall *Maslahah* of *Ummah*. Besides, ***Sharī'ah* occasionally obligates individuals to bear limited burdens in order to secure broader societal benefits**. This principle has a precedent in classical Islamic law *tahammul al-maqāṣid li-sabīl al-maṣāliḥ*, where temporary individual hardship is allowed for the sake of overarching justice, equity, and social protection. In economic terms, this could translate into compliance with certain regulatory controls, data-sharing mandates, or restrictions on high-risk financial tools when such measures are instituted to prevent systemic exploitation or economic colonization. In IoT-driven payment gateways, this insight underscores a critical issue: **technological systems that prioritize individual convenience or corporate efficiency at the expense of the *Ummah*'s moral or economic autonomy cannot be considered *Sharī'ah*-compliant**, even if they meet formalistic criteria. For instance, an IoT platform that automates payments through algorithms hosted on interest-based financial rails, or one that transmits sensitive consumer data to non-Muslim jurisdictions, may undermine the true spirit of the concept of *Maslahah*. . Thus, **the architecture of payment systems must align not only with personal piety but with the state-declared priorities for the collective *Ummah***, especially where sovereignty, social equity, and economic justice are at stake.

In conclusion, the *Sharī'ah* compliance of IoT-based financial technologies must be assessed through a substantive *Sharī'ah* and legal evaluation grounded in *Maqāṣid*, and a state-regulated framework that defines *maṣlaḥah* in response to contemporary socio-economic realities. Only by merging juristic ethics with legitimate authority can we develop payment systems that truly uphold the spirit of Islamic finance in the digital age.

Regulatory and Legal Framework

As Fintech rapidly transforms global finance, regulators all over the world have also started responding with frameworks designed to uphold innovation, consumer protection, state interests and systemic stability. International bodies such as the Financial Stability Board (FSB) and IOSCO introduce principles that address cybersecurity, data privacy, and anti-money laundering in digital finance, through regulatory sandboxes that often permit limited, supervised experimentation by Fintech firms (Dirk & Janos, 2017). Global legal frameworks such as the EU's GDPR and the U.S. IoT Cybersecurity Improvement Act (2020) are aimed at upholding user consent, data minimization, and device-level security (GDPR, 2018).

In term of Islamic Fintech, Global standard-setters such as AAOIFI and FSB have issued

**IoT-Driven Payment Gateways in Fintech:
Towards a *Shari'ah*-Compliant Digital Future**

comprehensive guidelines for ensuring *Shari'ah* compliance across financial instruments, including sukuk, takāful, and Islamic Fintech (AAOIFI, 2021). At the institutional level, *Shari'ah* Governance Frameworks (SGFs) assure religious supervision through mechanisms like *Shari'ah* Supervisory Boards (SSBs), compliance units, and audits. It has become very crucial for Islamic financial regulators to integrate digital ethics and the objectives of *Shari'ah* (*Maqāṣid al-Shari'ah*) into these emerging domains (Abdul Haseeb & Umar, 2019). Without this evolution, there is a risk that Islamic finance may either stagnate or dilute its integrity. Therefore, forward-looking *Shari'ah* governance is essential to ensure that technological innovation remains aligned with Islamic moral and legal norms.

In Pakistan, while comprehensive IoT-specific legislation remained unlegislated, laws like PECA 2016 and the draft Personal Data Protection Bill (PDPB) provide partial legal *grounding* (PECA, 2016). The State Bank of Pakistan's *Shari'ah* Governance Framework (2018) mandates such oversight for Islamic banks and Fintech platforms, especially about automated systems like IoT-driven payments (SBP, 2018). The State Bank of Pakistan has also issued key directives, including the EMI Regulations (2019) and the Digital Bank Framework (2022), which reflect an emerging legal architecture for digital banking and IoT-integrated payments (SBP, 2022).

However, these regulations lack precise guidelines for IoT applications in Fintech, such as wearable payments or smart billing. From an Islamic legal perspective, data security is deeply intertwined with the *Maqāṣid al-Shari'ah*, specifically the protection of privacy (*Hifẓ al-'Ird*) and wealth (*Hifẓ al-Māl*). Any breach that causes injustice or uncertainty (*Gharar*) contradicts Islamic principles. Ensuring *Shari'ah*-compliant Fintech demands not just legal compliance but ethical and *Shari'ah* assurance in the protection of users' rights, consent, and financial sanctity (Abdul Haseeb & Umar, 2019). No regulation in this context can be effective if it doesn't integrate conventional oversight with Islamic legal imperatives. (AAOIFI, 2021).

Challenges in Harmonizing Technology and *Shari'ah* Law

The rapid evolution in IoT-integrated payment gateways offers unprecedented efficiency on one hand but presents unique challenges for *Shari'ah*-compliant financial systems on the other. A core difficulty can be attributed to the asynchronous pace of technological development and Islamic jurisprudence. Innovations such as automated micro-transactions and biometric-based payments are swiftly adopted, while the *Shari'ah* process of legal reasoning, *fatwā* issuance, etc., follow a more deliberate and cautious trajectory (Najeeb, S. F., et al, 2024). This temporal dawdle often results in technologies being deployed before their compliance with Islamic principles is properly assessed. Certain classical *Shari'ah* principles—such as *Ījāb wa Qabūl* (offer and acceptance), *Milkiyyah* (ownership transfer), and risk distribution—to machine-initiated transactions further rarify the matter. In IoT-based payments, where financial decisions are autonomously executed by devices, ensuring valid consent, clear contractual terms, and fair risk allocation becomes more difficult (Nurul Huda & Oseni, 2019). The manifestations of impermissible elements like *Ribā*, *Gharar*, or *Maysir* may arise through algorithmic pricing, ambiguous fee structures, or default automation settings. In such cases, *Shari'ah* compliance must go beyond procedural legality to encompass the moral and ethical objectives of Islamic law (AAOIFI, 2023).

Compounding these challenges is the broader institutional vacuum within Muslim-majority countries, unfortunately at present, there is no recognized body in any Islamic state consistently tasked with defining and articulating the evolving *maṣlaḥah* of the Ummah in the light of contemporary economic realities. As a result, financial innovation proceeds without a clearly established ethical compass grounded in state-sanctioned *Shari'ah* objectives. The determination of what serves the public good a function historically reserved for the head of Islamic State or *Shari'ah* governance bodies has been left vague or fragmented, undermining the possibility of coherent policy or legal application in IoT-based payments in Fintech.

In parallel, another critical gap is the absence of institutional mechanisms to translate modern financial and technological innovations into a form that *Shari'ah* scholars can effectively evaluate. Most jurists are not trained in data systems, payment protocols, or algorithmic logic, while many Fintech developers lack the jurisprudential vision necessary to foresee *Shari'ah* implications. This mutual

disconnect prevents meaningful engagement and slows down ethical assessment. Without formal structures dedicated to bridging this divide—through translational bodies, research councils, or interdisciplinary sittings, technological advancements risk outpacing juristic oversight.

Proposed Framework for *Sharī'ah*-Compliant IoT Payment Gateways

The integration of Internet of Things (IoT) technologies into Fintech ecosystems has offered a remarkable opportunity for automating transactions, enhancing efficiency, and delivering financial services cosmically. However, for Islamic financial systems, such innovation must be grounded in a comprehensive *Sharī'ah* compliance architecture adheres to canonical Islamic legal principles and aligns with the broader *Maqāṣid al-Sharī'ah*. To fill this gap, this study proposes a novel ***Sharī'ah*-Integrated IoT Compliance Architecture (SIIoTCA)**, a three-tiered model designed to ensure contractual, ethical, and legal integrity across all levels of IoT-enabled payments.

Despite existing standards introduced by **Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI)** or the **Islamic Financial Services Board (IFSB)**, current frameworks do not adequately address the complexities caused by IoT environments particularly with respect to automated contracts, machine-triggered transactions, biometric consent, and decentralized data flow. These technological advancements challenge traditional *Sharī'ah* notions of offer and acceptance (*ījāb wa qabūl*), transparency (*bayān*), and mutual consent (*tarāḍī*). Without real-time validation and active governance, these systems can cause the incorporation of elements declared as impermissible by *Sharī'ah* (ISRA, 2024; Dusuki, 2023).

This research thus contributes a **multidimensional framework** to operationalize Islamic legal and *Sharī'ah* values in digital transactions, offering a systematic blueprint for compliance within the IoT-driven Fintech space.

The SIIoTCA Model: Three-Tier Framework

(a) IoT Interaction Layer (Device-Level Contractual Integrity)

This foundational layer consists of IoT-enabled devices—wearables, sensors, and POS terminals—that initiate financial transactions. To meet *Sharī'ah* conditions, all devices must record and verify **Lawful subject matter (*mabī'*)**, **clear offer and acceptance (*ījāb wa qabūl*)**, **transparent consideration (*thaman*)** and **User consent (*tarāḍī*)** via biometric or multi-factor authentication. To prevent *Sharī'ah* violations, interfaces must prohibit **automated consent** without explicit user action, **Bundled or hidden fees or any Pre-programmed interest clauses**. Such layer will ensure that each transaction mimics the contractual validity standards found in classical Islamic jurisprudence.

(b) Middleware Compliance Engine (Smart Contract Validator)

At the heart of SIIoTCA is the middleware engine, a smart compliance validator that executes Islamic contracts (e.g., bay', ijārah, wakālah) using blockchain or distributed ledger technology (DLT), conducts real-time compliance screening through **AI-powered *Sharī'ah* filters and logs** transactions immutably to support auditability and legal traceability. Tokenisation and digital asset models are employed to eliminate *Ribā* exposure, and smart contract structures are restricted to *Sharī'ah*-permissible models (Ali & Khairi, 2021).

(c) *Sharī'ah* Governance Interface (Supervisory Oversight Layer)

The top layer integrates human oversight with machine compliance which includes ***Sharī'ah* Supervisory Boards (SSBs)** with real-time access to transaction data, **certification mechanisms** to pre-approve smart contracts and **automated alerts** for non-compliance triggered by embedded *Sharī'ah* algorithms. This ensures accountability and maintaining the flexibility to adapt *ijtihād* to evolving technologies (Abdullah & Oseni, 2021).

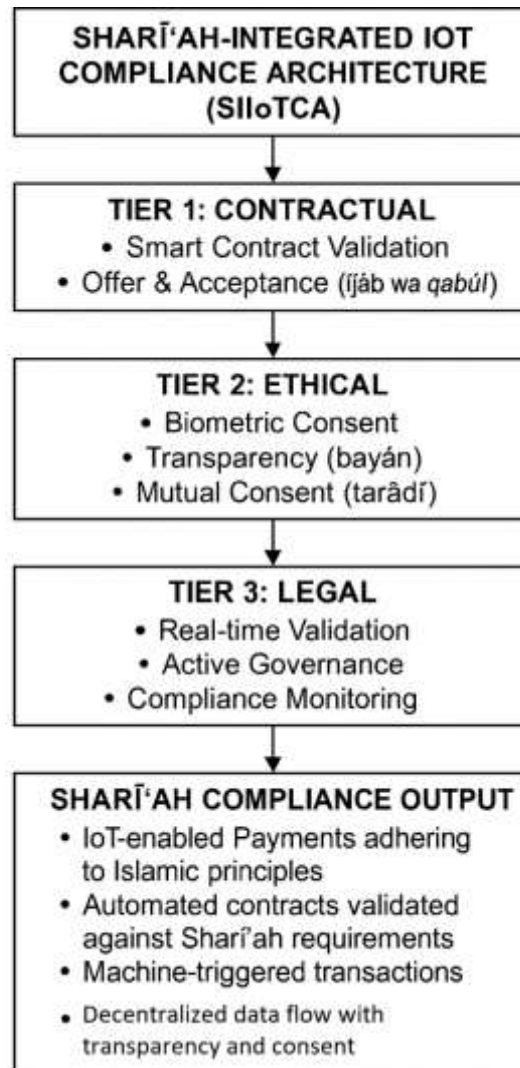
For all Islamic states, it has become imperative to establish sovereign regulatory oversight over all IoT-enabled payment transactions to ensure full alignment with *Sharī'ah* economic objectives and the welfare of the Muslim *Ummah*. In contrast to conventional Fintech models that emphasize decentralization

**IoT-Driven Payment Gateways in Fintech:
Towards a *Shari'ah*-Compliant Digital Future**

and algorithmic freedom, an Islamic model should prioritize moral control, economic sovereignty, and collective accountability (Oseni & Ali, 2019).

Modern IoT systems often bypass state scrutiny, enabling transactions that may indirectly support *Ribā*-based institutions, or data colonialism etc. The legitimacy of financial activity in Islam is not merely legalistic but rooted in its contribution to *maṣlaḥah* ‘Ummah and its compliance with state-declared *Maqāṣid*. Embedding *Sharī’ah* supervision at the infrastructural level transforms passive automation into an active tool of moral governance, ensuring justice, equity, and moral economy in all digital interactions. Consider a smart vending machine implanted with a *Sharī’ah*-compliant POS module. A user taps the wearable device, to initiate a transaction. The system displays contract terms (item, price, terms of sale, etc.), records biometric consent, and executes a bay’ contract through a certified smart contract module. The middleware validates the transaction in real-time, while the governance layer logs it for audit by the SSB. This workflow exemplifies how SIIoTCA operationalises *Sharī’ah* standards in IoT contexts. Regulatory sandboxes must include *Sharī’ah* scholars and technologists to co-develop systems that align innovation with religious values. Policies should also mandate digital literacy programs, data opt-in mechanisms, and disclosure of fee structures to ensure *Sharī’ah* transparency.

The following diagram explains the *Sharī’ah*-Integrated IoT Compliance Architecture (SIIoTCA).



The SIIoTCA framework can serve as a policy guide for central banks and regulators in Muslim-majority countries. National *Sharī’ah* boards, such as those under SBP, SAMA, or BNM, to enforce IoT-specific *Sharī’ah* regulations, requiring *Sharī’ah* certification of smart contracts and device interfaces and mandate appointment of tech-savvy *Sharī’ah* officers in Islamic financial institutions. The proposed SIIoTCA framework is not merely a compliance checklist but a transformative model for embedding

Shariah principles into the future of Fintech. By integrating traditional jurisprudence with cutting-edge technologies such as AI, DLT, and biometric interfaces, it offers a way forward where technology becomes a means to serve the *Sharī'ah*, not bypass it. This model upholds the *Maqāṣid al-Sharī'ah* and offers a viable roadmap for a morally grounded, sovereign Islamic digital economy.

Conclusion

This study explored the intersection between Internet of Things (IoT) technologies and the ethical-contractual imperatives of Islamic finance. The study aimed to construct a viable framework for *Sharī'ah*-compliant IoT-enabled payment gateways. The study revealed that IoT offers immense potential for financial inclusion, efficiency, and automation; it simultaneously raises critical *Sharī'ah* concerns, particularly with regard to the validity of contracts (*'aqd*), real-time mutual consent (*tarāḍī*), transparency (*bayān*), and lawful ownership transfer within autonomous transactions. Most existing IoT-based payment platforms fail to incorporate explicit mechanisms for verifying *ijāb wa qabūl*, regulating *gharar*, or blocking interest-bearing clauses, within pre-authorized or smart contract environments. Additionally, regulatory structures in Muslim-majority jurisdictions such as Pakistan remain technologically underdeveloped, with limited guidance on integrating Internet of Things (IoT) technologies into a *Sharī'ah* governance framework.

In response to these gaps, this research has proposed an original three-tier *Sharī'ah*-Integrated IoT Compliance Architecture (SIIoTCA). The framework included Islamic legal principles into the foundational layers of IoT payment ecosystems. It ensures that device-level contractual validation is achieved through different means such as biometric consent and transparent user interfaces, middleware systems, and AI-powered *Sharī'ah* screening of smart contracts; and a *Sharī'ah* governance interface enabling Supervisory Board oversight, auto-audit alerts, and certification protocols aligned with AAOIFI and IFSB standards.

Moreover, this study introduced the concept of state-level regulatory sovereignty in IoT-based payment platforms. It emphasised that, within an Islamic state, IoT-enabled financial systems must operate under institutional oversight that prioritises collective welfare, prevents digital exploitation, and aligns financial flows with the objectives of *Maqāṣid*.

The convergence of IoT and Islamic finance can open transformative opportunities ranging from automated *zakāh* distribution, waqf-linked donations, and usage-based microfinance, to interest-free financing models using Qard Ḥasan and Mushārah through smart meters and biometric contracts. Voice-activated payment interfaces, real-time consent verification, and AI-based *Sharī'ah* filters stand at the frontier of a new generation of *Halāl* Fintech innovations.

However, these advancements require responsible scaffolding through legally robust and technically resilient infrastructures. This includes the development of *Sharī'ah*-regulated sandboxes co-designed by technologists and jurists as well as the deployment of AI-governed auditing engines capable of detecting *Sharī'ah* violations, and the enforcement of cybersecurity protocols grounded in Islamic ethical values such as *'adālah* (fairness), *amānah* (trust), and *ḥifẓ al-māl*. It affirms that the future of Islamic finance lies not in passively adapting to digital change, but in proactively shaping ethical, sovereign, and spiritually coherent financial technologies.

1.1 Policy Recommendations

1. Islamic states must establish independent Public Interest Councils composed of qualified jurists, economists, and technology experts tasked to identify, interpret, and safeguard the evolving *maṣāliḥ* (interests) of the *Ummah* in the digital economy. These councils should operate under state mandate to determine context-specific interpretations of *maṣlaḥah* in emerging technologies, advise regulators and legislators on whether certain IoT-enabled financial innovations contribute to or undermine the *Maqāṣid al-Sharī'ah*, develop methodologies to assess *maṣlaḥah al-māl* and to propose moratoriums on digital financial tools if they contradict *maṣlaḥah* or promote structural injustice.

**IoT-Driven Payment Gateways in Fintech:
Towards a *Shari'ah*-Compliant Digital Future**

2. A *Sharī'ah*-Centric Legal Infrastructure should be established wherein regulatory authorities in Islamic jurisdictions should mandate that all IoT-based payment systems utilise pre-programmed smart contracts grounded in valid Islamic contract structures and prohibit the integration of interest-bearing mechanisms, ambiguous fee structures, or pre-authorized deductions unless explicitly disclosed and evaluated by *Sharī'ah* supervisory authorities for their consistency with the overarching Maslahah introduced by the mentioned council.
3. A national *Sharī'ah*-compliant regulatory sandbox should be institutionalised, bringing together qualified *Sharī'ah* scholars, Fintech engineers, compliance experts, and policy analysts to allow pre-market testing of IoT-integrated payment solutions under controlled conditions.
4. All IoT-triggered financial transactions should be recorded via permissioned blockchain or distributed ledger systems (DLT) to ensure immutability, transparency, and tamper-proof audit trails. These systems must be equipped with real-time *Sharī'ah* compliance filters powered by artificial intelligence to detect prohibited elements and to ensure Islamic data protection norms, safeguarding of biometric and behavioural data.
5. To satisfy the *Sharī'ah* requirement, regulators must require that all IoT payment interfaces—including wearables, home assistants, or vehicle-based systems—incorporate explicit, user-initiated consent mechanisms. Transactions must only be triggered upon biometric confirmation, password input, or authenticated voice commands terms of sale, service charges, and payment conditions must be clearly displayed.



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

(References)

- Abdul Haseeb, A., & Umar, O. (2019). Integrating Maqāṣid al-Sharī'ah into Shariah governance frameworks for digital ethics in Islamic finance. *ISRA International Journal of Islamic Finance*, 11(2), 215–232. <https://doi.org/10.1109/ISRA.2019.1122334>
- Abdullah, A. H., & Oseni, U. A. (2021). Sharī'ah governance for ethical Fintech: A case for data privacy and cybersecurity. In U. A. Oseni & S. S. Ali (Eds.), *Fintech in Islamic finance: Theory and practice* (pp. 88–103). IRTI.
- Abdullah, M., & Oseni, U. (2021). Sharī'ah governance and Fintech: Ethical frameworks in the digital age. *Journal of Islamic Monetary Economics and Finance*, 7(2), 121–139.
- Abdullah, R., & Oseni, O. (2021). Sharī'ah compliance in financial technology: A review of Islamic finance in the digital age. *Islamic Finance Journal*, 14(3), 256–270.
- Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI). (2024). Governance standard no. 17: Sharī'ah compliance and fiduciary ratings of Sukuk and other Islamic finance instruments. Manama, Bahrain: AAOIFI.
- Accounting and Auditing Organization for Islamic Financial Institutions. (2021). Shari'ah standard on fintech-based financial services (Clauses 3/1, 4/2). <https://www.aaofi.com>
- Accounting and Auditing Organization for Islamic Financial Institutions. (2023). Shari'ah standard for fintech-based financial services (Clauses 5/2, 6/4, 8/1). <https://www.aaofi.com>
- Al-Amine, M. A. (2023). Revisiting the objectives of Islamic contracts in the fintech era: Maqāṣid al-Sharī'ah and digital financial inclusion. *Journal of Islamic Accounting and Business Research*, 14(2), 322–340. <https://doi.org/10.1108/JIABR-01-2022-0022>
- Al-Ansari, K. A., & Aysan, A. F. (2022). Central bank digital currencies, Internet of Things, and Islamic finance: Blockchain prospects and challenges. MPRA Paper, 113287. <https://mpra.ub.uni-muenchen.de/113287/>
- Ali, A. M., Ali, A. N. M., & Khairi, K. F. (2021). Smart contracts and Shari'ah compliance in Islamic finance: A blockchain-based model. *International Journal of Islamic and Middle Eastern Finance and Management*, 14(2), 350–365.
- Amila, I., Perera, S., Khan, M. A., & Hassan, T. (2022). Blockchain-enabled micropayment solutions for IoT: Scalability, automation, and technical challenges. *IEEE Internet of Things Journal*, 9(18), 17520–17535. <https://doi.org/10.1109/JIOT.2022.3185432>
- Amin, M. R., & Hamid, A. B. (2025). Ethical foundations of Islamic fintech: Transparency, trust, and prohibitions of Ribā and Gharar. *Journal of Islamic Economics*, 24(1), 112–128. <https://doi.org/10.1109/JIE.2025.1567890>
- Asmadi, N., Naim, A., Hassan, S., & Rahman, M. (2023). Sharī'ah compliance of Malaysian e-wallets: Evaluating Wakālah and Wadi'ah frameworks for digital funds. *ISRA International Journal of Islamic Finance*, 15(2), 120–135.
- Aulia, R., Hassan, M. A., Ibrahim, A., & Aziz, S. (2024). Bibliometric analysis of Islamic fintech research: Ethics, emerging technologies, and IoT integration. *Journal of Islamic Finance*,

**IoT-Driven Payment Gateways in Fintech:
Towards a *Shari'ah*-Compliant Digital Future**

13(1), 45–62. <https://doi.org/10.1109/JIF.2024.1345678>

- Aysan, A. F., Belatik, A., Unal, I. M., & Ettaai, R. (2022). Fintech strategies of Islamic banks: A global empirical analysis. *FinTech*, 1(2), 206–215. <https://doi.org/10.3390/fintech1020016>
- Dawood, H., Al Zadjali, D. F., Al Rawahi, M., & Al Abri, S. (2022). Business trends & challenges in Islamic FinTech: A systematic literature review [version 1; peer review: 2 approved]. *F1000Research*, 11, 329. <https://doi.org/10.12688/f1000research.109400.1>
- Dirk, A., & Janos, W. (2017). Regulatory sandboxes in digital finance: Cybersecurity, data privacy, and anti-money laundering principles for fintech experimentation. *Journal of Financial Regulation*, 3(2), 145–162. <https://doi.org/10.1109/JFR.2017.1234567>
- Dusuki, A. W. (2023). "IoT Finance and the Maqāṣid of Wealth Protection: A Risk-Based Framework." *Journal of Islamic Economics*, 36(2), 112–135.
- Dusuki, A. W., & Abozaid, A. (2021). "Fintech, Shariah Governance and the Maqasid al-Shariah: A Critical Review." *Journal of Islamic Accounting and Business Research*, 12(5), 798-818.
- European Union. (2018). General Data Protection Regulation (GDPR); U.S. Congress. (2020). IoT Cybersecurity Improvement Act; California. (2018). California Consumer Privacy Act (CCPA).
- Gilchrist, A. (2016). *Industry 4.0: The industrial Internet of Things*. Apress.
- Government of Pakistan. (2016). Prevention of Electronic Crimes Act (PECA); Ministry of IT & Telecom. (2021). Personal Data Protection Bill (Draft).
- Hahn, T. (2020). Stripe's global payment infrastructure: A review of compliance in Islamic financial environments. *Journal of Islamic Economics*, 23(5), 87–100.
- Hasan, R. (2020). Islamic Fintech: Sharī'ah-compliant Fintech solutions for Islamic finance industry. *Journal of Islamic Accounting and Business Research*, 11(9), 1863–1877. <https://doi.org/10.1108/JIABR-12-2019-0210>
- Hassan, M. K. (2021). Ethical foundations of Islamic finance: A revisit of Maqāṣid al-Sharī'ah in modern economic contexts. *Journal of Islamic Accounting and Business Research*, 12(3), 412–429. <https://doi.org/10.1108/JIABR-02-2020-0051>
- International Shariah Research Academy. (2024). Decentralized IoT ecosystems and Shariah contractual frameworks: Beyond AAOIFI/IFSB standards [Working Paper No. 162]. <https://www.isra.my/en/research/working-papers>
- ISRA (International Shariah Research Academy). (2022). Blockchain, IoT, and Ribā: Settlement Risks in Automated Ecosystems. Research Paper No. 128.
- Kang, K.-D. (2022). A review of efficient real-time decision making in the Internet of Things. *Technologies*, 10(1), 12. <https://doi.org/10.3390/technologies10010012>
- Khando, K., Islam, M. S., & Gao, S. (2023). The emerging technologies of digital payments and associated challenges: A systematic literature review. *Future Internet*, 15(1), Article 21.

<https://doi.org/10.3390/fi15010021>

- Kurt, G., Smith, J., Lee, H., & Brown, A. (2022). LNGate2: A lightweight payment gateway for Bitcoin micropayments in IoT devices with minimal memory load. *IEEE Internet of Things Journal*, 9(15), 13245–13258. <https://doi.org/10.1109/JIOT.2022.3167890>
- Najeeb, S. F., Hasan, A., Bacha, O. I., & Mohd, S. (2024). Agile Sharī'ah governance: A framework for IoT finance. *ISRA International Journal of Islamic Finance*, 16(1), 78–95.
- Nurul Huda, M., & Oseni, U. A. (2019). Classical Sharī'ah principles in machine-initiated transactions: Consent, ownership, and risk allocation in IoT-based payments. *ISRA International Journal of Islamic Finance*, 11(1), 98–115. <https://doi.org/10.1109/ISRA.2019.9876543>
- Oseni, U. A., & Abdullah, N. H. (2019). Sharī'ah compliance in FinTech: Issues and framework. *ISRA International Journal of Islamic Finance*, 11(2), 240–254.
- Oseni, U. A., & Ali, S. S. (Eds.). (2019). *Fintech in Islamic finance: Theory and practice*. Islamic Research and Training Institute.
- Oseni, U. A., & Zubaidah, S. (2019). Fintech and the future of Islamic finance: Ethics, regulation and Sharī'ah compliance. *Islamic Finance Review*, 4(1), 18–28.
- Pereira, M., Tavassoli, M., & Ferreira, J. (2019). The impact of biometric authentication and tokenization in modern payment systems. *Journal of Financial Technology*, 12(4), 90–104.
- Rehman, S., & Shahid, A. (2020). Easypaisa and the challenges of Sharī'ah compliance in Pakistan's Fintech sector. *Asian Economic Review*, 8(1), 58–75.
- State Bank of Pakistan. (2018). Shariah governance framework for Islamic banking institutions [Framework]. <https://www.sbp.org.pk/publications/FrameWork/Shariah-Governance-Framework-2018.pdf>
- State Bank of Pakistan. (2019). Regulations for electronic money institutions; (2022). Digital bank regulatory framework.
- State Bank of Pakistan. (2022). Digital bank framework [Framework]. <https://www.sbp.org.pk/publications/FrameWork/Digital-Bank-Framework-2022.pdf>
- State Institute for Islamic Studies (IAIN) Metro. (2025). Rumah Jurnal IAIN Metro. <https://e-journal.metrouniv.ac.id/>
- State Islamic University (UIN) Syarif Hidayatullah Jakarta. (2025). E-Journal Portal. <https://journal.uinjkt.ac.id/>
- Sulartipurkar, A. R. (2024). IoT and blockchain integration in Takaful: Enhancing efficiency and Shariah-compliant monitoring. *Journal of Islamic Insurance and Takaful*, 8(1), 78–93. <https://doi.org/10.1109/JIIT.2024.1456789>
- Udeh, I., Okonkwo, G., & Alalibo, I. (2024). The role of big data in detecting and preventing financial fraud in digital transactions. *Journal of Financial Crime Analytics*, 31(2), 157–172. <https://doi.org/10.1016/j.jfca.2024.100357>

IoT-Driven Payment Gateways in Fintech:

Towards a *Shari'ah*-Compliant Digital Future

Zou, L. (2025). The integration of IoT into fintech: Enhancing payment systems and security – A case of PayPal. *Advances in Economics, Management and Political Sciences*, 171, 79–89.
<https://doi.org/10.54254/2754-1169/2025.21861>