HHH Research Blog
Research for Impact
https://doi.org/10.66246/hq1x6r23
Vol 1, Issue 2

Date Submitted: 11/07/2026
Date Accepted: 26/07/2026
Date Published: 07/08/2026

Securing the Digital Future of Islamic Banking: Fintech, Cybersecurity, and Shariah Governance

Hissan Khandakar[a], Md. Abu Hasnat[b], Khandakar Kamrul Hasan[c]
[a] Technical Partner, HHH Research Consultancy & Development, Dhaka, Bangladesh
[b] Managing Partner, HHH Research Consultancy & Development, Dhaka, Bangladesh
[b] Chairman, HHH Research Consultancy & Development, Dhaka, Bangladesh

Abstract

Fintech is reshaping Islamic banking through mobile services, artificial intelligence, digital payments, blockchain, and automated financial processes. These developments can improve access and efficiency, but they also create cybersecurity, privacy, governance, and Shariah compliance concerns. This research blog examines fintech and cybersecurity as interconnected dimensions of digital Islamic banking. It argues that technological innovation must develop alongside cyber resilience, ethical leadership, customer knowledge, digital financial literacy, and Shariah governance. Existing research often examines these areas separately. A more integrated approach can help Islamic banks protect customer assets and data while maintaining trust, regulatory resilience, and Shariah principles within an increasingly complex digital financial environment.

Keywords: *Fintech; cybersecurity; Islamic banking; Shariah governance; digital trust*

To cite this article:
Khandakar, H., Hasnat, M. A. & Hasan K. K. (2026). Securing the Digital Future of Islamic Banking: Fintech, Cybersecurity, and Shariah Governance. HHH Research Blog, 1(*2*). https://doi.org/10.66246/hq1x6r23

HHH Research Blog
Research for Impact
https://doi.org/10.66246/hq1x6r23
Vol 1, Issue 2

Rationale

What makes an Islamic bank ready for a digital financial future? A mobile application may make banking faster. Artificial intelligence can support customer service and financial decision-making. Blockchain may improve transparency. Digital platforms can also expand access beyond physical branches. Yet technological advancement alone cannot define successful digital Islamic banking. The system must remain secure, trustworthy, financially resilient, and consistent with Shariah principles.

A research rationale should establish why an issue matters within its practical and disciplinary context before developing the central argument (Hasan et al., 2026a). Fintech has created new possibilities for Islamic financial institutions. Research already shows the growing relationship between fintech, digitalisation, and blockchain within Islamic finance (Unal & Aysan, 2022). In Bangladesh, intelligent technologies are also reshaping organizational knowledge and creating new questions about how innovation can develop without weakening Shariah compliance (Hasnat et al., 2025a).

The customer side is equally important. Islamic financial decisions are not shaped only by convenience. Knowledge, previous experience, and religious beliefs can influence how individuals understand and choose between Islamic and conventional financial products (Hasna & Salleh, 2018; Hasnat et al., 2024). Digital Islamic banking therefore depends on more than providing an application. Customers must understand the services they use and trust both the technology and the institution behind it.

This creates a direct connection with digital financial literacy. As banking becomes more dependent on artificial intelligence and other digital technologies, customers and employees need stronger knowledge to navigate new financial environments responsibly (Hasan et al., 2026b). A customer who does not understand digital security may become vulnerable to fraud. An employee who lacks cyber awareness may unintentionally create organizational risk. Fintech development must therefore be accompanied by knowledge development.

The contracts themselves are also changing in form. Islamic banking traditionally depends on clear contractual structures and responsibilities. The implementation of arrangements such as Kafalah shows the importance of operational clarity within Islamic financial organizations (Hasnat & Alom, 2017). When these contracts move into digital platforms, questions about authentication, data integrity, automated execution, and accountability become more important.

Cybersecurity therefore cannot be treated simply as an information technology problem. Digital Islamic banking involves customer money, personal information, contractual obligations, and institutional trust. A cyber incident can affect all of these at once. Research on Islamic mobile banking also indicates that data security matters for continued customer use of digital financial services (Sofyani & Darma, 2024).

The organizational dimension should not be overlooked. Cyber-FinTech environments require clear communication between boards, managers, technical teams, and employees. Research connecting boardroom communication, artificial intelligence, human resource management, and Cyber-FinTech shows that technological change also creates internal organizational challenges (Hasan et al., 2025). Digital resilience therefore depends not only on software and security systems, but also on people, communication, and institutional culture.

HHH Research Blog
Research for Impact
https://doi.org/10.66246/hq1x6r23
Vol 1, Issue 2

Research Gap

The research gap lies in the separation between fintech development, cybersecurity, financial resilience, customer behaviour, and Shariah governance. Fintech studies often focus on adoption and efficiency. Cybersecurity research concentrates on technical risk. Islamic banking research examines Shariah compliance. Financial regulation focuses on capital and institutional stability. These areas are closely connected in practice, but they are still frequently examined separately.

A research gap should identify what remains unresolved and explain why the missing knowledge matters (Hasnat et al., 2026b). The key unresolved issue is how Islamic banks can govern digital innovation as one integrated system. A new fintech product may involve software developers, cybersecurity specialists, risk managers, regulators, Shariah scholars, customer service teams, and external technology providers. Yet these groups may evaluate the same product from different perspectives.

Financial resilience adds another layer. The global financial crisis demonstrated why banks need stronger systems for managing risk and maintaining institutional stability (Hasnat & Talukder, 2017). More recent evidence from Bangladesh also shows the importance of regulatory frameworks such as Basel III in shaping banking performance and resilience (Yamin et al., 2025). However, traditional prudential regulation does not address every risk created by artificial intelligence, data dependency, cloud services, digital fraud, or third-party fintech providers.

Cybersecurity governance must therefore connect with wider financial governance. Junita et al. (2026) demonstrates the relevance of a Maqasid al-Shariah perspective for cybersecurity risk management and data protection in Islamic banking. This raises an important question. Should the protection of digital assets and customer information be treated only as technical compliance, or should it also become part of Shariah governance?

The ethical dimension is also underdeveloped. Ethical leadership becomes increasingly important when artificial intelligence influences financial management and institutional decisions (Hasnat et al., 2026a). An automated system may improve efficiency, but someone must remain responsible for how it operates. The same issue applies when algorithms influence customer risk assessment, access to financial products, or fraud monitoring.

Islamic financial standards must also evolve with technology. Khandakar et al. (2025) emphasizes the importance of equity, justice, and inclusive development within Islamic financial systems. These principles should remain visible when financial services become automated. A technically efficient platform should not create unfair exclusion, hidden decision-making, or irresponsible use of customer information.

A deeper issue concerns organizational values. Research on human behaviour and ideological systems shows that institutional outcomes are influenced by the values that shape decisions and behaviour (Hasnat et al., 2025b; Babur et al., 2026). Cybersecurity culture works in a similar way. Policies may exist on paper, but employees and leaders must value responsibility, honesty, and accountability for those policies to work in practice.

Trust is therefore both a technical and social outcome. A secure system protects data. A trustworthy institution also communicates honestly, treats customers fairly, and responds responsibly when problems occur. A Shariah-aligned understanding of social well-being further emphasizes dignity, responsible conduct, and protection from harmful behaviour (Hasnat et al., 2026c). These principles have clear relevance to digital financial relationships.

HHH Research Blog
Research for Impact
https://doi.org/10.66246/hq1x6r23
Vol 1, Issue 2

Future Implications

Future development should begin with one principle. Islamic banks should not add cybersecurity and Shariah review after a fintech product has already been designed. Both should become part of the development process from the beginning. Future implications should connect research evidence with practical directions for policy, institutions, and innovation (Khandakar et al., 2026).

This suggests a model of security-by-design and Shariah-by-design. Fintech developers, cybersecurity professionals, risk managers, Shariah scholars, and senior leaders should work together when new digital products are created. Ethical leadership is particularly important because responsibility for artificial intelligence and digital financial decisions cannot be transferred entirely to technology (Hasnat et al., 2026a).

Islamic banks should also strengthen cyber resilience beyond technical controls. Encryption, secure authentication, monitoring, and incident response remain essential. However, employees need continuous training. Board communication must be clear. Cybersecurity responsibilities should be understood across the organization rather than remaining within one technical department (Hasan et al., 2025).

Customers also need stronger digital financial literacy. The earlier literature on Islamic investment behaviour shows that knowledge and experience matter in financial decision-making (Hasna & Salleh, 2018; Hasnat et al., 2024). The same principle becomes more important in digital banking. Customers need to recognize fraud, protect credentials, understand digital products, and know how their information is being used. Knowledge management can therefore become an important part of building safer digital financial ecosystems (Hasan et al., 2026b).

Future research should also examine how established Islamic contracts operate in automated environments. Concepts such as Kafalah may take new digital forms, but their underlying responsibilities must remain clear (Hasnat & Alom, 2017). Smart contracts and automated processes should not create uncertainty about who is accountable when technology fails.

The future of Islamic banking therefore depends on more than digitalisation. A fast application is not enough. A secure platform is not enough if customers do not trust it. Shariah compliance is also not enough if ethical principles are disconnected from data governance, cybersecurity, and automated decision-making.

The real opportunity lies in bringing these disciplines together. Fintech can improve access and efficiency. Cybersecurity can protect customers and institutions. Financial regulation can strengthen resilience. Shariah governance can preserve ethical and contractual integrity. Leadership can connect these responsibilities, while digital literacy can help customers and employees participate safely.

Islamic banking will become truly prepared for the digital future when innovation, security, knowledge, resilience, and ethical responsibility develop together. The goal should therefore be more than digital transformation. It should be the creation of a financial system in which technology strengthens, rather than weakens, trust.

Funding
This research received no external funding.

Acknowledgements
This Research Blog post was written by the founding members of HHH Research Consultancy & Development

Conflict of Interests
The authors declare that there is no conflict of interests.

REFERENCES

Babur, M. A., Hasnat, M. A., & Er, B. (2026). Changing human behavior based on ideologies can replace the system: Capitalistic system to Islamic system. *Uluslararası İktisadi ve İdari İncelemeler Dergisi, 51*, 195–210. https://doi.org/10.18092/ulikidince.1824851

Hasan, K. K., Hasnat, M. A., & Khandakar, H. (2025). Boardroom communication networks and AI driven HRM in Cyber-FinTech: A theory building framework for employee retention. *Telematics and Informatics Reports*, 100280. https://doi.org/10.1016/j.teler.2025.100280

Hasan, K. K., Hasnat, M. A., & Khandakar, H. (2026a). Framing the rationale in research blogging: Establishing relevance and context across disciplines. *HHH Research Blog, 1*(1). https://doi.org/10.66246/9acv8522

Hasan, K. K., Hasnat, M. A., & Khandakar, H. (2026b). Knowledge management as a catalyst for digital financial literacy in Bangladesh: Integrating AI and metaverse technologies for sustainable development. *Journal of Strategy & Innovation, 37*(2), 200577. https://doi.org/10.1016/j.jsinno.2026.200577

Hasna, M. A., & Salleh, M. C. M. (2018). Comparative analysis on EPF investors' knowledge, experience, and behaviour towards investing in Islamic and conventional unit trusts: The case of Malaysia. *Journal of Islamic Economics, Banking and Finance, 14*(1), 125–145.

Hasnat, A., Islam, M. M., Rahimi, Z., & Dağlı, H. (2024). A correlation analysis of knowledge, experience, religious belief, and behavior of Malaysian EPF investors towards investing in Islamic and conventional unit trusts. *Turkish Journal of Islamic Economics, 11*(1), 101–123. https://doi.org/10.26414/A3977

Hasnat, M. A., & Alom, S. (2017). The implementation of Kafalah in Islamic banking and finance organizations in Malaysia. *International Journal of Scientific and Research Publications, 7*(7), 768–777.

Hasnat, M. A., & Talukder, K. I. (2017). The role of banking sector during the global financial crisis of 2007 and 2008. *International Journal of Scientific and Research Publications, 7*(2), 189–225.

HHH Research Blog
Research for Impact
https://doi.org/10.66246/hq1x6r23
Vol 1, Issue 2

Hasnat, M. A., Hasan, K. K., & Khandakar, H. (2025a). Intelligent machines and organizational knowledge transformation in Bangladesh's Islamic banking sector: Navigating innovation and Shariah compliance. *Journal of Integrated Islamic Finance and Socio-Economic Systems, 1*, 11–28. https://doi.org/10.65638/2978-8196.2025.01.02

Hasnat, M. A., Khandakar, H., Rahman, M. A., Islam, S. N., & Hasan, K. K. (2025b). Capitalism in modern ignorance (jahilliyah): Exploring Islamic alternatives to reshape human behaviour and provide solutions for the 21st century. *International Journal of Islamic and Middle Eastern Finance and Management, 18*(4), 975–991. https://doi.org/10.1108/IMEFM-08-2024-0393

Hasnat, M. A., Hasan, K. K., & Khandakar, H. (2026a). Ethical leadership and AI-driven financial management in Bangladesh: Toward sustainable governance in the FinTech sector. *Leadership & Organization Development Journal*, 1–27. https://doi.org/10.1108/LODJ-06-2025-0545

Hasnat, M. A., Hasan, K. K., & Khandakar, H. (2026b). Identifying the research gap: A guide to articulating scholarly contribution in blog format. *HHH Research Blog, 1*(1). https://doi.org/10.66246/2yfmj747

Hasnat, M. A., Hasan, K. K., & Khandakar, H. (2026c). A Shariah-aligned framework for social well-being: Reducing ego, jealousy, greed, and hate-driven humiliation. *HHH Research Blog, 1*(2). https://doi.org/10.66246/5b9m2h37

Junita, B., Brennaf, M. S., Octaviano, D., & Fatiha, Z. D. (2026). Maqasid Al Shariah framework for cybersecurity risk management and data protection in global Islamic banking. *Journal of Business Management and Islamic Banking, 5*(1), 77–94.

Khandakar, H., Hasan, K. K., & Hasnat, M. A. (2026). Projecting future implications in research blogs: Connecting evidence to policy, practice, and innovation. *HHH Research Blog, 1*(1). https://doi.org/10.66246/rzq8tq72

Khandakar, H., Hasnat, M. A., Rahman, M. A., Aubhi, R. U. H., Babur, A., & Hasan, K. K. (2025). Reforming Islamic financial standards for inclusive and sustainable development: A Maturidi creed perspective on behaviour, equity and justice. *International Journal of Ethics and Systems, 41*(2), 1–25. https://doi.org/10.1108/IJOES-04-2025-0186

Sofyani, H., & Darma, E. S. (2024). Effect of architecture and efficiency of mobile banking application on the intention to continue using Islamic bank: Does data security matter? *Journal of Islamic Marketing, 15*(6), 1479–1497. https://doi.org/10.1108/JIMA-07-2023-0220

Unal, I. M., & Aysan, A. F. (2022). Fintech, digitalization, and blockchain in Islamic finance: Retrospective investigation. *FinTech, 1*(4), 388–398. https://doi.org/10.3390/fintech1040029

Yamin, N., Asif, M., Hasnat, M. A., Islam, M. M., Nasiruddin, M., Khandakar, H., & Rahman, M. A. (2025). The impact of Basel III implementation on the financial performance of the banking industry in Bangladesh. *Banks and Bank Systems, 20*(1), 98–108. https://doi.org/10.21511/bbs.20(1).2025.09