CYBERSECURITY AND OPERATIONAL RISK IN ISLAMIC BANKING: ENHANCING GOVERNANCE AND SHARIAH COMPLIANCE IN THE DIGITAL AGE

[1]Rifa Nur Alifah, [2]Rochmat Subagiyo, [3]Muhamad Aswad
[1,2,3]UIN Sayyid Ali Rahmatullah Tulungagung Indonesia
Email: rifanuralifah33@gmail.com

Abstract

The acceleration of digitalization in Islamic banking not only presents opportunities but also brings new threats in the form of increasingly complex cyber attacks and operational failures. These risks affect not only financial stability but also Shariah compliance. This study aims to analyze in depth cybersecurity and operational risks in Islamic banking. Using a qualitative approach based on literature analysis, this study finds that cyber attacks have the potential to directly result in Shariah non-compliance due to data manipulation and violation of customer trust. This study contributes to the literature by introducing a new paradigm regarding cyber risk, operational risk, and Shariah compliance that cannot be separated from the digital ecosystem of Islamic banking.

Keywords: Cybersecurity, Operational Risk, and Islamic Banking

INTRODUCTION

Advances in information and communication technology have brought rapid changes in various sectors, especially the banking industry. Digital transformation in banking has driven significant changes, from increased operational efficiency and reduced service costs to easier customer access to all services through digital platforms. However, behind these opportunities, digitization also brings challenges, namely cybersecurity risks and operational risks that are more complex, unpredictable, and have the potential to threaten system stability. In the context of Islamic banking, risk challenges are not only technical or financial in nature, but also concern sharia compliance, which is the foundation of Islamic financial institutions(Trinita, 2025).

Cybercrime is criminal activity carried out using technology or digital data, usually targeting the banking sector, where individuals' personal information is the target. Based on information from the Ministry of Communication and Information Technology, Indonesia ranks third globally in terms of the number of cybercrime cases (Muhammad Ghozali et al., 2024). In 2023, cyber threats to sharia digital platforms reached 170% since 2023, with 43% of threats targeting electronic payment systems, according to research by global cyber security company Fortinet (Putro et al., 2025).

In addition to complying with sharia principles, it is important to maintain the integrity of customer data because it is not only a matter of obligation but also reflects the trust that must be given to customers. Therefore, every sharia financial institution must adopt the latest security technology and not forget to conduct regular audits to identify and address potential threats in the future (Hera Susanti, 2024).

Research conducted by Ubay Harun explains that cybercrime significantly affects customer trust, while cybersecurity has a very strong positive influence. Therefore, his research concludes that there is a need to increase investment in digital security to maintain customer trust, which will indirectly support the stability and growth of the Islamic economy (Ubay Harun et al., 2025). Meanwhile, research conducted by Nurkhonzi S. Hadi explains that in order for Islamic banks to remain relevant and competitive, they must be more proactive in integrating and developing technology, while maintaining Islamic values in each of their new innovations. This will enable Islamic banks to not only survive in the digital era but also become a solution for ethical, sustainable, and relevant finance (Hadi, 2023).

By combining operational risk analysis, digital technology, and Sharia values, this article offers strategic insights needed by academia and industry to build a more resilient, secure, and trustworthy Islamic banking ecosystem.

RESEARCH METHOD

This research uses a qualitative library research method that focuses on analyzing academic and scientific sources related to the topic of Islamic banking. The main sources discuss Islamic banking, Islamic security, digital transformation, and operational risk. This method was chosen to gain an in-depth understanding of the concepts, implementation, and impact of digital transformation on banking. The data sources in this study are books, journal articles, and previous studies. The analysis process was carried out by identifying important patterns from the literature reviewed. These were then interpreted into descriptive sentences to draw comprehensive conclusions

RESULTS AND DISCUSSION

Cybersecurity as a New Source of Operational Risk in Islamic Banking

Banking is one industry that must be responsive to changes that pose various risks that can affect its performance. One risk that requires special attention is the issue of customer data leaks and various cyber attacks. The existence of technology in the Islamic banking industry provides many benefits, but behind it all, banks must face the threat of Cybersecurity. Therefore, Islamic banks must be able to increase their knowledge of cybersecurity due to the rise of cybercrime (Trinita, 2025).

Some of the challenges that Islamic banking must face in this digital era include: Phishing and social engineering attacks, which are generally carried out by targeting the psychology of the parties involved, where they manipulate the psychology of customers and employees to obtain confidential information. These attacks can have fatal consequences because they can destroy customer trust and tarnish the reputation of Islamic banks in an instant.

Malware and ransomware pose an even more serious threat because they cause data leaks, financial information theft, and can disrupt the smooth operation of Islamic banking systems, causing banks to lose control over highly confidential information systems. Islamic banks also face the more complex problem of maintaining cyber security while complying with Islamic principles. Islamic banks are required to guarantee compliance with Islamic norms and ethics in implementing cybersecurity. If banks cannot guarantee Sharia principles, it indirectly damages the image of Islamic banks and threatens the financial stability built on customer trus (Asrofi et al., 2024).

Therefore, it can be concluded that this cyber problem not only reduces operational performance but also indirectly threatens Sharia compliance. In the context of banking, this cyber attack threat has three fundamental implications. First, data leaks reflect a breach of trust, which is a value that is deeply ingrained in the principles of Sharia financial transactions. Second, interference or manipulation will affect Sharia validity. Third, algorithm errors in digital products are feared to cause gharar or inconsistency.

The era of digitalization offers great potential for banks to improve operational efficiency, but its implementation must be carefully planned, both in terms of risk management and the involvement of Shariah experts. By adopting the right technology and risk management, Islamic banks will continue to grow and meet customer needs in the digital era (Hutagalung, 2024).

Sharia Governance Vulnerabilities in the Digital Era

Good Corporate Governance in Islamic banks plays a strategic role in ensuring healthy, transparent, and Shariah-compliant bank management (Trinita, 2025). Shariah Governance is key to ensuring that the operations of Islamic financial institutions are in accordance with Shariah principles (Aditya & Citra Lestari, 2024). In this era of digital transformation, Islamic business institutions are required to adapt Shariah principles to governance, where digital changes are becoming increasingly complex and feared to diminish the value of Shariah itself. Digital transformation brings great opportunities for Islamic banking, from improving operational efficiency to the emergence of innovative products. Therefore, flexible, collaborative, and inclusive governance is needed so that digital transformation can be directed to strengthen the Sharia ecosystem

The success of digital transformation in Islamic banking is highly dependent on an adaptive and comprehensive governance system that includes DPS, responsive regulations, and technical frameworks such as blockchain and AI. Therefore, we can consider adaptive governance to be a key pillar in achieving sustainability and competitiveness in the future (Bahtiar et al., 2025).

Integration of Cybersecurity, Operational Risk, and Sharia Compliance

Digitalization in Islamic banking has created a new landscape, where risks previously associated with manual process failures have now been replaced by cyber attacks. These risks not only threaten the stability and image of banks but also cause non-compliance with Sharia principles, which directly impacts customers. To overcome these risks, a security system is needed that not only protects the system but is also capable of maintaining Sharia principles. Therefore, awareness of cybersecurity is needed for proactive measures in protecting important data and assets. According to research by Riki Sandrina Ayu, we can adopt COBIT and the NIST Cybersecurity Framework to increase resilience against attacks (AYU et al., 2025).

The risks faced by Islamic banking due to digitalization cannot be avoided, including information technology risks, cybersecurity risks, and complex operational risks. To respond to these issues, Islamic banking can adopt a risk-based approach that utilizes data analytics for real-time monitoring of risk exposure. Some banks have already utilized artificial intelligence (AI). Additionally, there are efforts to digitize Islamic audit functions to ensure that financial transactions comply with Islamic principles (Ahady, 2025).

CONCLUSION

Digital transformation not only brings change but also carries risk consequences such as cyber attacks that have a fatal impact on Islamic banking and sharia compliance. Cyber attacks are not only financially damaging but also disrupt customer trust and have the potential to create usury, gharar, or uncertainty. Therefore, a security strategy is needed that not only focuses on the banking system but also upholds sharia principles.

REFERENCES

1. Aditya, R., & Citra Lestari, B. (2024). Sinergi Pengawasan Syariah dan Tantangan Regulasi Fintech dalam Penguatan Tata Kelola Perbankan Syariah di Indonesia. *JIMU: Jurnal Ilmiah Multi Disiplin*, *03*(02), 3031–9498.
2. Ahady, A. A. (2025). Strategi manajemen risiko perbankan syariah : Adaptasi di era digital dan ketidakpastian ekonomi. *Maliki Interdisciplinary Journal (MIJ)*, *3*, 96–100.
3. Asrofi, A. K., Sanawati, C. K., & Sya'idun, S. (2024). Menakar Risiko Pembiayaan Bank Syariah di Era Digital. *Lab*, *8*(02), 205–225. https://doi.org/10.33507/lab.v8i02.2478
4. AYU, R. S., RivaI, M. M., Mubarak, N. Al, & Pratama, D. (2025). KEAMANAN INFRASTRUKTUR TEKNOLOGI INFORMASI: ANALISIS ANCAMAN SIBER DAN PENDEKATAN MITIGASI. *Jurnal Pendidikan Sosial Dan Humaniora*, *4*(2), 195–222. https://doi.org/10.1201/9781032622408-13
5. Bahtiar, Diantama, S., & Arlovin, T. (2025). Transformation Of Sharia Business Management Governance In The Digital Era Transformasi Manajemen Bisnis Syariah Governance Di Era Digital. *Jurnal Fokus Manajemen*, *5*(3), 635–644.
6. Hadi, N. S. (2023). Urgensi Bank Syariah di Indonesia Pada Era Digital. *Jurnal Sisfortek*, *1*(1), 1–5.
7. Hera Susanti, K. (2024). Tantangan dan Peluang Perbankan Syariah di Era Digital dalam Pertumbuhan Berkelanjutan. *Persya: Jurnal Perbankan Syariah*, *2*(1), 13–19. https://doi.org/10.62070/persya.v2i1.53
8. Hutagalung, M. W. R. (2024). *Manajemen Risiko Bank Syariah*. Merdeka Kreasi Group. https://books.google.co.id/books?id=35lrEQAAQBAJ&pg=PA68&dq=tantangan+utama+dalam+keamanan+siber+yang+dihadapi+oleh+bank+syariah&hl=id&newbks=1&newbks_redir=0&sa=X&ved=2ahUKEwiy2J-jvIaRAxWgVmwGHYXeKgoQ6AF6BAgHEAM#v=onepage&q=tantangan utama dalam keamanan
9. Muhammad Ghozali, Nora Liana, Cut Afra, Zulfadly Siregar, Nurfahni, Malahayati, & Muhammad Hatta. (2024). Kejahatan Siber (Cyber Crime) dan Implikasi Hukumnya: Studi Kasus Peretasan Bank Syariah Indonesia (BSI). *Cendekia : Jurnal Hukum, Sosial Dan Humaniora*, *2*(4), 797–809. https://doi.org/10.70193/cendekia.v2i4.113
10. Putro, H. K., Andriani, & Sifa, M. A. (2025). Manajemen Resiko Pembiayaan Bank Syariah Indonesia: Tantangan dan Solusi. *Journal of Islamic Banking*, *3*, 78–90.
11. Trinita, C. H. (2025). Implementasi Hukum Ekonomi Syariah dalam Penyelenggaraan Good Corporate Gonvernande bank syariah. *Media Hukum Indonesia (MHI)*, *2*, 61–66. https://doi.org/https://doi.org/10.5281/zenodo.15575235
12. Ubay Harun, Muthmainnah, & Rizki Amalia. (2025). Cyber crime vs cyber security: implications for customer trust in e-banking at Indonesian Islamic banks. *Jurnal Ilmu Perbankan Dan Keuangan Syariah*, *7*(1), 35–54. https://doi.org/10.24239/jipsya.v7i1.320.35-54