International Conference on Islam, Law, and Society (INCOILS)
Conference Proceedings 2025

Cyber Attack Risk Mitigation in the Digital Transformation of Islamic Banks in Indonesia

Herlina Wati, S.E.[1] Dr. Mohammad Aswad, M.A.[2] Dr. Rokhmat Subagiyo, M.E.I.[3] Dr. Binti Nur Asiyah, M.Si., C.E.[4]

[1234] UIN Sayyid Ali Rahmatullah Tulungagung

[1]herlinasofi70@gmail.com, [2]MuhammadAswad@uinsatu.ac.id,
[3]rokhmatsubagyo@uinsatu.ac.id, [4]binti.nur.asiyah@uinsatu.ac.id

ABSTRACT :

This study aims to analyze the forms of cyber attacks that arise in the process of digital transformation of Islamic banking in Indonesia and to examine relevant mitigation strategies based on the principles of maqashid syariah. The accelerating pace of digital transformation has increased exposure to cyber risks, including phishing, ransomware, and data leaks that have the potential to disrupt the operational stability of banks. This study uses a descriptive qualitative approach with secondary data sourced from official reports from the National Cyber and Crypto Agency (BSSN), the Financial Services Authority (OJK), scientific publications, and regulations related to digital data protection. The analysis was conducted using document analysis techniques to identify threat patterns and mitigation strategies applied in the literature and national policies. The results of the study indicate that cyber risk mitigation in Islamic banks requires an integrated approach that is not only technical in nature but also reflects Sharia values such as amanah, hifdz al-mal, and maslahah.

Key words: *Cybersecurity, Digital Transformation, Islamic Banking.*

INTRODUCTION

The digital transformation in Islamic banking in Indonesia has shown rapid development in line with advances in financial technology (fintech) and increasing customer demand for fast, secure services that comply with Islamic principles[1]. The implementation of various innovations such as Islamic mobile banking, digital payments, and peer-to-peer financing services has brought significant changes to the efficiency and convenience of customer transactions[2].

This innovation not only supports the improvement of Islamic financial inclusion, but also expands the reach of services to communities that previously had difficulty accessing the formal financial system[3]. Furthermore, this progress is in line with the vision of the government and the Financial Services Authority (OJK) to strengthen the digital-based Islamic financial ecosystem, as

[1] Umul Nuraini, "Dinamika Perbankan Syariah Di Era Digital: Tantangan, Inovasi, Dan Arah Masa Depan," *ACTIVA : Jurnal Ekonomi Syariah* 6, no. 2 (2023), https://jurnal.stitnualhikmah.ac.id/index.php/activa/article/view/2606/1468.

[2] Hasni Hasni, "Peran Financial Technology Dalam Meningkatkan Kinerja Perbankan Syariah Di Indonesia," *Jurnal Ekonomi dan Bisnis* 23, no. 1 (2022): 56, https://doi.org/https://doi.org/10.59729/alfatih.v7i1.134.

[3] Risna Nur Ainia, "Peran Financial Technology Dalam Meningkatkan Kualitas Layanan Pada Perbankan Syariah Di Indonesia," *Jurnal Al-fatih Global Mulia* 7, no. 1 (24 Agustus 2025): 20–33, https://doi.org/10.59729/alfatih.v7i1.134.

reflected in the increasing market share of Islamic banking, which reached 10% in 2023, along with regulatory encouragement and the continuous development of digital literacy among the public[4].

The growth of Islamic banking in the context of Industry 4.0 is also driven by the application of various digital technologies such as the Internet of Things (IoT), blockchain, and artificial intelligence (AI), which facilitate the automation of financial services[5]. Islamic banks are now focusing on product innovation and operational efficiency, as well as strengthening their competitiveness through collaboration with the fintech sector. Digitalization enables faster and more accessible service processes, improves customer experience, and expands the inclusiveness of Islamic financial services[6]. Thus, digital transformation not only supports business innovation but also serves as an important strategy for maintaining the sustainability of the Islamic banking industry in the digital era.

Previous studies have shown that the issue of cybersecurity in Islamic banking has not been comprehensively studied. Fasa (2024)[7] discusses the digital transformation of Islamic banking, but the study does not elaborate on cybersecurity risks in depth. Parulian et al. (2021)[8] examined cyberattack threats in Indonesia, but the context of the study was still general and not specific to Islamic banks. Meanwhile, Anugrah et al. (2025)[9] highlighted ethical aspects in the BSI data breach incident, but the focus was more on professional ethics without developing a technical mitigation model. Another study by Sari et al. (2025)[10] discusses risk oversight in Islamic banks, but does not touch on defensive strategies against cyber attacks. This indicates a research gap that needs to be filled by this study.

---

[4] Fatkhul Wahab dan Moh. Ihsan, "Revolusi Digital Perbankan Syariah: Mendorong Inovasi Keuangan Islam di Indonesia," *Journal of Islamic Finance and Syariah Banking* 2, no. 2 (20 April 2025): 87–99, https://doi.org/10.63321/jifsb.v2i2.74.

[5] Azizah Shodiqoh Rafidah K K dan Happy Novasila Maharani, "Inovasi Dan Pengembangan Produk Keuangan Syariah: Tantangan Dan Prospek Di Era Revolusi Industri 4.0," *Jurnal Ilmiah Edunomika* 8, no. 1 (2024), https://doi.org/https://doi.org/10.29040/jie.v8i1.11649.

[6] Muhammad Iqbal Fasa, "Transformasi Digital Era Industri 4.0 Revolusi Layanan Yang Mengubah Lanskap Perbankan Syariah Di Indonesia," *Jurnal Intelek Dan Cendikiawan Nusantara* 1, no. 5 (2024): 7653–65.

[7] Fasa.

[8] Sahat Parulian, Devi Anassalifa Pratiwi, dan Meiliya Cahya Yustina, "Ancaman dan Solusi Serangan Siber di Indonesia," *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)* 1, no. 2 (2021): 85–92, http://ejournal.upi.edu/index.php/TELNECT/.

[9] Suci Anugrah et al., "Pengaruh Etika Profesi Terhadap Keamanan Informasi dalam Konteks Kebocoran Data BSI (Bank Syariah Indonesia): Studi Literatur Sistematis The Influence of Professional Ethics on Information Security in the Context of the BSI Data Breach : A Systematic Li," *JTK3TI: Jurnal Tata Kelola dan Kerangka Kerja Teknologi Informasi* 11, no. 2 (2025): 106–12, https://doi.org/https://doi.org/10.34010/jtk3ti.v11i2.17033.

[10] Sitti Nikmah Marzuki Surya Karmila Sari, Lisa Anggryani, Rahmat Hidayat, "Tantangan Dan Solusi Dalam Pengawasan Risiko Di Perbankan Syariah Pada Era Cyber: Tinjauan Literatur Bank Syariah Indonesia," *LAN TABUR: Jurnal Ekonomi Syariah* 6, No. 1 (2024): 91–109, Https://Doi.Org/Https://Doi.Org/10.53515/Lantabur.2024.6.1.91-109.

Behind the progress of digitalization, the implementation of digital banking, open banking, and artificial intelligence (AI) in Islamic banking systems also presents serious challenges in the form of potential cyber attacks. Threats such as phishing, malware, ransomware, and data breaches are risks that must be anticipated comprehensively. Banking digitalization does increase efficiency, but it also expands the attack surface for cybercriminals, especially against digital banking systems that are connected to global networks[11]. These threats can cause financial losses, damage to the bank's reputation, and a decline in customer confidence in the security of their personal data.

The increasing frequency of cyber attacks on the financial sector has also been identified as one of the biggest risks in the era of digital transformation. Various attacks such as malware, ransomware, and DDoS attacks have grown in complexity and destructive power, and can even paralyze banking operational systems entirely[12]. In the context of Islamic banking, these threats have broader implications because they concern public trust and the principle of amanah in safeguarding assets (hifdz al-mal). Therefore, the implementation of a robust digital security system based on Islamic principles is an absolute necessity for the sustainability of the digital transformation of Islamic banks in Indonesia.

Based on the results of previous research mapping, it can be concluded that studies on cybersecurity in Islamic banking in Indonesia are still limited, especially those that link digital transformation, emerging cyberattack patterns, and mitigation strategies in line with the principles of maqashid sharia. Most studies only discuss technical or ethical aspects, without integrating the two into a single framework. Therefore, this study specifically focuses on identifying the types of cyber attacks that most frequently occur in Islamic banks in Indonesia and developing cyber risk mitigation strategies that are not only technically effective but also in line with the principles of amanah, maslahah, and hifdz al-mal. This narrowing of focus was done to address the feedback that the previous theme was still too broad and did not indicate a specific research problem.

Based on the 2024 report from the National Cyber and Crypto Agency (BSSN), cyber attacks on the financial sector in Indonesia increased by more than 35% compared to the previous year, with the majority of attacks taking the form of malware, ransomware, and Distributed Denial of Service (DDoS) targeting financial institutions, including Islamic banking[13]. This increase indicates that the digitization of the financial system has not been fully matched by adequate cybersecurity

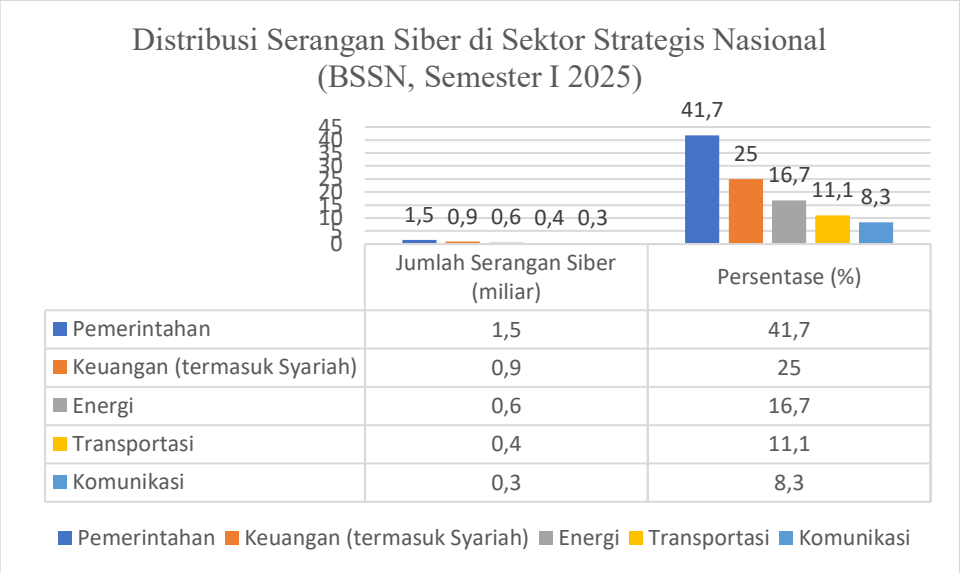
---

[11] Romy Setiawan dan Rahmadsyah, "Digitalisasi Perbankan dan Ancaman Keamanan Siber: Tantangan dan Strategi Mitigasi Risiko Operasional," *Advanced Studies in Economic, Finance and Banking* 1, no. 2 (2025), https://doi.org/10.123456/asefba.v1i1.xxxx.

[12] Eka Febriantika Nur Afifah, Diny Widya Evriyanti Simatangkir, dan Nafiza Salsabila Faliha, "Keamanan Siber Dalam Perbankan Serta Tantangan Dan Solusi Di Era Digital," *Jurnal Multidisiplin Ilmu Akademik* 2, no. 1 (2025): 33–42, https://doi.org/https://doi.org/10.61722/jmia.v2i1.3119.

[13] Susilo Wibowo, Y.B, "LAPORAN KINERJA 2024 Badan Siber dan Sandi Negara" (Jakarta: Badan Siber dan Sandi Negara, 2024).

preparedness[14]. BSSN data also reveals that throughout 2025, there were more than 3.6 billion cyber attacks in various national strategic sectors, emphasizing the urgency of protecting data and sharia-based financial transaction systems[15]. This condition requires increased supervision and integration of cybersecurity systems in accordance with national standards and BSSN regulations so that sharia bank operations remain safe, stable, and reliable.



	Jumlah Serangan Siber (miliar)	Persentase (%)
Pemerintahan	1,5	41,7
Keuangan (termasuk Syariah)	0,9	25
Energi	0,6	16,7
Transportasi	0,4	11,1
Komunikasi	0,3	8,3

Source: National Cyber and Cryptography Agency (BSSN)

Given the rapid pace of digital development and the increasing threat of cyber attacks on the financial sector, it is important for Islamic banks in Indonesia to have a comprehensive mitigation strategy based on Islamic values. However, to date there has been very limited academic research that thoroughly discusses how Indonesian Islamic banks manage cyber risks amid a massive and complex digitalization process. This makes this research relevant and urgent, as it can contribute to strengthening the literature on cybersecurity in Islamic financial systems, while also providing practical recommendations for regulators and Islamic financial institutions in formulating digital risk mitigation policies that are not only technically effective, but also in line with the principles of amanah, maslahah, and justice in Islam.

Methods

This study uses a descriptive qualitative approach because it aims to provide a comprehensive understanding of the risks of cyber attacks in the digital transformation process of Islamic banking in Indonesia. This approach was chosen to examine the phenomenon in depth through the

[14] Puteri Ananda Khairunnisa et al., "Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI: Studi Kasus di Indonesia," *Jurnal Ilmu Teknik dan Informatika* 4 (2024): 9–16, https://doi.org/https://doi.org/10.51903/teknik.v3i1.570.

[15] Saepudin Hidayat dan Aris Setyo Radyawanto, "Kemandirian Siber Indonesia: Tantangan Dan Peluang Menuju Kedaulatan Digital," *International Journal of Social and Management Studies* 6, no. 5 (2025): 98–102, https://doi.org/https://doi.org/10.5555/ijosmas.v6i5.537.

interpretation of data and information sourced from official documents and scientific literature, without collecting field data. The data used in this study is entirely secondary data, obtained from official reports from the National Cyber and Crypto Agency (BSSN), the Financial Services Authority (OJK), Bank Indonesia, regulations related to personal data protection, as well as various academic journals and scientific publications from 2019–2025 that are relevant to the topics of cyber security and the digital transformation of Islamic banking. The data collection technique was carried out through library research by examining previously published documents, reports, and scientific findings. The collected data was analyzed using document analysis techniques, which included the process of identifying, categorizing, and interpreting the main themes related to cyber attack patterns, digital risks, and mitigation strategies in accordance with sharia maqashid values such as amanah, maslahah, and hifdz al-mal. This approach allows researchers to map the development of cyber threats and formulate mitigation strategies based on valid and credible information without involving primary data.

Result

Subsection 1. Growth in the Adoption of Digital Islamic Banking

The results of the study show a significant increase in the adoption of digital services in Indonesian Islamic banking. Based on data from the Financial Services Authority (OJK, 2024), the number of customers using Islamic digital banking services increased from 9.8 million in 2022 to 13.9 million in 2024, or a growth of around 42% in the last two years. This growth has been influenced by the increasingly widespread use of smartphones, ease of internet access, and the availability of increasingly varied sharia-based digital services.

The most widely used digital services include Islamic mobile banking, digital onboarding, Islamic QRIS, and zakat, infaq, and waqf payments through official Islamic banking applications. Mobile banking has become the most dominant feature because it offers easy transactions such as checking balances, transfers, bill payments, and even Islamic-based donations. Digital onboarding also makes it easy to open an account without having to physically visit a branch office, thereby reaching areas that do not have access to conventional banks.

In addition, the increased use of Sharia QRIS has expanded cashless transactions in the halal MSME sector, mosques, Islamic educational institutions, and shopping centers. According to internal data from Islamic banks, there was an increase in Sharia QRIS transactions at halal merchants of more than 60% during 2023–2024. These results show that digital transformation not only facilitates transaction needs but also supports the Islamic economic ecosystem at the community level.

Overall, the growth of digital services in Islamic banking has proven to have an impact on service efficiency, increased customer satisfaction, and expanded financial inclusion. Islamic banks can reach more customers without having to add physical branches, making the service process faster, more cost-effective, and digitally integrated.

The most frequently used innovations include:

- Sharia mobile banking
- Digital onboarding
- Sharia QRIS
- Zakat and alms payments through digital platforms

These improvements reflect the acceleration of digital transformation, which has resulted in more efficient services and expanded sharia-based financial inclusion.

Subsection 2. Cyber Attack Trends in the Sharia Finance Sector

The following findings show the relationship between increased digitization and the growing risk of cyber attacks on sharia financial institutions. According to a report by the National Cyber and Crypto Agency (BSSN, 2024), cyber attacks on the financial sector increased from approximately 2.4 million attacks in 2022 to approximately 3.5 million attacks in 2024, an increase of around 46%. These attacks involved data theft, disruption of digital services, and intrusion into banking application systems.

The most dominant type of attack is phishing, which involves fake messages or links that mimic official bank services to steal customer login data. Attacks through ransomware have also increased, which is malware that encrypts banking system data and demands a ransom. In addition, there are DDoS attacks, which send large amounts of fake traffic to paralyze digital systems and make them inaccessible to customers.

Internal industry data shows that targeted attacks not only affect banks, but also customer devices such as mobile phones and laptops used for digital transactions. This shows that security weaknesses do not only originate from the bank's server side, but also from the user side, especially those who do not have adequate digital security literacy. A number of banks reported that more than 50% of phishing cases were successful because customers clicked on fraudulent links.

This trend shows that the more widespread the digitization of services, the greater the attack surface that can be exploited by cybercriminals. The surge in digital transactions, which is not balanced by improvements in security, opens up loopholes that can potentially harm banks and customers. These attacks mainly target core banking systems, mobile applications, and databases that store customers' personal data.

Subsection 3. Cybersecurity Implementation and Mitigation Measures

The results of the study show that the three largest Islamic banks provide a concrete picture of the implementation of digital transformation and cybersecurity. Bank Syariah Indonesia (BSI) focuses on developing BSI Mobile as an integrated digital transaction service center. Users can make transfers, digital payments, and even zakat and waqf through a single application. After the ransomware incident in 2023, BSI strengthened its system security layers through firewall updates, internal audits, and improved mechanisms for monitoring suspicious activity.

BTPN Syariah prioritizes a community-based digital model. The mobile agent banking application provides access to banking services to rural communities without having to visit a branch office. This system improves the distribution of Islamic financial services and helps housewives and small MSME players to conduct digital transactions. On the security side, BTPN Syariah implements double authentication and a layered transaction verification system.

Bank Muamalat Indonesia (BMI) has developed a digital platform called Muamalat DIN (Digital Islamic Network). This service includes QRIS Syariah features, mobile banking, and MSME payment system integration. BMI also implements an artificial intelligence (AI)-based anomaly detection algorithm to identify cyber attack patterns in real time.

In addition to these three banks, most Islamic financial institutions in Indonesia have begun to implement multi-layer security, data encryption, scheduled backup systems, and periodic security audits. The implementation of Zero Trust architecture is becoming the new standard in detecting illegal access in digital networks. This step shows that Islamic banks are not only expanding innovation but also enhancing digital resilience to ensure services remain secure and sustainable. These findings prove that improving cyber resilience is an urgent need to ensure that digital transformation remains secure, stable, and trusted by the public.

Table 1. Types of Cyber Attacks and Risk Mitigation Strategies in Islamic Banks

Type of Attack	Impack	Mitigation Strategy
Phising	Theft of customer account data and funds	Customer education, email authentication, anti-phishing filter
Ransomware	Digital services paralyzed and data encrypted	Data backup, endpoint protection, incident response plan
Data breach	Leakage of customer personal data	Encryption, access control, compliance with Personal Data Protection Law
DDoS	Service is inaccessible	Firewall and traffic filtering
AI-driven Attack	Automatic manipulation	AI anomaly detection and Zero Trust systens

The table shows that the most frequent cyber attacks on Islamic banks are not only technical in nature, but also exploit human error and digital system vulnerabilities. Phishing is the most dominant form of attack, as perpetrators take advantage of customers' carelessness through emails or fake links that look like official bank services. When customers enter their username and

password, the perpetrators gain access to steal funds and personal information. Customer education and email authentication systems are important mitigating measures because the source of the problem lies in user error, not just system weaknesses.

In the second type of attack, ransomware, perpetrators infiltrate the bank's digital system through malicious files that then lock data and shut down core banking services. The most significant impact is the cessation of digital services and the threat of losing important data. Banks affected by ransomware often have to suspend operations, as has happened to several financial institutions in Indonesia[16]. Therefore, mitigation strategies such as data backup, endpoint protection, and incident response plans are essential to ensure that services can be restored quickly.

Data breaches pose a more long-term threat because the leakage of personal data can lead to identity fraud, fund theft, and the sale of data to illegal parties. This is particularly sensitive for Islamic banks because it concerns the principles of trust and customer privacy. Mitigation measures such as encryption, access control, and compliance with the Personal Data Protection Law (PDP) are mandatory steps to ensure that digital data is protected legally and technically.

Distributed Denial of Service (DDoS) attacks aim to paralyze banks' digital services through a flood of fake traffic[17]. When the system is attacked, customers cannot access mobile banking services, transactions fail, and the bank's reputation declines. Due to the nature of these attacks on service availability, mitigation strategies using firewalls, traffic filtering, and load balancing are important to ensure that services continue to run even under attack.

Finally, AI-driven attacks demonstrate the evolution of cybercrime, which is becoming increasingly intelligent and automated. These attacks use artificial intelligence to adapt attack patterns to make them difficult to detect by conventional security systems[18]. The impact is more widespread because they can manipulate data, infiltrate systems, and steal information on a large scale. Therefore, Islamic banks have begun to implement similar technologies to defend themselves, such as AI anomaly detection and Zero Trust Architecture, which verifies all activities, even those from within the system.

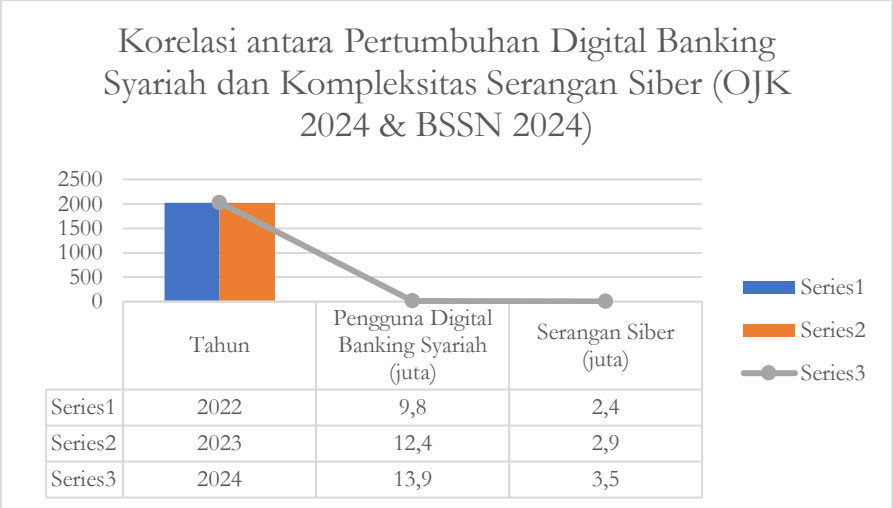
---

[16] Sitti Nikmah Marzuki Surya Karmila Sari, Lisa Anggryani, Rahmat Hidayat, "Tantangan Dan Solusi Dalam Pengawasan Risiko Di Perbankan Syariah Pada Era Cyber: Tinjauan Literatur Bank Syariah Indonesia," *LAN TABUR: Jurnal Ekonomi Syariah* 6, no. 1 (2025), https://doi.org/10.36418/syntax-literate.v9i10.

[17] Hartini Maharaja Yasin Alifsyah, Ramli, "Analisis Keamanan Komputer Terhadap Serangan Distributed Denial Of Service (DDOS)," *Journal of Renewable Energy and Smart Device* 1, no. 1 (2023): 25–30, https://pdfs.semanticscholar.org/d664/a72f4873ba7e8246c5e04b822baa9d999fcb.pdf.

[18] Rasya Amanda Novalina Khairunissa, Juhar Ananda Dika, Allyssa Az Zahra Wijanarko, Rafika Widalala, "Dampak Penggunaan Artificial Intelligence Pada Keamanan Siber: Sebuah Kajian Terhadap Potensi Keuntungan Dan Ancaman," *Berajah Journal* 4, no. 8 (1805): 1541–52, https://doi.org/https://doi.org/10.47353/bj.v4i8.458.

Overall, this interpretation shows that Islamic banks' cybersecurity systems must be multi-layered, not only technical but also educational, regulatory, and preventive. Digitalization without security will lead to operational risks, customer losses, and a loss of public trust.



	Tahun	Pengguna Digital Banking Syariah (juta)	Serangan Siber (juta)
Series1	2022	9,8	2,4
Series2	2023	12,4	2,9
Series3	2024	13,9	3,5

Source: OJK (2024); BSSN Performance Report (2024)

The graph "Correlation between Sharia Digital Banking Growth and Cyber Attack Complexity" shows that the increase in the digitization of sharia banking services goes hand in hand with an increase in the risk of cyber attacks. In 2022, the number of Islamic digital banking users reached 9.8 million, and cyber attacks in the financial sector reached 2.4 million incidents. The following year, the number of users increased to 12.4 million, followed by an increase in attacks to 2.9 million cases. This condition continued in 2024, where digital service users increased to 13.9 million, while cyber attacks jumped to 3.5 million. This pattern shows that the higher the adoption of digital transactions, the greater the attack surface that can be exploited by cyber criminals.

This correlation reinforces the interpretation in the previous table, that attacks such as phishing, ransomware, data breaches, DDoS, and AI-driven attacks continue to increase because perpetrators exploit loopholes in digital systems and low customer security literacy. This graph shows that digital transformation provides convenience and service efficiency, but without strengthening cybersecurity, digitization can create new vulnerabilities for Islamic banks. Therefore, the graph emphasizes the urgency of implementing a layered mitigation strategy through AI anomaly detection technology, Zero Trust Architecture, customer education, and personal data protection. In other words, the data in the graph proves that digital service innovation must be balanced with increased cyber resilience to ensure that the Islamic financial system remains secure, stable, and trustworthy.

Discussion

Subsection 1. The Relationship Between Digital Transformation and Increased Efficiency in Islamic Banking Services

The findings of this study show that digitization has significantly accelerated the operational efficiency of Islamic banking in Indonesia. The 42% increase in the adoption of digital banking services not only reflects technological growth but also increased convenience in transactions for the public. The use of mobile banking, digital onboarding, and QRIS Syariah has reduced dependence on face-to-face services, making transactions, payments, and account opening faster and more integrated. This shows that digitization is not merely a technical innovation but an important instrument in increasing the competitiveness of Islamic banks amid national financial industry competition.

This increase in efficiency is in line with Fasa's (2024)[19] research, which explains that digital transformation enables Islamic banks to increase transaction speed and minimize manual errors. In addition, digitization encourages the expansion of service coverage to areas that were previously difficult to reach by physical bank networks. BTPN Syariah, for example, utilizes mobile agent banking to reach rural and non-bankable communities, so that literacy and the use of sharia-based financial services can gradually increase. Thus, digitization plays a direct role in promoting sharia financial inclusion.

These findings reinforce the theory that digital transformation is a strategic instrument for promoting sharia financial inclusion nationwide. Digitalization is not only a form of service modernization, but also part of the application of sharia maqashid in realizing the economic welfare of society. From the perspective of sharia maqashid, the digitalization of services also supports the principle of maslahah, which is to provide benefits to society at large. Zakat, infaq, sadaqah, and waqf services through sharia-based applications make it easier for people to carry out their religious obligations transparently and accountably[20]. With the digital model, the muamalah process becomes more effective, secure, and in accordance with sharia guidance. This proves that technological innovation does not conflict with Islamic principles, but rather strengthens the ethical mission of Islamic financial institutions.

Subsection 2. The Relationship Between Increased Digitalization and Vulnerability to Cyber Attacks

---

[19] Fasa MI Bagas, "Transformasi digital era industri 4.0 revolusi layanan yang mengubah lanskap perbankan syariah di Indonesia," *JICN: Jurnal Intelek dan Cendikiawan Nusantara.* 1, no. 5 (2024): 7653–65, https://jicnusantara.com/index.php/jicn.

[20] Ahmad Hendra Rofiullah, "Pengembangan Ekonomi Syariah dalam Perspektif Maqashid Syariah di Era Ekonomi Digital," *SAUJANA : Jurnal Perbankan Syariah dan Ekonomi Syariah* 07, no. 02 (2025): 24–43, https://doi.org/https://doi.org/10.59636/saujana.v7i2.295.

Although digital transformation provides many benefits, research findings also show that increased digital activity has consequences in the form of a higher potential for cyber attacks. BSSN (2024) data shows that cyber attacks on the financial sector increased from 2.4 million in 2022 to 3.5 million in 2024. This increase is an indication that Islamic banking digital systems are increasingly becoming strategic targets for cybercriminals. Core banking systems, customer databases, and mobile banking services are vulnerable points that can be exploited.

The most dominant types of attacks are phishing, ransomware, malware injection, and data breaches. Phishing attacks exploit customer negligence and low digital security literacy. Meanwhile, ransomware attacks target core systems and lock access to important data until a ransom is paid. Such attacks not only cause financial losses but also undermine public trust. Parulian et al. (2021)[21] mention that digital attacks on the financial sector have a cumulative impact because they not only shut down systems but also affect economic stability and customer psychology.

Cyber vulnerability in the context of Islamic banking has broader implications than conventional banks because it concerns the principles of trust and protection of property (hifz al-mal)[22]. When customer data is leaked or their transactions are compromised, it is not only a technical violation but also a moral violation. Therefore, digitization must be balanced with increased cyber resilience so as not to cause harm to society. This shows the need for synergy between technology, regulation, and digital security education.

Subsection 3. Integration of Technology-Based Mitigation Strategies and Sharia Principles

Based on the results of the analysis, Islamic banks have developed various mitigation strategies to maintain the security of digital systems. The implementation of multi-factor authentication (MFA), data encryption, layered firewalls, endpoint protection, and the use of AI anomaly detection are preventive measures to detect attacks more quickly. BSI, for example, strengthened its information technology governance after the 2023 ransomware incident[23]. Meanwhile, Bank Muamalat built a security system based on Zero Trust Architecture, which ensures that every network access must be verified without exception.

---

[21] Parulian, Pratiwi, dan Cahya Yustina, "Ancaman dan Solusi Serangan Siber di Indonesia."

[22] Jasmiko Aryo Lestarm Shodini Putri, Lindy Arina Pramudita, Suci Marhania, Bella Sartika, Arin Ardianty, Walid Syauq, "Perbandingan Perlindungan Harta (Hifdz Al-Mal) Antara Perbankan Dan Konvensional," *Journal of Economics and Business* 2, no. 1 (2024): 87–98, https://doi.org/https://doi.org/10.61994/econis.v2i1.468.

[23] Anugrah et al., "Pengaruh Etika Profesi Terhadap Keamanan Informasi dalam Konteks Kebocoran Data BSI (Bank Syariah Indonesia): Studi Literatur Sistematis The Influence of Professional Ethics on Information Security in the Context of the BSI Data Breach : A Systematic Li."

These findings are in line with research by Rabbani and Diana (2023)[24], which concluded that the application of machine learning can increase attack detection accuracy to over 99%. This shows that developments in cyber technology can be an effective defense tool when adopted in a planned manner. Furthermore, mitigation is not only carried out at the technological level, but also at the governance level. Periodic system audits, employee training, penetration testing, and compliance with the Personal Data Protection Law (PDP) are part of a sustainable security strategy.

From a sharia perspective, risk mitigation is part of the moral responsibility of financial institutions to protect the interests of society. The principle of amanah requires banks to maintain the confidentiality of customer data and assets. The principle of maslahah requires banks to protect the public from potential losses due to digital crime. Meanwhile, the principle of 'adl emphasizes the importance of fairness in providing protection and services to all customers equally. Thus, strengthening cybersecurity is a concrete manifestation of the implementation of maqashid sharia in the era of digital transformation.

Subsection 4. Strengthening Sharia cyber resilience through governance and ethical integration

The transformation of Islamic banking towards digitalization requires not only technological readiness, but also strong governance mechanisms that reflect compliance with sharia principles and ethical responsibilities. Governance in the context of cyber security means establishing comprehensive policy structures, involving management commitment, clear risk management procedures, and coordination with national cyber security authorities such as BSSN and OJK. In Islamic banking, governance should not stop at administrative compliance alone, but must reflect the essence of the ethics of amanah (trust) and 'adl (justice), which require every institution to safeguard customer data as amanah (hifz al-mal).

According to (Surya Karmila Sari, Lisa Anggryani, Rahmat Hidayat, 2024)[25], Islamic financial institutions need to adopt a Cybersecurity Governance Framework that integrates risk assessment, incident management, and sharia compliance audits. This framework is not only reactive to attacks but also proactive in building resilience through adaptive monitoring and learning systems. The implementation of Artificial Intelligence (AI)-based anomaly detection, for example, enables early identification of attack patterns before they develop into data breaches or ransomware attacks. However, the technological dimension alone is not enough; ethical oversight,

[24] Saddam Rabbani dan Diana Diana, "Prediksi Kategori Serangan Siber dengan Algoritma Klasifikasi Random Forest Menggunakan Rapidminer," *SMATIKA JURNAL* 13, no. 02 (21 Desember 2023): 284–93, https://doi.org/10.32664/smatika.v13i02.934.

[25] surya Karmila Sari, Lisa Anggryani, Rahmat Hidayat, "Tantangan Dan Solusi Dalam Pengawasan Risiko Di Perbankan Syariah Pada Era Cyber: Tinjauan Literatur Bank Syariah Indonesia."

transparent reporting, and increased employee awareness are equally important to ensure that digital transformation remains in line with sharia principles.

In addition, the establishment of a Sharia Cyber Ethics Committee within the Islamic banking sector can serve as a bridge between technology, sharia supervision, and governance. This committee functions to ensure compliance with ethical principles in the use of data, the application of AI, and the protection of customer privacy. Through such an institution, Islamic banks not only meet legal standards but also demonstrate moral responsibility to stakeholders, thereby strengthening public confidence in the integrity of Sharia-based financial services[26].

Subsection 5. Towards a Sustainable Sharia Cyber Security Framework

Sustainability in the digitalization of Islamic banking must include three main pillars: technological resilience, institutional governance, and ethical responsibility. These three pillars form the basis of the model proposed in this study, namely the Islamic Cyber Resilience Framework (ICRF), which combines conventional cybersecurity best practices with Sharia values.

1. Technology Dimension: Implementation of AI-based anomaly detection, Zero Trust architecture, and data encryption as forms of active protection and early prevention.
2. Governance Dimension: Transparency in risk reporting, periodic security audits, and the involvement of the Sharia supervisory board in cyber policy.
3. Sharia-Ethics Dimension: Upholding the principles of amanah (trust), maslahah (benefit), and 'adl (justice) in customer data protection and fair digital access.

In practical terms, ICRF translates the values of maqashid sharia into measurable indicators such as data confidentiality, system reliability, and ethical integrity in information management. Sharia banks that adopt this model can demonstrate dual compliance, technological compliance and ethical compliance, which reflects professional excellence and moral integrity.

As stated by Wahab & Ihsan, 2025[27], the future of Islamic finance depends not only on innovation, but also on the ability to maintain security, integrity, and public trust. Therefore, digital resilience built on Sharia ethics is the foundation for a trusted and sustainable Islamic financial ecosystem in the Society 5.0 era.

Conclusion

Digital transformation has become an important milestone in the modernization of the Islamic banking system in Indonesia. Through innovations such as mobile banking, digital

---

[26] Saepudin Hidayat Aris Setyo Radyawanto, "Kemandirian Siber Indonesia : Tantangan," *IJOSMAS: International Journal of Social and Management Studies* 6, no. 5 (2025): 98–102, https://doi.org/https://doi.org/10.5555/ijosmas.v6i5.537.

[27] Wahab dan Ihsan, "Revolusi Digital Perbankan Syariah: Mendorong Inovasi Keuangan Islam di Indonesia."

onboarding, and QRIS Syariah, Islamic financial institutions such as BSI, BTPN Syariah, and Bank Muamalat have succeeded in expanding financial access and improving the efficiency of services based on maqashid syariah values. However, this acceleration in digitalization also presents serious challenges in the form of an increase in increasingly complex cyberattack risks. Based on data from the OJK (2024) and BSSN (2024), attacks on the financial sector have increased significantly by more than 35% compared to the previous year, while the adoption of Islamic digital banking services has grown by 42% in the last two years. This phenomenon shows that increased digital innovation is accompanied by increased vulnerability to threats such as phishing, ransomware, malware injection, and data breaches. To ensure the sustainability of the digital transformation of Islamic banking, financial institutions need to integrate cyber risk management into the Islamic governance framework. The principles of amanah (trustworthiness), maslahah (benefit), and 'adl (fairness) form the ethical basis for maintaining customer trust, protecting digital assets, and ensuring fairness in risk management. Thus, cyber risk mitigation is not only a technical necessity, but also a form of moral and social responsibility for Islamic financial institutions in maintaining the stability of the Islamic financial system in the digital era.

Reference

Afifah, Eka Febriantika Nur, Diny Widya Evriyanti Simatangkir, dan Nafiza Salsabila Faliha. "Keamanan Siber Dalam Perbankan Serta Tantangan Dan Solusi Di Era Digital." *Jurnal Multidisiplin Ilmu Akademik* 2, no. 1 (2025): 33–42. https://doi.org/https://doi.org/10.61722/jmia.v2i1.3119.

Amanda Novalina Khairunissa, Juhar Ananda Dika, Allyssa Az Zahra Wijanarko, Rafika Widalala, Rasya. "DAMPAK PENGGUNAAN ARTIFICIAL INTELLIGENCE PADA KEAMANAN SIBER: SEBUAH KAJIAN TERHADAP POTENSI KEUNTUNGAN DAN ANCAMAN." *Berajah Journal* 4, no. 8 (1805): 1541–52. https://doi.org/https://doi.org/10.47353/bj.v4i8.458.

Ananda Khairunnisa, Puteri, Norul Annisa, Jadiaman Parhusip, Alamat Kampus, Jl Yos Sudarso, Kec Jekan Raya, Kota Palangka Raya, Kalimantan Tengah, dan Korespondensi Penulis. "Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI: Studi Kasus di Indonesia." *Jurnal Ilmu Teknik dan Informatika* 4 (2024): 9–16. https://doi.org/https://doi.org/10.51903/teknik.v3i1.570.

Anugrah, Suci, Nabila Raihana Qalby, Muhammad Zaky Himawan, dan Evy Nurmiati. "Pengaruh Etika Profesi Terhadap Keamanan Informasi dalam Konteks Kebocoran Data BSI (Bank Syariah Indonesia): Studi Literatur Sistematis The Influence of Professional Ethics on Information Security in the Context of the BSI Data Breach : A Systematic Li."

JTK3TI: Jurnal Tata Kelola dan Kerangka Kerja Teknologi Informasi 11, no. 2 (2025): 106–12. https://doi.org/https://doi.org/10.34010/jtk3ti.v11i2.17033.

Aris Setyo Radyawanto, Saepudin Hidayat. "KEMANDIRIAN SIBER INDONESIA : TANTANGAN." *IJOSMAS: International Journal of Social and Management Studies* 6, no. 5 (2025): 98–102. https://doi.org/https://doi.org/10.5555/ijosmas.v6i5.537.

Bagas, Fasa MI. "Transformasi digital era industri 4.0 revolusi layanan yang mengubah lanskap perbankan syariah di Indonesia." *JICN: Jurnal Intelek dan Cendikiawan Nusantara.* 1, no. 5 (2024): 7653–65. https://jicnusantara.com/index.php/jicn.

Bowen, Glenn A. "Document Analysis as a Qualitative Research Method." *Qualitative Research Journal* 9, no. 2 (2009): 27–40. https://doi.org/https://doi.org/10.3316/QRJ0902027.

Fasa, Muhammad Iqbal. "TRANSFORMASI DIGITAL ERA INDUSTRI 4.0 REVOLUSI LAYANAN YANG MENGUBAH LANSKAP PERBANKAN SYARIAH DI INDONESIA." *Jurnal Intelek Dan Cendikiawan Nusantara* 1, no. 5 (2024): 7653–65.

Hasni, Hasni. "Peran Financial Technology Dalam Meningkatkan Kinerja Perbankan Syariah Di Indonesia." *Jurnal Ekonomi dan Bisnis* 23, no. 1 (2022): 56. https://doi.org/https://doi.org/10.59729/alfatih.v7i1.134.

Hidayat, Saepudin, dan Aris Setyo Radyawanto. "KEMANDIRIAN SIBER INDONESIA: TANTANGAN DAN PELUANG MENUJU KEDAULATAN DIGITAL." *International Journal of Social and Management Studies* 6, no. 5 (2025): 98–102. https://doi.org/https://doi.org/10.5555/ijosmas.v6i5.537.

K, Azizah Shodiqoh Rafidah K, dan Happy Novasila Maharani. "INOVASI DAN PENGEMBANGAN PRODUK KEUANGAN SYARIAH: TANTANGAN DAN PROSPEK DI ERA REVOLUSI INDUSTRI 4.0." *Jurnal Ilmiah Edunomika* 8, no. 1 (2024). https://doi.org/https://doi.org/10.29040/jie.v8i1.11649.

Lestarm Shodini Putri, Lindy Arina Pramudita, Suci Marhania, Bella Sartika, Arin Ardianty, Walid Syauq, Jasmiko Aryo. "Perbandingan Perlindungan Harta (Hifdz Al-Mal) Antara Perbankan Dan Konvensional." *Journal of Economics and Business* 2, no. 1 (2024): 87–98. https://doi.org/https://doi.org/10.61994/econis.v2i1.468.

Lexy J, Moelong. *METODOLOGI PENELITIAN KUALITATIF / Lexy J. Moleong*. Revisi. Bandung: PT Remaja Rosdakary, 2018. https://perpustakaan.binadarma.ac.id/opac/detail-opac?id=40.

Maharaja Yasin Alifsyah, Ramli, Hartini. "ANALISIS KEAMANAN KOMPUTER TERHADAP SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS)." *Journal of Renewable Energy and Smart Device* 1, no. 1 (2023): 25–30.

https://pdfs.semanticscholar.org/d664/a72f4873ba7e8246c5e04b822baa9d999fcb.pdf.

Mestika, Zed. *Metode Penelitian Kepustakaan*. 1 ed. Jakarta, 2004.

Nur Ainia, Risna. "PERAN FINANCIAL TECHNOLOGY DALAM MENINGKATKAN KUALITAS LAYANAN PADA PERBANKAN SYARIAH DI INDONESIA." *Jurnal Al-fatih Global Mulia* 7, no. 1 (24 Agustus 2025): 20–33. https://doi.org/10.59729/alfatih.v7i1.134.

Nuraini, Umul. "DINAMIKA PERBANKAN SYARIAH DI ERA DIGITAL: TANTANGAN, INOVASI, DAN ARAH MASA DEPAN." *ACTIVA : Jurnal Ekonomi Syariah* 6, no. 2 (2023). https://jurnal.stitnualhikmah.ac.id/index.php/activa/article/view/2606/1468.

Parulian, Sahat, Devi Anassalifa Pratiwi, dan Meiliya Cahya Yustina. "Ancaman dan Solusi Serangan Siber di Indonesia." *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)* 1, no. 2 (2021): 85–92. http://ejournal.upi.edu/index.php/TELNECT/.

Rabbani, Saddam, dan Diana Diana. "Prediksi Kategori Serangan Siber dengan Algoritma Klasifikasi Random Forest Menggunakan Rapidminer." *SMATIKA JURNAL* 13, no. 02 (21 Desember 2023): 284–93. https://doi.org/10.32664/smatika.v13i02.934.

Rofiullah, Ahmad Hendra. "Pengembangan Ekonomi Syariah dalam Perspektif Maqashid Syariah di Era Ekonomi Digital." *SAUJANA : Jurnal Perbankan Syariah dan Ekonomi Syariah* 07, no. 02 (2025): 24–43. https://doi.org/https://doi.org/10.59636/saujana.v7i2.295.

Setiawan, Romy, dan Rahmadsyah. "Digitalisasi Perbankan dan Ancaman Keamanan Siber: Tantangan dan Strategi Mitigasi Risiko Operasional." *Advanced Studies in Economic, Finance and Banking* 1, no. 2 (2025). https://doi.org/10.123456/asefba.v1i1.xxxx.

Sonita, Era. "Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah : Menjaga Stabilitas Keuangan di Era Digital." *KRIGAN: Jurnal of Management and Sharia Business* 1, no. 2 (2023). https://doi.org/https://doi.org/10.30983/krigan.v1i2.7929.

Surya Karmila Sari, Lisa Anggryani, Rahmat Hidayat, Sitti Nikmah Marzuki. "TANTANGAN DAN SOLUSI DALAM PENGAWASAN RISIKO DI PERBANKAN SYARIAH PADA ERA CYBER: TINJAUAN LITERATUR BANK SYARIAH INDONESIA." *LAN TABUR: Jurnal Ekonomi Syariah* 6, no. 1 (2024): 91–109. https://doi.org/https://doi.org/10.53515/lantabur.2024.6.1.91-109.

———. "TANTANGAN DAN SOLUSI DALAM PENGAWASAN RISIKO DI PERBANKAN SYARIAH PADA ERA CYBER: TINJAUAN LITERATUR BANK SYARIAH INDONESIA." *LAN TABUR: Jurnal Ekonomi Syariah* 6, no. 1 (2025). https://doi.org/10.36418/syntax-literate.v9i10.

Susilo Wibowo, Y.B. "LAPORAN KINERJA 2024 Badan Siber dan Sandi Negara." Jakarta: Badan Siber dan Sandi Negara, 2024.

Wahab, Fatkhul, dan Moh. Ihsan. "Revolusi Digital Perbankan Syariah: Mendorong Inovasi Keuangan Islam di Indonesia." *Journal of Islamic Finance and Syariah Banking* 2, no. 2 (20 April 2025): 87–99. https://doi.org/10.63321/jifsb.v2i2.74.