

Cybersecurity in Islamic Banks in the Context of Digital Transformation

Belbachir Wafa¹

Laboratory for the Evaluation of Development Policies in Algeria /
Assistant Professor –B- /Abou Bakr Belkaid University (Tlemcen)
Algeria

wafaabelbachir7@gmail.com

Received date : 28/09/2025, Accepted date : 29/10/2025,Publication date:05/12/2025

Abstract :

This study investigated the cybersecurity of Islamic banks within the environment of digital transformation, which aimed at the challenges and risks that digitization poses on data protection and Shariah compliance financial transactions. While digitization enhances efficiency and broadens service delivery, it exposes users to significant threats from category-level risks, such as cyber threats and electronic fraud. The study pointed to the need for regulatory frameworks and adopting artificial intelligence, blockchain, and other high-tech solutions to secure transactions. Integrated cybersecurity strategies are recommended to safeguard customer trust and support the digital transformation that continues in Islamic finance.

Keywords: Cybersecurity ,Digital Transformation ,Islamic Banks ,Artificial Intelligence, Blockchain.

Jel Classification Codes: G21 ,G28 , O33 ,L86 ,Z12

Introduction :

Today you can see digital revolution changes within almost every sector, the major one being banking. Digitalization nowadays is an integral strategic alternative to make the process efficient, improve the quality of services, and extend the customer base. Islamic banks are also under the process of digital transformation to keep pace with the advancement in technology globally as they are also using modern tools of artificial intelligence, blockchain, cloud computing, and mobile applications. Such undertakings are meant to enhance competition vis-a-vis conventional banks and promote financial inclusion based on Sharia principles.

However, as much as it has numerous opportunities and potentials, digitization has also birthed some new challenges, cyber risks being the primary challenge in the form of hacking attempts, data theft, and electronic fraud. Such challenges are

¹ Corresponding Author.

majorly critical to the Islamic banking environment as it carries its specific nature based on the principle of transparency, trust, and safeguarding of depositor funds under Sharia-compliant regulation. Such breaches in security or leakage of sensitive information would eventually stigmatize the reputation of not just the bank but the credibility of the entire Islamic financial system, thereby making cybersecurity a strategic pillar to the success of digital transformation.

There is an urgent need to set up new advanced systems of security at technical, regulatory, and Sharia levels for the protection of digital transactions and privacy for customers. There is benefit from international top practices that have already satisfied the technological innovation and cybersecurity prerequisites while modifying those lessons to fit the specific Islamic bank context of the Arab world, especially with Algeria.

The central research problem can hence be articulated: **How can Islamic banks convert the test of digital transformation into a strengthening of cybersecurity, particularly with the customer trust built on Sharia principles?**

- **Research Objectives:**

- Investigating the reality of digital transformation in Islamic banks;
- Understanding the primary cyber risks associated with digitalization;
- The definition of the nexus between artificial intelligence and blockchain in transaction security;
- Implementation of relevant strategies for Islamic banks in Algeria.

- **Research Importance:**

This study essentially attempts to fill the gap in knowledge on cybersecurity issues concerning the Islamic banking system and recommends many practical implications for banks and regulatory authorities.

- **Research Methodology:**

Descriptive-analytical approach that is based on reviewing literature and former studies, borrowing experiences from pioneering countries for example Malaysia, UAE, and Bahrain, on effect of digitalization on financial inclusion and increase in opportunities available, with the increase of risk faced by cyberattacks which will ultimately require innovation in security policies.

- **Previous Studies:**

- 1- **Bara Samir. (2017)²:**

This paper focuses on the evolution of cybersecurity in Algeria in accordance with government policies and institutions. It highlights the increasingly alarming threats posed by cybercrime and the urgent need for effective protection of digital infrastructures. While national defense and security bodies play a central role, there is lack of adequate institutional coordination and legal frameworks. The authors emphasize the importance of updating legislation, establishing technical and human capabilities, and raising public awareness. Conclusions indicate that cybersecurity should be integrated into Algeria's overall security and development strategies.

- 2- **Shoushan, Khadija, Bououina, Hamou. (2023)³:**

² Bara, Samir. (2017), « Cybersecurity in Algeria: Policies and Institutions », Algerian Journal of Human Security, vol. 4, July 2017.

³ Shoushan, Khadija, Bououina, Hamou. (2023), « The Role of Digital Transformation in Improving the Services of Algerian Islamic Banks – Case Study of Al Salam Bank », Op. cit.

This study highlights the idea of digital transformation, as well as the most important techniques by which digital promotion and digitization of banking financial services can occur, and analyzes the reality of digital transformation in Islamic banks in Algeria and examines the major challenges that accompany it, and also investigates the case of Al Salam Bank Algeria based on the annual reports of the bank. Harnessing digital capabilities will actualize new fast and cheap business models and services. The development of technology has a significant positive effect especially with Islamic banks, since such new digital technologies enable banks to introduce their products and services more easily, very efficiently and of high quality to compete better in the market.

3- Hamel Dalila. (2025)⁴:

This research intends to showcase the contribution of artificial intelligence in fortifying cybersecurity in Islamic banks, with a case study on Bank Syariah Indonesia. The learned aspects of this research show that AI technologies, such as machine learning and big data analytics, prove beneficial in detecting and mitigating cyber threats and thereby enhancing incident response and engendering customer trust. The research findings demonstrate that constant investment in advanced technological solutions and the formulation of digital governance policies in harmony with Shariah principles are necessary for the cybersecurity sustainability of Islamic financial institutions.

1- General Concepts of Cybersecurity and Digital Transformation :

1.1. Cybersecurity: Concept, Importance and Challenges:

Cybersecurity is undoubtedly one of the most important fields in the age of digitization; it is primarily focused upon the protection of information systems, networks, databases, and software against electronic attacks and threats aimed at stealing, manipulating or disrupting data. This definition compiled the following assertions provided by the internal working group of the International Organization for Standardization (ISO/IEC 27032) stating that its objectives include processes and practices set up to secure the confidentiality, integrity, and availability of data in cyberspace. On the other hand, the definition provided by the U.S. National Institute of Standards and Technology (NIST) refers because such ability is concerned with "protecting and recovering electronic information and services from cyber intrusion while ensuring the continuity of those services." Based on these definitions, cybersecurity represents both the shield and the cornerstone for the stability of the digital infrastructures across all sectors.

This area subdivided into several key areas, such as network security. These include application security to deal with the vulnerabilities of software and data security which ensures confidentiality and protection against manipulation or leakage. Cybersecurity plays an important role due to global changes brought about by the digital revolution, which made data the most valuable assets today as it is often called as "new gold." Rapid improvement concerning the use of technology for the

⁴ Hamel, Dalila. (2025), « The Role of Artificial Intelligence in Enhancing Cybersecurity in Islamic Banks – Case Study of Bank Syariah Indonesia », Journal of Economic, Management, and Commercial Sciences, University of M'sila, Vol. 18, N°1.

functioning of affairs of persons, institutions, and states reminds that the protection of this strategic resource becomes urgent.

Types of cyber-attacks include viruses, malware, and phishing with various effects from data loss, identity theft, and disruption of systems. These types of risks are controlled using a plethora of technical measures such as firewalls, encryption, and regular updating of software, as individuals would do things like keep strong individual passwords and avoid dubious attachments. Cyber threats against critical infrastructure-such as electricity, water, and airport systems-fall under the worst-modern threats known as "cyber wars" because of their ability to paralyze sectors deemed essential to the economy. To this end, the government is working to develop these holistic national cybersecurity strategies and improve cooperation on an international level, which is also needed to guarantee stability at the economic, social, and sovereign level⁵.

1.2. Digital Transformation in Islamic Banks:

Digital transformation in Islamic banks is the whole new approach and process which includes the adoption and integration of the modern digital technology enabling banks to get into strong communication networks and internet-based applications or intelligent systems that allow working towards the achievement of institutional objectives while enabling effective service provision. This new technology enabled banking transactions to be executed remotely, much faster and more secure, and at lower costs for customers availing themselves of accounts to execute financial operations without having to visit the branch physically. In addition, it further expands the client base by reaching out to those underserved groups, especially in rural areas, bringing into line with the scalability and flexibility of the digital services⁶.

Hence, the importance of digital transformation is even much higher, as it would have been an effort on the bank's part to comply with the very fast emerging global technological change scenario and enhanced financial inclusion achieved through offering a variety of payment and settlement options in accordance with the needs of different clients' targets. There is, therefore, distinct Sharia-sourced characteristics regarding the banking transformation in digital Islamic institutions, as all digital solutions must be in consonance with Islamic law. This is to make products and services comply with the prohibitions against interest (riba) and illicit speculation while promoting transparency and fairness in transactions. Hence, clients get a more robust assurance that Islamic digital banking is a safe and ethical alternative balancing technological innovation with religious values⁷.

1.3. Digitalization and Cybersecurity in Banking:

Digital transformation and cybersecurity are complementary and inseparable in the banking system. It is therefore not surprising that as innovations like online banking, mobile applications, and artificial intelligence are adopted-hence opening huge opportunities for delivering faster and efficient services at lower costs-it also exposes

⁵Al-Hawi. (2025), «Cybersecurity: Concept and Dimensions », <http://https://22ale3lami.net> (28/08/2025).

⁶Shoushan, Khadija, Bououina, Hamou. (2023), « The Role of Digital Transformation in Improving the Services of Algerian Islamic Banks – Case Study of Al Salam Bank » , Journal of Social Protection Research, vol. 4, N°1, p.99.

⁷Amany, Fawzi. (2021), « The Role of Digital Transformation in the Banking Sector in Light of the COVID-19 Pandemic – A Field Study », National Criminal Journal, vol. 64, N°2.

increasing risk to the institutions for potential attacks and breaches through cyberspace. For this reason, cybersecurity becomes the first line of defense in ensuring continuity in digital transformation while protecting sensitive financial data and customer information.

Digital transformation becomes a risk as the opportunities for growth become threats in the absence of well-developed cybersecurity systems, with customer confidence being undermined in the meantime, eroding trust people had in banking through electronic services. The integration of the two, however, ensures there is an optimally balanced state whereby extra innovation and agility are brought about by digital transformation while cybersecurity channels security and trust. The future success of the banking sector, therefore, in the digital age will rely on the ability to combine technological expansion and strict adaptive security strategy, matching the risks that develop⁸.

2- Cybersecurity in Islamic Banking:

2.1. Cybersecurity in Islamic Banks: Historical Facts Definition:

Cybersecurity in Islamic banks comprises a set of varied measures with technologies and policies to protect the digital systems, databases, and electronic financial transactions from threats due to cyber hacking, malware, data manipulation, and electronic fraud. The additional dimension comprises an aspect of distinguishing cyber security: not just confidentiality, integrity, and availability of data as in conventional banks, but compliance with the regulations in Sharia with respect to Islamic financial transactions⁹.

2.2. Security Challenges and Cyber Risks Facing Islamic Banks:

Since Islam banks were joined among the conventional banks, like conventional banks, Islamic banks do face a varied range of possible cyber risks emerging owing to the rapid advancement of information and communication technologies. Their Sharia-based aspect does create distinct sensitivity to these risks because any breach in security would not only affect the financial and technical dimensions but also that

⁸Alaa Ahmad Shahada Khalifa, Adnan Abdullah Mohammed Oweidah. (2024), « The Role of Digital Transformation in Enhancing Cybersecurity of Islamic Financial Institutions in Palestine – An Analytical Study », Middle East Journal for Scientific Publishing, vol. 7, n°2, p. 1-19.

⁹Ali Ibrahim Dawood Jaber. (2025), « Assessing the Effectiveness of Cybersecurity Solutions in Islamic Banks to Reduce Financial Risks », Our Islamic Economy Journal, vol. 7, Jordan, May 29.

of the customers' trust and the institution's religious credibility. Increasingly diverse threats:

- cyber threats among others comprise malware, ransomware, and distributed denial-of-service (DDoS)-systems-disabling or stealing financial data via control or extorting banks.
- Fraud and phishing: familiar threats to clients deceptively being lead through false emails or links to lost log credentials and sully their names.
- Poor technical setup: many Islamic banks mostly use antiquated systems, exposing them to newfound threats, particularly within emerging markets.
- Skilled human resource gaps: the absence of cybersecurity professionals limits banks in their success in managing cyber incidents.
- Insider threat: onto internal risks, this refers to an action in most cases by a negligent or purposeful misuse of access rights by employees.
- Reconciling Sharia: balancing Sharia compliance against security-ensuring breaches do not introduce prohibited elements (i.e. riba or gharar) into financial contracts.
- Fraud in identity theft: allowing unauthorized people to alter transactions by manipulating financial transactions.
- Weaknesses in digital banking services: card skimming and weakly secured mobile applications, for example.
- Inconsistent and poor legal frameworks: cross-border operations endow an entirely different legal environment for banks, part of which lacks strong anti-cybercrime legislation.
- Reputational risks and cyber extortion: being of ethical and religious foundations, a breach in Islamic banks can draw disproportionate damage relative to other financial institutions.

2.3. Effects on Consumer Confidence and Financial Stability¹⁰:

- Consumer Confidence:
 - Decrease in intelligence that results from security breaches or fraud.
 - Reduced incidence of adoption of digital services following phishing or fraud events.
 - Reputational damage, particularly, as mentioned, holds true for banks built on ethical and religious principles.
- Financial Stability:
 - Increased operation costs from investments made to improve security infrastructure and compensations made for affected clients.
 - Increasing systemic risks if several Islamic banks in a country or region are attacked simultaneously.
 - Reduced competitiveness as compared to technologically advanced financial institutions, including FinTech.
 - Decreased investor as well as regulatory confidence, which might lead to fines or investments being withdrawn.
 - Business continuity risks from severe attacks such as those created by ransomware or DDoS.

3- Strategies for Improving Cybersecurity in the Islamic Banks of Algeria:

The worldwide banking sector, including Algeria's Islamic banks, is rapidly moving towards digitalization and electronic financial services. However, as the transformation changes on how banks operate, it tends to open areas of improvement for overall bank performance, quality service, and financial inclusion. On the other hand, this transformation is coupled with unprecedented threats in the form of cyber risks, which have made banking stability and customer trust face new challenges. For instance, in Algeria, the importance of cybersecurity for Islamic banks lies in their simultaneous need to comply with Sharia as well as to gain the customer's trust in a financial environment that is still adapting to the digitalization of services, hence raising the important issue of what strategies could enhance digital protection for Islamic banks so as to safeguard customer data, ensure service continuity, and compliance with Sharia and regulatory standards, strengthening financial stability, and increasing positions in the national financial system.

3.1. Sharia and Legal Frameworks for Securing Digital Transactions:

- General framework Sharia prohibits riba, fraud, and illicit practices; demands transparency and justice; and obliges the banks to guard their clients' funds and data as a religious trust. Sharia supervisory boards monitor compliance regularly with regard to banking transactions irrespective of whether they are done digitally or not.
- Legal frameworks (Algeria): The provisions of the new Algerian law on cybercrime (2018), regulations applicable to data protection from 2022, and banking regulations established by the Bank of Algeria.
- International standards: for example, PCI DSS, ISO/IEC 27001, and the Islamic Financial Services Board (IFSB).

These Sharia-based principles and laws provide a strong foundation for protecting digital transactions within an Algerian Islamic bank.

3.2. Role of Artificial Intelligence (AI) and Blockchain in Bruising Cybersecurity Improvement:

The applications of artificial intelligence are a useful tool in improving aspects of cybersecurity for Islamic banks, as they indicate forthcoming threats to

address them efficiently through the compliance of Shari'ah standards. This is realized via¹¹:

- Automatic threat identification: through deep learning techniques in profiling network behavior to identify abnormal activities.
- Incident reaction systems: accomplishments in automating a response to cyber attack, thus reducing interaction time with threats.
- Big data analytics: intelligence through the processing of very large amounts of data to determine patterns that signal attempts at intrusion.
- Predictive ability on attacks: using machine learning to create predictive models about future attacks to predict limitations before exploitation.
- Real-time fraud detection: financial transaction monitoring that seeks fast identification of suspicious acts, all in accordance with Shari'ah provisions.
- Improvement in encryption and secured protection: making possible dynamic encryption algorithms to adjust to the evolution of cyber threats.

Undoubtedly, blockchain technology has gained notoriety as one of the most striking contemporary technologies that can contribute to raising the scales of security and transparency in digital transactions of Islamic banks in light of growing cyber challenges. The technology relies on an entirely decentralized distributed system which makes sure that data cannot be changed and puts a very high level of trust among the parties that involved. The role of the blockchain can be seen in the following points:

- Guaranteeing the integrity and transparency: all financial transactions are recorded in unchangeable strings of blocks meaning there are reduced chances of manipulating or defrauding a customer with increased customers' trust.
- Protecting the digital transactions: through the characteristic of the advanced encryption facility that characterizes the block-chain system, confidentiality of the financial data is preserved from intrusion attempted.
- Reducing third-party risks: the necessity of having traditional intermediaries in most transactions is eliminated, lessening any possibility of security vulnerabilities associated with intermediation.
- Complies with Sharia regulations: a reliable mechanism for documenting smart contracts as compliant with Islamic law, especially on finance with respect to investments.
- Detection of suspicious activities: entirely transparent transactional history provided by the blockchain makes it possible to track the transactions path and easy to identify deviations that may be connected to financial crime or laundering.
- Further Fine-tuning of Financial Stability: in reducing the possibility of manipulation and fraud, it strengthens resilience in the financial architecture of Islamic banks and, thus, overall financial stability.

3.3. Best Practices and International Experiences in Cybersecurity

International experiences have shown that establishing a strong cybersecurity regime requires an approach covering all layers and fronts, extending not only

¹¹ Hamel, Dalila. (2025), « The Role of Artificial Intelligence in Enhancing Cybersecurity in Islamic Banks – Case Study of Bank Shariah Indonesia », Op.cit, p.88.

to the technical dimension but also to the legislative and regulatory frameworks, development of human competencies, and the culture of digital awareness. Some of the pioneering countries, such as Estonia, Singapore, and the European Union, have formulated national cybersecurity strategies that focus on protecting their critical financial infrastructures, promoting investment in advanced technologies such as AI and blockchain, and bolstering their legal frameworks with the likes of the European General Data Protection Regulation (GDPR). Such experiences, too, have highlighted the necessity for international cooperation and information-sharing concerning cyber threats integrated within the risk management matrix of corporate governance frameworks.

Even though Islamic banks face their own challenges when it comes to reconciling modern banking practices with Sharia compliance, several leading Islamic finance countries have begun to adopt state-of-the-art cybersecurity frameworks that Algeria can draw on.

- ✚ **Malaysia:** Malaysia represents a major model in Islamic banking and cybersecurity. The Central Bank of Malaysia has drawn out an integrated framework that combines Sharia with technology governance. Given that Bank Islam Malaysia has implemented blockchain technology to secure smart contracts, such contracts would obviously be transparent.
- ✚ **Kingdom of Saudi Arabia:** Under SAMA, there are cybersecurity programs created for Islamic banks focusing on the protection of electronic payments and digital Islamic finance platforms. The experience of Al Rajhi Bank remains an excellent example of using AI in monitoring for fraudulent activity while complying with Sharia.
- ✚ **United Arab Emirates:** Policies to safeguard digital assets have been spearheaded by the Dubai Cybersecurity Center and the Dubai International Financial Centre. Such frameworks have benefited Islamic banks like Dubai Islamic Bank in developing secure blockchain-supported payment systems ensuring transparency and fostering customer trust.
- ✚ **Bahrain:** A regional hub for Islamic finance, Bahrain has adopted an integrated approach through the Central Bank of Bahrain, which mandates all Islamic financial institutions to implement the Cybersecurity Framework for Islamic Banks, coupled with specialized training programs to bolster employee awareness.
- ✚ **Pakistan:** The State Bank of Pakistan is working on a digital transformation plan for Islamic banks; this plan imposes strict cybersecurity policies to ensure promotion of online Islamic financial services while enhancing the oversight on data protection and compliance with Sharia.

These experiences show that best practices in cybersecurity pivot around three main axes: first, existence of stringent and transparent legislative and regulatory functions; second, investment in advanced technologies that can anticipate and efficiently address threats; third and the last, consolidation of a culture of cybersecurity awareness at both institutional and individual levels. The success of Islamic banks in confronting digital challenges will depend on their blending

of these global practices with Sharia precepts to reinforce customer trust and financial stability.

3.4. Suggestions to Reinforce Cybersecurity in Algerian Islamic Banks

An investigation of some of the most adopted best practices and international experiences in the cybersecurity field permits getting practical lessons for Islamic banks in Algeria which could then help better confront digital threats. These lessons include the following:

- An integrated legislative and regulatory framework taking into account the particularities of Islamic banking should be developed, similar to Malaysia and Bahrain, to firm trust and ensure Sharia and legal compliance.
- NBS adopted national cybersecurity strategies in the banking sector, focused on protecting the critical infrastructure of financial systems while actively involving Islamic banks in the development of these policies.
- Investing in advanced technologies such as artificial intelligence and blockchain to enhance the early threat-detection capability, ensure transparency in financial operations, and develop Sharia-compliant smart contracts.
- Creating a culture of cybersecurity awareness among staff and customers through continuous training and awareness campaigns, given that the human factor usually constitutes the weakest link.
- Become a player in international and regional cooperation networks for exchanging intelligence and expertise on cyber threats and attacks while getting the share of technical and knowledge-based support from the international organizations.
- Integrating cyber risk management into a corporate governance framework would mean that it becomes a component of long-term strategies in ensuring sustainable financial stability.

Thus, with lessons from the above, Algerian Islamic banks can consistently improve and redefine their positioning in a rapidly transforming global financial environment, enabling them to face future challenges with greater efficiency and flexibility, thus maintaining their Sharia-compliant identity.

Conclusion:

Digital transformation in Islamic banks, despite its wide opportunities and advantages in improving operational efficiency, reducing transaction costs, and broadening the range of financial services, brings complex and very serious cybersecurity challenges injurious to the confidentiality of financial data, client privacy, and integrity of transactions. Such challenges are very technical-oriented, but in the wider scheme, they impinge on institutional stability and customer trust—both of which are very important for the credibility of Islamic banking. Cybersecurity therefore assumes a different dimension because it is not only compliance with technical and legal requirements but also complying with Shariah principles in Islamic financial practices and highlights the dilemma of having to balance modernization through digitization while maintaining that religious and ethical identity.

Thus, the Algerian Islamic banks' prospective success in catching up with the rapid pace of digitization depends on adopting integrated multidimensional strategies combining strengthening legislative and regulatory frameworks with Shariah compliance and investing in modern high-end technologies including artificial

intelligence and blockchain while building human capital through developing specialized competencies. Only through such an overall approach can Islamic banks build a resilient cybersecurity system capable of ensuring safekeeping of digital transactions apart from promoting client trust and enhancing their competitive position in an increasingly globalized and technologically dynamic financial environment.

The findings from the research may be summarized as follows:

- ✓ The cyber security forms the backbone pillar for ensuring, henceforth, the stability of Islamic banks and confidence from clients under conditions that are digitally transformative.
- ✓ Islamic banks are very exposed to a wider variety of risks that runs from cyber intrusions, financial fraud, digital identity theft, and to direct attacks on the technological infrastructures.
- ✓ The absence of specialized legislative and regulatory frameworks in cybersecurity for Algeria is one of the key hindrances in developing a complete and efficient protection system.
- ✓ A growing dependence on digital technologies, combined with a lack of awareness among employees and customers, creates serious vulnerabilities that pave the way for extreme cyber threats.
- ✓ International experiences, particularly Malaysia and the United Arab Emirates, show that coupling advanced technologies such as artificial intelligence and blockchain with a well-designed legal and Shariah-compliant framework creates a higher level of safety and trust.

From these findings, the following recommendations will arise:

- Creating a national comprehensive legal framework on cybersecurity that is particularly aligned with the specificities of Islamic banking and is Shariah-compliant in addition to being administratively strict.
- Cyber risk management will become incorporated in corporate governance systems and internal control mechanisms of Islamic banks so that it becomes part of long-term strategic planning.
- Invest more in advanced technologies including artificial intelligence and blockchain to secure transactions, improve transparency, and make smart contracts compliant with Islamic finance.
- Enhancing continuous awareness raising and training programs directed at employees as well as customers because the human element often represents the weakest link in cybersecurity.

References :

- 1- Shoushan, Khadija, Bououina, Hamou. (2023), « The Role of Digital Transformation in Improving the Services of Algerian Islamic Banks – Case Study of Al Salam Bank », Journal of Social Protection Research, vol. 4, N°1.
- 2- Amany, Fawzi. (2021), « The Role of Digital Transformation in the Banking Sector in Light of the COVID-19 Pandemic – A Field Study », National Criminal Journal, vol. 64, N°2.
- 3- Alaa Ahmad Shahada Khalifa, Adnan Abdullah Mohammed Oweid,ah. (2024), « The Role of Digital Transformation in Enhancing Cybersecurity of Islamic Financial Institutions in Palestine – An Analytical Study », Middle East Journal for Scientific Publishing, vol. 7, n°2.
- 4- Ali Ibrahim Dawood Jaber. (2025), « Assessing the Effectiveness of Cybersecurity Solutions in Islamic Banks to Reduce Financial Risks », Our Islamic Economy Journal, vol. 7, Jordan, May 29.
- 5- Hamel, Dalila. (2025), « The Role of Artificial Intelligence in Enhancing Cybersecurity in Islamic Banks – Case Study of Bank Syariah Indonesia », Journal of Economic, Management, and Commercial Sciences, University of M'sila, Vol. 18, No. 01.
- 6- Hassan, Ibrahim. (2021), Cybersecurity Risk Analysis in Islamic Banks: Challenges and Solutions, 1st Edition, Dar Al-Uloom Publishing House.
- 7- Bara, Samir. (2017), « Cybersecurity in Algeria: Policies and Institutions », Algerian Journal of Human Security, vol. 4, July 2017.
- 8- Al-Hawi. (2025), « Cybersecurity: Concept and Dimensions », <http://https://22ale3lami.net> (28/08/2025).