



The Role of AI and Big Data in Detecting Illegal Finance, Sharia Violations, and Cybercrime in the Digital Society Era Society 5.0

Tuti' Nadhifah  , Heni Risnawati ,
Dian Rosita 

Faculty of Economics, Education and Law, Universitas Muhammadiyah Kudus, Kudus,
Indonesia

 Corresponding email: tutinadhifah@umkudus.ac.id

Abstract

Technological developments in the Society 5.0 era have driven massive digital transformation in various sectors, including in the financial system and law enforcement. In this context, artificial intelligence (AI) and Big Data have a strategic role in detecting illegal financial activities, violations of sharia principles in transactions, and increasingly complex cybercrime. This article discusses how AI and Big Data are used as real-time detection and prevention tools for transaction anomalies, money laundering patterns, and online fraud practices. In addition, this study highlights the regulatory and ethical challenges in the application of this technology, especially in ensuring compliance with sharia principles and personal data protection. With a normative qualitative method

and a multidisciplinary approach, this paper offers a legal and technological perspective in responding to the dynamics of digital crime and the importance of collaboration between regulators, financial institutions, and technology providers to create a safe and equitable digital ecosystem. The findings in this article are expected to be strategic input in formulating legal policies and strengthening technology-based supervision systems in the digital era.

KEYWORDS *Artificial Intelligence; Big Data; illegal finance; Sharia violations; Cybercrime.*

Introduction

The rapid development of digital technology accompanied by the widespread use of social media and online platforms as a means of social and economic interaction has significantly transformed the way people conduct business activities, transact and manage financial information. This change not only has an impact on accounting practices and financial reporting which are now increasingly digitalized but also poses new challenges in the application of sharia economic principles that demand clarity, fairness and compliance with Islamic ethical values. On the other hand, this new reality also expands the scope of legal regulations, especially in the field of cyber law. The complexity of legal protection for digital activities is increasingly in the spotlight along with the increasing risk of personal data breaches and the development of financial crimes operating in cyberspace.

The development towards the Society 5.0 Era describes a new phase in the structure of Society which is marked by the high use of Information Technology in everyday life. This era is a continuation of the industrial revolution 4.0 which previously revolutionized the way humans do activities and work through the application of digital technology, automation, and artificial intelligence in various sectors¹. In this context, society is no longer just a user of technology but also part of a complex digital ecosystem.

One of the phenomena that attracts attention is how social media is not only a means of communication but also a fertile ground for various illegal

¹ Luluk Setyowati and Deni Nasir Ahmad, "Pemanfaatan Big Data Dalam Era Teknologi 5.0," *Jurnal Pengabdian Kepada Masyarakat* 1, no. 2 (December 2021): Hal.117-122.

financial activities, including illegal investment-based fraud to money laundering practices packaged in online business models. In addition, the emergence of technology-based financial services (fintech) with claims based on sharia has also become a spotlight, especially when practices are found that are contrary to the principles of fiqh muamalah such as gharar, hidden usury and tadlis in digital transactions². Furthermore, digital platforms are increasingly being used as a tool to disguise cybercrime, both organized and individual. Social manipulation techniques such as phishing, scamming and misuse of personal data are frequently used. The complexity of these problems not only shows the high threat to legal and economic aspects but also indicates the inability of conventional detection systems to combat digital crime.

In response to the challenges arising from these developments, various initiatives have been directed at utilizing Artificial Intelligence (AI) technology and Big Data analytics which are effectively used to track suspicious patterns, identify unusual digital behavior³, and develop early indicators that point to potential violations of law and ethical principles in the digital realm⁴. Previous studies have shown how machine learning techniques can be trained to recognize signs of financial manipulation through uploaded text, comments and other digital interactions⁵. Natural Language Processing (NLP) digunakan untuk memahami narasi penipuan yang tersembunyi dalam bentuk testimoni palsu, ajakan investasi fiktif, atau konten promosi yang mengarahkan ke skema ponzi⁶. Efforts to enforce sharia principles in the digital realm have also encouraged the development of technology-based approaches designed to detect and filter content and transactions that potentially contain elements of usury, gharar, or practices that are not in accordance with the rules of muamalah fiqh. One of the approaches currently developing is the use of an automatic classification system supported by a deep learning algorithm, in order to increase

² Muhammad Ayub, *Understanding Islamic Finance* (Jakarta: Gramedia Pustaka Utama, 2013).

³ Hsinchun Chen, Roger H. L. Chiang, and Veda C. Storey, "Business Intelligence and Analytics: From Big Data to Big Impact," *MIS Quarterly* 36, no. 4 (December 2012): 1165–88.

⁴ Dara Sawitri, "Artificial Intelligence for a Digital Technology Smart Society in the Era of Society 5.0," *Journal of Artificial Intelligence and Software Engineering* 5, no. 1 (March 2025): 135–43.

⁵ Sindu Prasetyo and Totok Dewayanto, "Penerapan Machine Learning, Deep Learning, Dan Data Mining Dalam Deteksi Kecurangan Laporan Keuangan - A Systematic Literature Review," *DIPONEGORO JOURNAL OF ACCOUNTING* 13, no. 3 (2024): 1–12.

⁶ Dewati Sallma Syahtri, "Peran Natural Language Processing (NLP) Untuk Mendeteksi Penipuan Dalam Dokumen Keuangan," <https://Accounting.Binus.Ac.Id/2024/12/06/Peran-Natural-Language-Processing-Nlp-Untuk-Mendeteksi-Penipuan-Dalam-Dokumen-Kuangan/>, June 2024.

the accuracy of identifying sharia non-compliance in the digital financial⁷. On the other hand, efforts to detect cybercrime through social media rely heavily on social network analysis, which is designed to reveal relationships between suspicious accounts by examining accounts suspected of carrying out illegal activities, by tracing digital interaction traces and content distribution patterns as part of constructing legally valid electronic evidence⁸.

In the context of legal evidence, data and AI analysis results used to detect cybercrime must comply with the principles of electronic evidence validity as stipulated in the ITE Law. Electronic evidence generated through AI systems must be able to guarantee data integrity and authenticate information sources to be admissible in court. Without guarantees regarding the validity and security of the data processing process, the validity of AI analysis results could potentially be questioned in court.

Although various achievements show significant progress in the application of AI and Big Data to monitor activities in the digital realm, there are still a number of methodological and conceptual issues that have not been fully resolved. Many studies focus solely on technical aspects, thus failing to consider essential normative dimensions, such as the applicable legal framework, ethical values based on local wisdom, and principles of compliance with sharia that vary from one national legal system to another.

The absence of integration between technological approaches with the legal basis and principles of sharia creates a gap in the development of a digital detection system that is not only technically effective but also normatively valid. Therefore, an analytical model is needed that is able to combine the ability to automatically process data through AI and Big Data with sensitivity to national legal norms, the principles of *maqāsid al-sharī‘ah*, and local digital ethics. This idea offers a multidisciplinary approach that combines algorithmic logic with a normative framework, which can be used as a basis for designing a digital activity monitoring system that is not only sophisticated, but also legally valid and in accordance with sharia principles. This approach is expected to provide a solution to the challenges of regulatory fragmentation and diverse interpretations of norms in the digital world.

⁷ Kirti Ranjan Swain and Subhasmita Mallick, “Artificial Intelligence in Finance: Challenges and Opportunities,” *Scope* 13, no. 2 (June 2023).

⁸ Julián Ramírez Sánchez et al., “Uncovering Cybercrimes in Social Media through Natural Language Processing,” *Complexity* 2021 (2021), doi:10.1155/2021/7955637.

The purpose of this paper is to formulate a conceptual framework that bridges the sophistication of digital surveillance technology with legal norms and sharia principles, through a critical review of previous literature and exploration of possible interdisciplinary integration approaches. In order to answer the question of how the Role of AI and Big Data in analyzing and detecting illegal financial activities on digital platforms and social media and what are the challenges and limitations of using AI and Big Data in supporting compliance with big data agreements, this study will use a qualitative method with a normative and conceptualization approach, accompanied by a critical analysis of the results of previous studies and secondary data from testing and digital sharia finance literature.

Method

This study uses the approach method or commonly known as qualitative descriptive. Qualitative research aims to understand holistically (completely) what is experienced by the subject of the study by describing data using words and using various natural methods⁹. In a study, data is a very important element because the quality of the study is highly dependent on the data. The data sources in this study were taken through literature studies with conceptual review techniques, namely methods for collecting data that are in accordance with the research context sourced from literature library materials, books, previous studies and others. Conceptual review can provide an understanding of an issue through the conceptual coverage process. This study collects various academic literature relevant to AI (artificial intelligence), big data, Illegal Finance, Sharia Violations, Cybercrime and Society 5.0.

The data collection process was carried out through a literature search using the keywords Artificial Intelligence (AI), Big Data, illegal finance, sharia violations, cybercrime, and Society 5.0. Library source searches were conducted through various academic platforms, including Google Scholar, Mendeley, and Publish or Perish. The literature used in this research prioritizes sources that are openly accessible and relevant to the research focus. The process of searching and collecting literature was carried out systematically during the research period.

⁹ Lexy. J. Moleong, *Metodologi Penelitian Kualitatif* (Bandung: PT Remaja Rosdakarya, 2000).

Furthermore, the literature obtained was selected based on certain inclusion criteria, namely literature that discusses the Unified Theory of Acceptance and Use of Technology 2 (UTAUT 2), Artificial Intelligence (AI), Big Data, sharia compliance theory, cybercrime, and the concept of Society 5.0. Then, Literature that meets these criteria is critically analyzed to identify concepts, theories, and findings that are relevant to the research objectives. The analysis was conducted by comparing various views and previous research results to gain a more comprehensive understanding of the use of AI and Big Data in supporting the detection and monitoring of digital activities that have the potential to violate the law or sharia principles.

To maintain the quality and validity of the research, each literature source is reviewed repeatedly to ensure its suitability, relevance and credibility to the topic being researched. The analysis results are then compiled systematically and descriptively to produce a conceptual framework that is able to explain the role of AI and Big Data in detecting illegal finance, sharia violations, and cybercrime, as well as identifying various challenges and limitations of its implementation in supporting regulatory compliance in the digital era of Society 5.0.¹⁰

Result & Discussion

A. The Role of AI in Analyzing and Detecting Illegal Financial Activities, Sharia Violations and Cybercrime in the Digital Era Society 5.0

Artificial Intelligence or AI is a technology designed to make computer systems capable of imitating and thinking like humans¹¹ This is also often used in fraud detection systems using machine learning and deep learning algorithms¹². The use of AI is capable of identifying suspicious transaction patterns in real time using machine learning and deep learning. Then the use

¹⁰ Muhammad Fahli Saputra and Aji Prasetya Wibawa, "Peran Dan Tantangan Cyber Security Di Era Society 5.0," *Jurnal Inovasi Teknik Dan Edukasi Teknologi* 2, no. 7 (n.d.): 349–54, doi:10.17977/um068v1i72022p349-354.

¹¹ Febryan Alam Susatyo and Dian Rosita, "Relevansi Pertanggungjawaban Pidana Atas Culpability Kecerdasan Buatan (Artificial Intelligence)," *Literasi Hukum* 8, no. 2 (2024): 59–68.

¹² Farah Labibah Caseba and Totok Dewayanto, "Penerapan Artificial Intelligence, Big Data, Dan Blockchain Dalam Fintech Payment Terhadap Risiko Penipuan Komputer (Computer Fraud Risk): A Systematic Literature Review," *Diponegoro Journal of Accounting* 13, no. 3 (July 2024).

of systems such as fraud detection engines in financial institutions will be able to prevent money laundering. Artificial Intelligence is considered to have high accuracy in detecting fraud in business. The level of use of artificial intelligence to detect fraud in companies reaches 91-92%. This indicates that artificial intelligence will be safer than using other methods. Even AI can also help auditors in particular to be able to issue an opinion

Artificial intelligence (AI) can analyze thousands of transactions in seconds to detect fictitious transactions, identity fraud and the use of fake accounts. Large banks and fintechs use real-time fraud detection systems powered by AI. The use of AI can help relationships between accounts, companies and individuals in uncovering illegal finances. AI is also very useful in uncovering terrorism funding schemes and criminal syndicates. AI can be a continuous update of the fraud detection model, so that it can deal with various fraud methods that are increasingly developing. The effectiveness of fraud detection using AI using a logistic regression model provides a high accuracy of 95%, meaning that all transactions can be classified correctly. This model has high precision for legitimate transactions (96%) and fraud (83%). However, this model has a fairly low recall for fraud (43%), seeing this situation, an evaluation can be carried out to improve the detection of all fraudulent transactions¹³.

The application of AI is an innovation in reducing financial risk that can increase operational efficiency by processing and analyzing data quickly. AI can also facilitate better decision-making for financial risk management. This can optimize financial performance and reduce losses. An example of the application of AI in finance is credit scoring where AI can analyze financial data and customer behavior to determine creditworthiness and appropriate interest rates. AI can also predict the possibility of default and take preventive action. Then there is fraud detection, AI that can detect fraud or irregularities in financial data using techniques such as pattern analysis and provide warnings or block suspicious transactions. For regulatory compliance, AI can help in meeting applicable regulations in anti-money laundering and automate the verification process¹⁴.

¹³ M. Rafie Akbar, Kgs M. Syarif Hidayatullah, and Tata Sutabri, "Evaluasi Efektivitas Sistem Deteksi Penipuan Berbasis Ai Menggunakan Metode Regresi Logistik Untuk Meningkatkan Keamanan Transaksi Pada Startup Finance," *J-ENSITEC* 10, no. 2 (2024): 10107–11.

¹⁴ Nurul Ilahi and I Nyoman Budiono, "Penerapan Artificial Intelligence Sebagai Inovasi Di Era Disrupsi Dalam Mengurangi Resiko Keuangan," *MONETA: Jurnal Manajemen Dan Keuangan Syariah* 3, no. 1 (2024).

The relevance of Artificial Intelligence (AI) and Machine Learning (ML) in combating illicit financial activity is increasingly evident in today's financial and technology reports. Implementing advanced AI and ML systems demonstrates a strong commitment to security and transparency, which can increase customer trust and strengthen an institution's reputation. As financial crimes become more sophisticated and regulatory pressures increase, the role of AI and ML in ensuring financial security is more important than ever. These technologies provide sophisticated, efficient, and practical solutions to detect and prevent financial crimes, making them an indispensable tool for financial institutions around the world. For an auditor, the implementation of AI in detecting fraud in financial reports has provided many benefits. With AI's ability to analyze data on a large scale, detect patterns and anomalies, and provide early warnings, AI has proven to be a very valuable tool in improving audit effectiveness. This technology not only helps auditors detect fraud more quickly and accurately, but also improves the reliability and integrity of financial reports. However, the implementation of AI requires special attention to challenges such as data security and a lack of understanding of how AI works. The success of AI integration in auditing depends on how audit firms are able to overcome these challenges, while ensuring that the role of humans in the audit process remains valuable and is not completely replaced by technology.

The use of AI is not only in conventional finance, but also in Sharia-based finance. The convergence of AI and Islamic finance presents an opportunity to leverage technology while remaining aligned with Islamic principles. The use of AI technologies such as Natural Language Processing (NLP) and predictive analytics can improve Sharia compliance by automating key tasks. NLP can be used to analyze financial documents and contracts to detect non-compliance with Sharia principles, such as the presence of Riba (usurious interest) or Gharar (excessive uncertainty). This automation ensures that contracts are in line with Islamic teachings by flagging potentially prohibited elements in real time¹⁵.

The use of AI in sharia-based financial markets must take into account the importance of compliance with sharia principles such as the prohibition of usury, gharar, and maysir, as well as how Artificial Intelligence (AI) can

¹⁵ Hebah Shalhoob and Iman Babiker, "Exploration of AI in Ensuring Sharia Compliance in IF Institutions: Focus on Accounting Practices," *Open Journal of Business and Management* 13, no. 2 (2025).

improve sharia compliance in Islamic finance by increasing the accuracy, efficiency, and consistency of monitoring and auditing processes. This will require solutions on how the use of AI can help strengthen sharia compliance through machine learning-based contract analysis and detection of transactions that are not in accordance with sharia principles¹⁶.

The use of AI to detect cyber attacks enables faster automated responses, reduces response times, and minimizes the impact of attacks on a business. Modern technologies such as behavioral analysis, machine learning, and anomaly detection are becoming increasingly important for early detection of complex and unpredictable attacks. In addition, ongoing security education and awareness among all stakeholders is needed to improve response and reduce the success of attacks¹⁷. AI, especially through Machine Learning algorithms, can significantly increase the effectiveness of network security threat detection and mitigation. However, the implementation of this technology requires a careful approach to overcome challenges such as false positives and the need for robust infrastructure.

In addition to its role in detecting and mitigating network security threats, the advancement of AI technology has driven improvements in digital security, particularly in the detection of image manipulation. This technology enables photographers and content creators to automatically verify the authenticity of images before they are used or shared. Several image editing software programs, such as Adobe Photoshop and GIMP, have integrated AI features capable of accurately detecting traces of visual tampering. Additionally, the emergence of cloud-based systems allows creative professionals across various regions to access these detection tools more widely. This technological development not only enhances the protection of visual content but also strengthens the legal position of content owners by providing proof of authenticity that supports the protection of Intellectual Property Rights (IPR) in cases of infringement or misuse¹⁸.

¹⁶ Elman Nafidzi and Khabib Musthofa, "Peluang, Strategi, Dan Tantangan Industri Perbankan Syariah Dalam Menghadapi Artificial Intelligence (AI)," *Journal of International Multidisciplinary Research* 3, no. 2 (2025): 68–76.

¹⁷ Muhammad Habib Rifai, Dimas Akbar Pramudya, and Rohmad Rafi Narfandi, "Analisis Peran Teknologi Kecerdasan Buatan Dalam Mengoptimalkan Proses Deteksi Terhadap Serangan Siber," *Semin. Nas. Teknol. Inf. Dan Bisnis* 18, no. 6 (2024): 495–502.

¹⁸ Dian Rosita et al., "Analysis of Legal Protection of Intellectual Property Rights from a Criminal Law Perspective," *Jurnal USM Law Review (JULR)* 8, no. 2 (2025): 609–21.

The success of AI implementation is highly dependent on user acceptance, and this is related to the Unified Theory of Acceptance and Use of Technology theory as an appropriate analytical tool in understanding the factors influencing AI adoption, especially in the financial, legal and government institutions. The higher the benefits felt, the greater the acceptance of the use of technology.

B. The Role of Big Data in Analyzing and Detecting Illegal Financial Activities, Sharia Violations and Cybercrime in the Digital Society Era Society 5.0

Big data is a collection of very large and complex data where the data has certain characteristics. Caseba in his research also added that big data is the process of collecting, processing and analyzing big data in order to gain insights that can be used in decision making¹⁹.

There are 4 (four) characteristics of big data, namely the first volume (big data), second Velocity (speed), third Variety (type of data) and the last Varacity (data quality). Therefore, big data here refers to data that is very large, varied and moves at high speed cannot be processed by traditional systems²⁰. In today's digital era, the term Big Data is often used to describe technology that is able to manage and analyze various types of data, both structured and unstructured. Structured data generally consists of numbers and text that are arranged systematically, while unstructured data includes formats such as images, audio, and video that do not have a fixed pattern. In addition, Big Data can also detect fraud that usually occurs in financial transactions by recognizing patterns or anomalies or commonly called indications of crime²¹.

¹⁹ Caseba and Dewayanto, "Penerapan Artificial Intelligence, Big Data, Dan Blockchain Dalam Fintech Payment Terhadap Risiko Penipuan Komputer (Computer Fraud Risk): A Systematic Literature Review."

²⁰ Chen, Chiang, and Storey, "Business Intelligence and Analytics: From Big Data to Big Impact."

²¹ Hasri Ainun Syahfir et al., "Melampaui Batas Penglihatan Manusia: Peran AI Dalam Mendeteksi Fraud Pada Proses Audit Tinjauan Literatur Sistematis," *Jurnal Revenue: Jurnal Ilmiah Akuntansi* 5, no. 2 (2025).

Big data for fraud detection in digital transactions requires organizations to analyze large amounts of data, identifying patterns that indicate fraudulent activity. For example, money laundering, terrorism financing, double and fictitious transactions. In addition, big data can be used to take immediate action to prevent fraud²². Big data analysis relies on a variety of data sources to detect and prevent financial fraud in digital transactions. Some common data sources used for fraud detection include: Transaction logs contain detailed records of financial transactions, including transaction amounts, timestamps, and transaction IDs. By analyzing transaction logs, organizations can identify patterns and anomalies that indicate fraudulent activity, such as unusually large transactions, frequent transfers to unknown accounts, or transactions that occur outside normal business hours²³

Real-time fraud detection mechanisms allow an organization to monitor transactions as they occur, allowing the organization to detect and respond to fraudulent activity in real time. By analyzing transaction data in real time, organizations can identify patterns that indicate fraudulent activity, such as an unusual number of transactions, unexpected changes in transaction volume, or transactions originating from suspicious locations. Real-time transaction monitoring allows organizations to detect anomalies and flag suspicious activity for further investigation, thereby taking immediate action to prevent fraud. By continuously monitoring transactions in real time, organizations can identify and respond to fraudulent activity before it results in financial losses that can damage the company's reputation²⁴.

The role of big in analyzing fraud is a solution used by various organizations. Big data analysis provides the ability to reliably capture, store, analyze, and visualize very large and heterogeneous data. These analytics help develop predictive models that can drive alerts as soon as an entry point for fraudulent activity is detected²⁵. The role of big data is very relevant in today's business world because it provides benefits including: decision making, identifying business opportunities, company operational efficiency,

²² Ezekiel Onyekachukwu Udeh et al., "The Role Of Big Data In Detecting And Preventing Financial Fraud In Digital Transactions," *World Journal of Advanced Research and Reviews* 22, no. 02 (2024).

²³ Xueqi Cheng et al., "Combating Emerging Financial Risks in the Big Data Era: A Perspective Review," *Fundamental Research* 1, no. 5 (September 2021): 595–606.

²⁴ Yanjiao Dong et al., "Real-Time Fraud Detection in e-Market Using Machine Learning Algorithms," *Journal of Multiple-Valued Logic and Soft Computing* 36, nos. 1–3 (2021): 191–209.

²⁵ Hanae Abbassi, Imane El Alaoui, and Youssef Gahi, "Fraud Detection Techniques in the Big Data Era," in *Proceedings of the 2nd International Conference on Big Data, Modelling and Machine Learning (BML 2021)*, 2021, 161–70.

Personalizing Customer Satisfaction, Creating Product and Service Innovation²⁶.

The use of big data in monitoring and detecting sharia violations in the context of sharia economics and finance includes:

(a) Validation of transactions according to sharia principles: Big data can identify products or activities that contain elements of usury, gharar or maysir; (b) Monitoring the compliance of sharia financial institutions through analytical dashboards and historical data, sharia authorities can monitor deviant business practices; and (c) Analysis of customer behavior can map the need for halal and sharia-based products based on preferences and consumption patterns.

Apart from the context of Islamic economics and finance, big data is also very effective in dealing with cybercrime by collecting and analyzing data from various sources. Through real-time large-scale data processing capabilities, big data enables early detection of suspicious behavior, both from users and systems, such as logins from unusual locations, inconsistent access patterns, or sudden large fund transfers. This technology can also identify unauthorized transactions that occur on e-commerce platforms, mobile banking, and other digital systems by comparing normal transaction patterns against suspicious anomalous activity.

Furthermore, big data acts as an early warning system that helps financial institutions and cybersecurity authorities to respond to potential attacks quickly and appropriately. By integrating data from multiple sources, such as social media, financial applications, and system activity logs, big data creates an adaptive and predictive security ecosystem. This not only improves the effectiveness of preventing and controlling digital crimes, but also strengthens the digital defense system through continuously evolving machine learning.

In the era of Society 5.0, data collaboration and integration are the main keys to creating comprehensive digital security, including supporting decision-making by regulators, financial institutions, and law enforcement²⁷. Empowering digital communities is also an important part, namely by

²⁶ Gunawan Widjaja, "The Role Of Big Data Anlysis In Financial Decision Making: The Case Of Islamic Banking," *Februari* 2, no. 2 (2024): 264–76.

²⁷ Andrii Shalaginov, Jan William Johnsen, and Katrin Franke, "Cyber Crime Investigations in the Era of Big Data," in *2017 IEEE International Conference on Big Data (Big Data)* (Boston: IEEE, 2017).

providing safe, transparent and easy-to-understand information access to increase awareness and resilience towards complex cyber threats.

C. Challenges and Limitations of Using AI dan Big Data to Support Digital Financial Regulatory Compliance

The application of artificial intelligence (AI) in a corporate environment faces various challenges, especially in the context of financial audits in Indonesia. One of the main issues is the adoption gap, where small-scale companies still struggle to access affordable and relevant AI technologies. This is aggravated by the lack of comprehensive regulations and limited training programs adjusted to their necessity. In addition, the integration of AI systems into organizational structures requires significant investment, both in terms of technological infrastructure and human resource competency development. The limitations of AI in responding to dynamic and complex situations, due to its dependence on historical data, is also a barrier itself. Moreover, data security aspects are a crucial concern, considering the potential risk of leakage or misuse of sensitive information. Equally important, the resistance of some professionals to this technology, particularly in understanding and trusting the outputs generated by AI systems, indicates the need for an educational approach and sufficient time to build trust and adequate technological literacy among users.

The use of Big Data in digital financial systems has great potential in increasing the effectiveness of supervision, tracking suspicious activities, and supporting compliance with applicable regulations, including sharia principles. However, the implementation of Big Data in this sector is not free from a number of significant challenges and limitations. One of the main challenges is related to data quality and validity. Big Data often consists of unstructured information originating from various sources such as social media, digital transaction applications, and distributed financial systems. Data inaccuracy or inconsistency can cause failures in the analytical process, which in turn reduces the effectiveness of the violation or anomaly detection

system²⁸. In addition, there are obstacles in terms of infrastructure and technological capacity, especially for Islamic financial institutions that do not yet have adequate big data-based information systems. Many small and medium-sized institutions do not have the resources to develop or adopt the sophisticated analytical systems needed to manage high volumes and speeds of data²⁹. This challenge is compounded by limited human resources, where there is a gap between the need for data analysts who understand the technical aspects of Big Data and have competence in sharia principles and regulations.

From a legal and policy perspective, the use of Big Data also faces challenges in terms of personal data protection regulations and legal frameworks that are not yet adaptive to the development of digital technology. Although a number of countries have implemented personal data protection laws, in practice there are still violations of the principle of privacy, and this creates a conflict with Islamic values that uphold the mandate and protection of individual rights³⁰. Furthermore, in the context of Islamic economics, ethical challenges arise regarding the use of data for non-transparent commercial purposes, which can lead to practices that conflict with the maqashid of Islamic law, especially in terms of protecting property (ḥifẓ al-māl).

Another equally important challenge is the lack of system integration between institutions and limited collaboration between regulators and industry. This has led to data silos that hinder the exchange of information in order to detect illegal financial activities comprehensively. In addition, the cybersecurity aspect is also a serious concern because the increasing dependence on digital data makes the financial system more vulnerable to cyber attacks and leaks of confidential information³¹. Thus, although Big Data has great potential in strengthening regulatory compliance in the era of digital finance, its implementation requires a comprehensive cross-sector strategy, starting from increasing digital literacy and human resource capacity,

²⁸ Caseba and Dewayanto, "Penerapan Artificial Intelligence, Big Data, Dan Blockchain Dalam Fintech Payment Terhadap Risiko Penipuan Komputer (Computer Fraud Risk): A Systematic Literature Review."

²⁹ Amir Gandomi and Murtaza Haider, "Beyond the Hype: Big Data Concepts, Methods, and Analytics," *International Journal of Information Management* 35, no. 2 (April 2015): 137–44.

³⁰ Tal Zarsky, "Incompatible: The GDPR in the Age of Big Data," *Seton Hall Law Review* 47, no. 4(2) (July 22, 2017).

³¹ Chen, Chiang, and Storey, "Business Intelligence and Analytics: From Big Data to Big Impact."

strengthening adaptive regulations, to developing safe and sharia-compliant infrastructure. Collaboration between regulators, academics, and industry players is key to answering these challenges in a sustainable and beneficial manner.

Conclusion

The use of Artificial Intelligence (AI) and Big Data in the Society 5.0 era has proven to provide significant contributions in analyzing and detecting illegal financial activities, violations of sharia principles, and cybercrime. AI is able to identify suspicious transaction patterns, provide early warnings of the risk of violations, and help assess compliance with laws and regulations automatically through algorithms that continue to learn. The role of Big Data complements this function by providing large-scale, fast, and diverse data sets that enable deeper and real-time analysis of financial behavior. However, the application of this technology is not without challenges and limitations. AI faces obstacles in interpreting complex legal norms and ethical values, including sharia principles that are interpretative and contextual. Meanwhile, Big Data faces issues of privacy, data security, information quality, and limited human resources who are able to manage data effectively and ethically. Optimizing the use of AI and Big Data in the digital financial sector requires strengthening the regulatory framework, implementing technology ethics, and close cooperation between regulators, industry players, and technology developers. This synergy is key to building a safe, fair, and sustainable digital ecosystem amidst the challenges of global digital transformation.

References

- Abbassi, Hanae, Imane El Alaoui, and Youssef Gahi. "Fraud Detection Techniques in the Big Data Era ." In *Proceedings of the 2nd International Conference on Big Data, Modelling and Machine Learning (BML 2021)*, 161–70, 2021.
- Akbar, M. Rafli, Kgs M. Syarif Hidayatullah, and Tata Sutabri. "Evaluasi Efektivitas Sistem Deteksi Penipuan Berbasis Ai Menggunakan Metode

- Regresi Logistik Untuk Meningkatkan Keamanan Transaksi Pada Startup Finance.” *J-ENSITEC* 10, no. 2 (2024): 10107–11.
- Caseba, Farah Labibah, and Totok Dewayanto. “Penerapan Artificial Intelligence, Big Data, Dan Blockchain Dalam Fintech Payment Terhadap Risiko Penipuan Komputer (Computer Fraud Risk): A Systematic Literature Review.” *Diponegoro Journal of Accounting* 13, no. 3 (July 2024).
- Chen, Hsinchun, Roger H. L. Chiang, and Veda C. Storey. “Business Intelligence and Analytics: From Big Data to Big Impact.” *MIS Quarterly* 36, no. 4 (December 2012): 1165–88.
- Cheng, Xueqi, Shenghua Liu, Xiaoqian Sun, Zidong Wang, Houquan Zhou, Yu Shao, and Huawei Shen. “Combating Emerging Financial Risks in the Big Data Era: A Perspective Review.” *Fundamental Research* 1, no. 5 (September 2021): 595–606.
- Dara Sawitri. “Artificial Intelligence for a Digital Technology Smart Society in the Era of Society 5.0.” *Journal of Artificial Intelligence and Software Engineering* 5, no. 1 (March 2025): 135–43.
- Dewati Sallma Syahtri. “Peran Natural Language Processing (NLP) Untuk Mendeteksi Penipuan Dalam Dokumen Keuangan.” <https://Accounting.Binus.Ac.Id/2024/12/06/Peran-Natural-Language-Processing-Nlp-Untuk-Mendeteksi-Penipuan-Dalam-Dokumen-Kuangan/>, June 2024.
- Dong, Yanjiao, Zhengfeng Jiang, Mamoun Alazab, and Priyan Malarvizhi Kumar. “Real-Time Fraud Detection in e-Market Using Machine Learning Algorithms.” *Journal of Multiple-Valued Logic and Soft Computing* 36, no. 1–3 (2021): 191–209.
- Gandomi, Amir, and Murtaza Haider. “Beyond the Hype: Big Data Concepts, Methods, and Analytics.” *International Journal of Information Management* 35, no. 2 (April 2015): 137–44.
- Hasri Ainun Syahfir, Anastasia Gloria Panggeso, Amiruddin, and Syamsuddin. “Melampaui Batas Penglihatan Manusia: Peran Ai Dalam Mendeteksi Fraud Pada Proses Audit Tinjauan Literatur Sistematis.” *Jurnal Revenue : Jurnal Ilmiah Akuntansi* 5, no. 2 (2025).
- Ilahi, Nurul, and I Nyoman Budiono. “Penerapan Artificial Intelligence Sebagai Inovasi Di Era Disrupsi Dalam Mengurangi Resiko Keuangan.” *MONETA : Jurnal Manajemen Dan Keuangan Syariah* 3, no. 1 (2024).
- Kirti Ranjan Swain, and Subhasmita Mallick. “Artificial Intelligence in Finance: Challenges and Opportunities .” *Scope* 13, no. 2 (June 2023).

- Lexy. J. Moleong. *Metodologi Penelitian Kualitatif*. Bandung: PT Remaja Rosdakarya, 2000.
- Luluk Setyowati, and Deni Nasir Ahmad. "Pemanfaatan Big Data Dalam Era Teknologi 5.0 ." *Jurnal Pengabdian Kepada Masyarakat* 1, no. 2 (December 2021): Hal.117-122.
- Muhammad Ayub. *Understanding Islamic Finance*. Jakarta: Gramedia Pustaka Utama, 2013.
- Nafidzi, Elman, and Khabib Musthofa. "Peluang, Strategi, Dan Tantangan Industri Perbankan Syariah Dalam Menghadapi Artificial Intelligence (AI)." *Journal of International Multidisciplinary Research* 3, no. 2 (2025): 68–76.
- Ramírez Sánchez, Julián, Alejandra Campo-Archbold, Andrés Zapata Roza, Daniel Díaz-López, Javier Pastor-Galindo, Félix Gómez Mármol, and Julián Aponte Díaz. "Uncovering Cybercrimes in Social Media through Natural Language Processing." *Complexity* 2021 (2021). doi:10.1155/2021/7955637.
- Rifai, Muhammad Habib, Dimas Akbar Pramudya, and Rohmad Rafi Narfandi. "Analisis Peran Teknologi Kecerdasan Buatan Dalam Mengoptimalkan Proses Deteksi Terhadap Serangan Siber." *Semin. Nas. Teknol. Inf. Dan Bisnis* 18, no. 6 (2024): 495–502.
- Rosita, Dian, Arina Novitasari, Naili Azizah, Nila Maulida Cahyaningrum, and Zuniarti. "Analysis of Legal Protection of Intellectual Property Rights from a Criminal Law Perspective." *Jurnal USM Law Review (JULR)* 8, no. 2 (2025): 609–21.
- Shalaginov, Andrii, Jan William Johnsen, and Katrin Franke. "Cyber Crime Investigations in the Era of Big Data." In *2017 IEEE International Conference on Big Data (Big Data)*. Boston: IEEE, 2017.
- Shalhoob, Hebah, and Iman Babiker. "Exploration of AI in Ensuring Sharia Compliance in IF Institutions: Focus on Accounting Practices." *Open Journal of Business and Management* 13, no. 2 (2025).
- Sindu Prasetyo, and Totok Dewayanto. "Penerapan Machine Learning, Deep Learning, Dan Data Mining Dalam Deteksi Kecurangan Laporan Keuangan - A Systematic Literature Review." *DIPONEGORO JOURNAL OF ACCOUNTING* 13, no. 3 (2024): 1–12.
- Susatyo, Febryan Alam, and Dian Rosita. "Relevansi Pertanggungjawaban Pidana Atas Culpability Kecerdasan Buatan (Artificial Intelligence)." *Literasi Hukum* 8, no. 2 (2024): 59–68.

- Udeh, Ezekiel Onyekachukwu, Prisca Amajuoyi, Kudirat Bukola Adeusi, and Anwulika Ogechukwu Scott. "The Role Of Big Data In Detecting And Preventing Financial Fraud In Digital Transactions." *World Journal of Advanced Research and Reviews* 22, no. 02 (2024).
- Widjaja, Gunawan. "The Role Of Big Data Analysis In Financial Decision Making: The Case Of Islamic Banking." *Februari* 2, no. 2 (2024): 264–76.
- Zarsky, Tal. "Incompatible: The GDPR in the Age of Big Data." *Seton Hall Law Review* 47, no. 4(2) (July 22, 2017).

Acknowledgment

None

Funding Information

None

Conflicting Interest Statement

The authors state that there is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

Generative AI Statement Statement

N/A