

RESEARCH ARTICLE

Exploring the role of AI in shaping social behavior: An Intersectional psychological perspective on financial risk assessment through digital platforms

Ma Howard¹, Guo Wei²

¹ aSSIST University, 136-791, South Korea

² Tsinghua University, Beijing, 100084, China

* Corresponding author: Guo Wei, edwin93@163.com

ABSTRACT

Artificial intelligence analytics in digital finance platforms is important in the modern digital world. AI can conduct analytics quickly and provide the outcomes for the system users to make informed, data-driven conclusions. AI can scan through large datasets and provide meaningful information on social media platforms, historical quantitative transactions, and finances to give critical findings, unlike traditional systems. This review article assessed previous research articles on financial risk evaluation using AI analytics in the finance industry and digital finance platforms. The outcomes outlined the capabilities of financial risks evaluated with the help of AI in digital finance platforms. The key identified risks were credit risks, market risks, operational risks, fraud risks, and compliance risks. The study outlined the key capabilities of AI in shielding firms against such risks through predictive analytics, anomaly detection, sentiment analysis, and credit scoring. The AI systems should be hosted on the cloud to have access to large datasets to give accurate, data-driven conclusions. The identified challenges are algorithm bias, data privacy, regulatory compliance (especially across platforms and countries), and skill gaps in the market. In conclusion, using AI in digital finance platforms has increased the efficiency in making informed decisions for sustainability and strategic growth.

Keywords: artificial intelligence; financial analytics; digital finance platforms

1. Introduction

Financial risk evaluation using Artificial Intelligence (AI) in digital finance platforms is a rapidly growing field due to the emergent benefits to the financial service providers^[1]. AI makes use of deep learning (DL), machine learning (ML), natural language processing (NLP), and big data analytics to help organizations make informed decisions due to the weight of the evidence presented^[2-3]. This prevents the organizations from making wrong financial decisions that would pose a risk of sustained operations for the firms or hinder the achievement of the objectives optimally. Artificial intelligence is the use of technology through analysis of quantitative and qualitative data to make human-intelligent decisions^[4]. The systems can assess vast volumes of data and information as a basis for helping organizations make strategic choices.

Financial risks are the uncertainties regarding the operation of financial service providers to their client

ARTICLE INFO

Received: 1 January 2025 | Accepted: 16 January 2025 | Available online: 31 January 2025

CITATION

Howard M, Wei G. Exploring the role of AI in shaping social behavior: An Intersectional psychological perspective on financial risk assessment through digital platforms. *Environment and Social Psychology* 2025; 10(1): 3375. doi:10.59429/esp.v10i1.3375

COPYRIGHT

Copyright © 2025 by author(s). *Environment and Social Psychology* is published by Arts and Science Press Pte. Ltd. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0/>), permitting distribution and reproduction in any medium, provided the original work is cited.

base. The digital finance platforms in this contest are banking applications and other digital money phone and computer applications used by clients. The uncertainties associated with digital finance applications include fraud risks, compliance risks, operational risks, market risks, and credit risks. ^[5]. Using digital finance platforms exposes the users and the firms to fraud risks; these are fraudulent activities performed by cybercriminals that lead to the loss of money. Compliance risks are the uncertainties associated with adherence to regulatory frameworks such as data protection regulations, abiding by government and central bank regulator frameworks regarding financial services provision, and other laws within the country or region. ^[6]. Operational risks are the uncertainties regarding internal systems and processes that would render the organization (service provider) or the user vulnerable. ^[7]. Market risks in digital finance platforms are uncertainties regarding the market conditions external to the business; the fluctuations regarding the economic and industry conditions are examples of market risks. ^[8]. Credit risks are the uncertainties associated with the likelihood of loan defaults and advancement of credit to the clients. The finance industry has advanced with the risk of technology solutions in providing services. However, they face vulnerabilities in adopting these technological solutions.

The use of AI for evaluation arises from its ability to conduct predictive analytics, sentiment analysis, anomaly detection, and credit scoring ^[9]. Predictive analytics is the use of real-time and historical data to predict the trends in a phenomenon under investigation; it is often used to check the potential fraud, loan defaults, the optimal loans to offer to an entity, or any other service that needs forecasting using historical or real-time data ^[10]. Sentiment analysis is the use of NLP to conduct a qualitative analysis of information on platforms to anticipate financial risks. NLP analyzes the qualitative data (sentiments on various online platforms, e.g., news platforms and social media) to make an anticipation for financial risks ^[11]. For example, clients and regulatory bodies may use sentiment analysis to assess the quality of reviews given to financial service providers to assess whether such providers meet the law and regulatory requirements or utilize predatory tactics and are fraudsters disguised as financial service providers. Anomaly detection is the use of machine and deep learning algorithms to detect unusual patterns in the security of the systems, in particular to detect malware, system intrusions, fraud, and any irregularities ^[12]. AI is also used for credit scoring, where it leverages the powerful data analytics of AI using historical and real-time data, social media, and other platforms to find the right credit score for potential clients and come up with the terms of credit advanced to them. Unlike traditional data sources, which are limited hence the service provider is not able to make the right decisions from inconclusive evidence, incorporating AI in creditor and debtor analytics, the information will help providers arrive at the right data-driven decisions ^[13].

The adoption of AI in has positive trends in Asian countries as they leverage the use of technology to ease effective strategic decision-making for sustained and profitable business operations. Since there are billions of transactions processed daily, the need for AI embedded in the systems is a critical connection to keep up with the systems to prevent risky situations such as fraud detection, cybersecurity anomalies, and trend analysis. The goal of this study is to highlight how firms have used AI to conduct risk evaluation and prevent some of the avoidable risks, especially in digital finance platforms, and the challenges in AI implementation.

2. Materials and methods

The paper used the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) methodology to identify the articles on risk evaluation using AI in digital finance platforms.

Eligibility criteria: the inclusion criteria for the articles were peer review articles in the field of financial risk using AI in digital platforms, the exclusion criteria were articles that were comprehensive in the abstract of the use of AI in risk evaluation, especially in digital finance platforms.

Information sources: the databases used for research were Elsevier, SpringerLink, ResearchGate, Ebscohost, and Google Scholar, which led to the right articles to be included in the study.

Risk of Bias: To minimize the risk of bias in the study, the researcher assessed both the abstract and findings of the studies to come up with conclusive information regarding the articles to be included in the study and other critical information for the study.

Synthesis of results: The results were summarized in tables, charts, and elaborated findings in the results section. The discussions interpreted the findings in line with the research objectives.

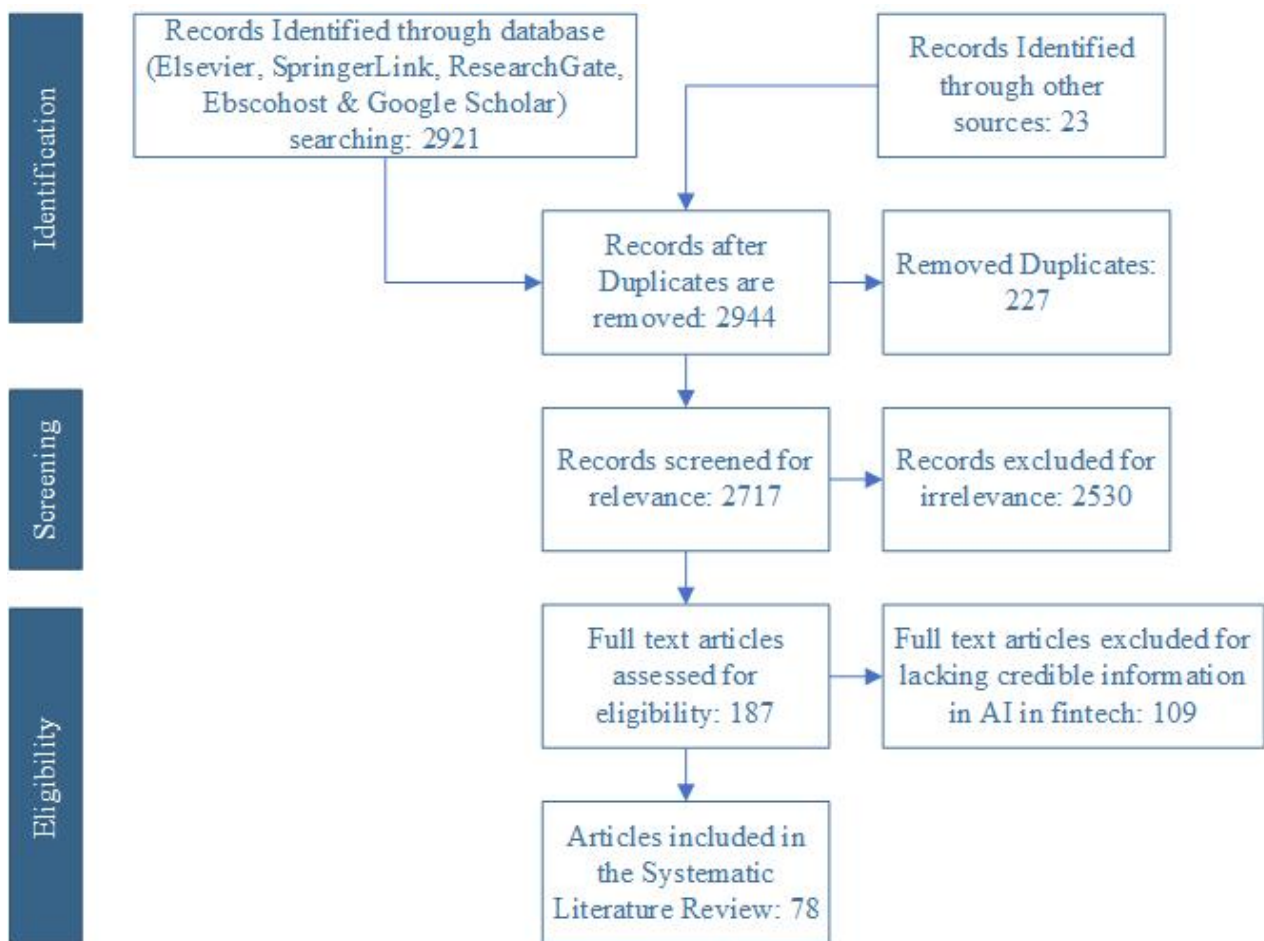


Figure 1. The PRISMA methodology used in systematic literature review.

3. Results and discussion

3.1. Financial risks evaluation

It is the assessment of uncertainties that could lead to financial losses. The core financial risks that digital finance firms face are credit risks, market risks, operational risks, fraud risks, and compliance risks. It is expedient for firms to understand the operating environment in the banking and finance industry to effectively shield their business goals from the exploitation of wrong strategic decisions. AI analytics refers to the use of artificial intelligence techniques to analyze data and derive insights. It makes use of machine

and deep learning to effectively and efficiently assess and protect firms against the financial risks they face. [14].

3.1.1. Credit risks

Financial challenges in individuals and firms pose the challenge of loan defaults of fulfillment of obligations in contractual agreements. The assessment of creditworthiness needs systems that effectively conduct assessments of all the features in the data to rate the clients. While traditional systems depend on fewer features and less data, AI assesses millions of transactions in various datasets to ensure the right conclusions are arrived at. As discussed before, it analyzes not only statistical data but also qualitative data from the company websites, financial reports, strategic plans, and social media platforms so that the right prospects can be made on credit. [15-16].

The other advantage of AI in financial assessment analytics is the increased automation and efficiency in analyzing large datasets to detect any issues in real time. [17]. The speedy analysis of large datasets with different characteristic features makes it easy to interpret the findings and make informed data-driven decisions. It also offers early warning signs that help easily detect the deterioration of the creditworthiness of customers. For instance, some of the customers may have been credit-worthy previously. However, the firms may accumulate higher debt. Such leveraged firms degenerate their creditworthiness due to wrong financial decisions during tough economic times for businesses. Financial organizations, thus, manage the risks proactively to prevent bias and assumptions for their customers. [14,18].

Other advantages are AI is effective in risk profiling, risk monitoring, risk reporting, and regulatory reporting. [19]. In risk profiling, deep learning and machine learning can profile the risk based on the source and rate it, whether it is manageable or too risky to invest in [20]. If it can be corrected, the financial service providers can advise the companies on what course of action to take to improve their credit score. In risk reporting, the AI systems will generate automated reports to help the clients and the financing institution keep a record of their leverage and performance; this will help the firms to make calculated strategies to control debt. In risk monitoring, the real-time dashboards will give reports for monitoring the financial risks and the forecasts for effective control. In regulatory reporting, the firms, through AI reporting and the following of real-time reports, will be able to ensure compliance with the regulatory framework. [21]. For instance, it will prevent or raise the alarm when firms are going bankrupt and have not raised the alarm or reported any fraud or credit malpractice. This prevents the financial and digital platforms from engaging in activities that would be risky and legally punitive. [22].

3.1.2. Market risks

AI analytics plays a quintessential role in determining market risks. The AI algorithms employ sophisticated means of data processing to handle massive quantities of market data and analyze them. This includes but is not limited to analyzing economic indicators, financial reports, and news articles. With very fitting extraction, pattern detection, and recognition of correlation, AI algorithms would assist in the discovery of probable market disruption or risks affecting the course of operations and investment undertaken by a financial institution. [23].

Predictive analytics, for example, is very important for predicting market trends and volatility. AI modeling can simulate several risk scenarios, helping organizations quantify and manage uncertainties. Risk predictions are better because they capture quite complicated patterns in financial data, which might be lost by other methods. Predictive analytics can forecast the impacts of inflation on businesses and the deterioration of credit scores for firms, for example, when credit is advanced to a firm, and inflation rises sharply, the money paid will not reflect the true value of money for the future. [24]. Thus, it considers all the

drivers of inflation and predicts the right inflation rate to be used when computing the interest for the credit facility to prevent the lender from making losses due to the depreciation of the true value of money. ^[25].

Stock prices are always determined by various factors in the market; these are analyzed as features in the datasets. ^[26]. Both the structures and unstructured data from various sources can be used to predict stock prices; this will eliminate the false impressions that firms may increase in stock value or market capitalization when there are market forces that will reduce the value of the company both within the firm or outside as depicted from financial reports, social media, and other market reports. ^[27]. This will be critical for credit providers to determine the financial risks of firms.

The labor force is a critical market risk in the operation of firms. The labor force always needs better packages for allowances, salaries, and remuneration that reflect the market and industry forces. ^[28]. It will always have a financial consequence on firms. In Human Resource (HR) analytics, it critically analyzes labor requirements and make predictions so that firms are not entangled in huge wage bills that will jeopardize operations and make them unsustainable. ^[29]. Therefore, AI can analyze the patterns in economic data from different sources and help digital finance platforms make the right data-driven decisions for their clients.

However, new problems emerge as well. Public confidence in the financial system can be undermined when the opacity of AI decisions, vulnerability to manipulation, and robustness-related issues are married to privacy concerns. ^[30]. AI can thus even bring in new sources and transmission channels of systemic risks. For example, if many institutions rely on similar asset allocation AI models, then the demand and supply for financial assets may systematically tend towards distortions that could incur very high costs in adjustments in their markets, making them less resilient. Thus, there is significant improvement financial risk assessment for real-time understanding and better decision-making, it can also include a basket of new risks that need to be cautiously managed and instituted regulation.

3.1.3. Operational risks

The operational risks for firms are related to internal systems in the organizations. The risks may lead to losses since they affect the trust the clients have for the system, hence leading to a decline in financial performance. ^[31]. The common risks are system human errors, technical glitches, and system failures. All these hurt the operations since they hinder effective operations and lead to financial losses in the organization. The clients for digital finance platforms always expect hosted services to work efficiently and seamlessly. Failure of one of the functional requirements or non-functional requirements leads to distrust in the digital platforms, and negative sentiments will be found in various platforms when reviews are given about the product.

System failures are common if the firms do not implement the right hardware and software components. The system failures may be due to hardware or software limitations. While AI may not so effectively handle the hardware challenges, it can give predictive analytics on the use of the hardware platforms so that the limitations are overcome. ^[32]. Rather than some of the platforms being overworked, AI can distribute the load to all the hardware to reduce the instances of failure. On software capabilities, AI integration into the software makes predictive analytics to the system user so that when the capacity is exceeded, the system automatically regulates or gives an early warning. It also transfers some of the roles to the cloud for flexibility and scalability and increases the capacity to handle the volume of transactions and other operations. Failure of systems is greatly minimized by the efficient integration of cloud platforms and analytics to automatically schedule system usage. ^[33].

Human errors often occur in traditional systems, which are often uncovered later through disaster recovery and system audits. ^[34]. However, human errors are significantly reduced by automation and AI

since AI will implement the desired internal audit controls before errors are committed. The reduction of human errors in digital platforms reduces the changes of financial risks in digital fintech platforms. If there are any suspicious transactions, they are withheld until investigations are conducted and approved. [35]. The system will provide recommendations based on prior analytics into various databases about the clients to prevent money laundering, fraudulent activities, and any suspicious patterns in the data. [36].

3.1.4. Fraud risks

The common fraud risks in digital finance platforms are identity theft, fraudulent transactions, money laundering, and phishing scams. [37]. To prevent identity theft, embedded AI systems can assess the features of the source, such as IP address and MAC address assigned to devices. [38]. If the identifiers are not consistent, the AI system rejects access to the information and alerts the users of potential breaches. Thus, systems often require two-factor authentication (2FA) to prevent identity theft. This also happens for SIM Swap fraud and other data breaches that would perpetrate fraud. The AI systems can detect anomalies and effectively prevent any suspicious activities that would otherwise be impossible for the millions of users or transactions the systems handle at any particular moment. [37,39].

Phishing is common when cyber-attackers deceive users into installing malware or revealing sensitive information to scammers when sent through emails or text messages. [40]. However, integrating AI into cybersecurity can prevent malicious access points from affecting the system's integrity. Another attack point is pharming, where the browser settings are attacked and redirected to attacker-controlled websites. However, the browsers can be secured by AI systems, which can prevent pharming to deceptive sites that decoy as digital financing platforms. [41]. AI systems also prevent money laundering activities since the sophisticated system of analytics can trace the source of funds and prevent the laundering activities. This ensures compliance with international regulations and countering criminal activities. [42].

3.1.5. Compliance risks

Compliance with statutory regulations is critical to the sustainability of operations. The issues of compliance are the monetary policies, the ethics and data privacy requirements, and the shifting from black-box models to white-box models in analytics. [43]. The monetary policies are the lending rates, adjusting to inflation, and other requirements needed to regulate the money supply in the economy. The central banks in countries often institute policies to remedy various economic conditions, such as limiting access to credit to reduce the money supply and slow economic growth till all market and industry conditions are stable or increasing the money supply through increasing access to credit and lowering the lending rate to spur economic growth. Integrating AI systems into digital fintech platforms enables compliance with the statutory regulations regarding monetary policies since they can learn and make the required adjustments automatically. [44].

On data privacy concerns, AI systems are effective since they can detect malicious attacks and mend anomalies to prevent data breaches. The increased cybersecurity of the systems prevents access to the data in the cloud through anomaly detection and neutralizing such attacks. Authorized access using AI is enabled by assessment of the entry point features such as biometric data, multiple factor authentication, assessment of device and IP address accessing the system, etc. Apart from that, AI-enabled data encryption helps prevent any unauthorized decryption schemes from accessing personal data. [45-46].

Previous models on financial data were based on black-box models, the outcome could be given by the systems but could not be explained how the systems came up with the findings. This was a malpractice that is now restricted by law; the modern models need to be explainable, hence the term white-box models. The development of explainable AI models helps arrive at conclusions that can be explained to clients, such as

the reasons for the credit score, since the findings can be traced to outcomes of the analytics. [47-48]. It is easier to explain the findings using AI since each step can be iterated than traditional models, which are often black-box models in which system users are not able to deduce the reasons for every finding.

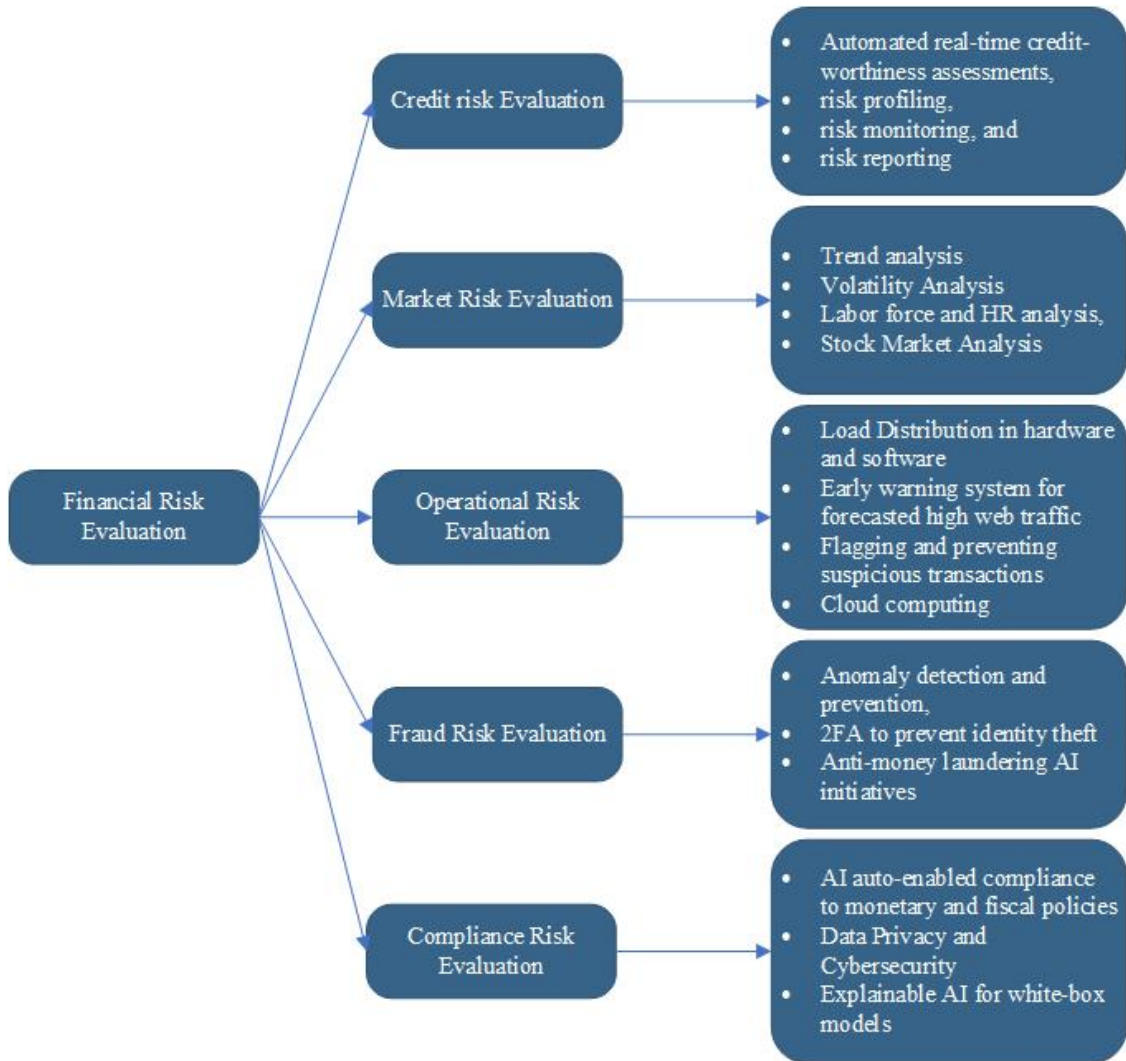


Figure 2. The uses of AI in risk evaluation in digital platforms.

3.2. Key AI capabilities in digital finance platforms

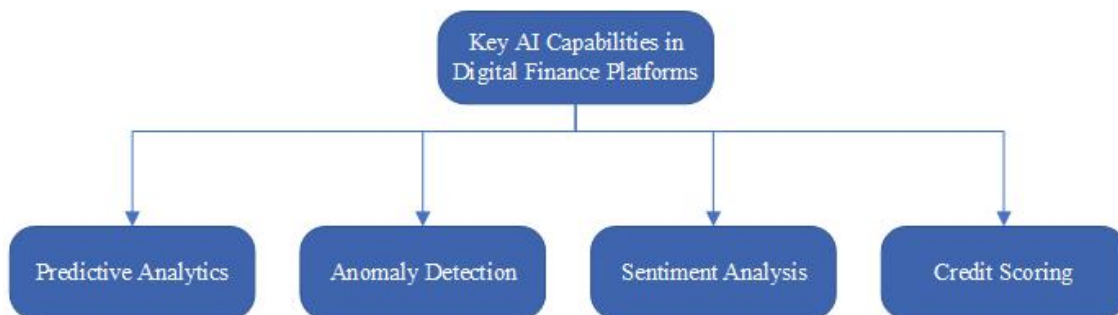


Figure 3. The identified key AI capabilities for systematic literature review.

3.2.1. Predictive analytics

AI predictive analytics offers an effective method to analyze big data from various sources due to the increased sophistication of both structured and unstructured data. ^[49] . It offers an effective mode of anticipating and mitigating financial risks before they occur. ^[50] . Predictive analytics has been integrated with Cyber Threat Intelligence (CTI) to assess malware logs, phishing campaigns, dark web forums, and social media for anomaly detection and assess the risks and threat patterns hence, firms give a proactive response to cyber threats. ^[51].

Predictive analytics has been effectively used for financial inclusion; the traditional credit histories are often biased against low-income individuals and small businesses because they do not have a long history of existence or the volume and value of transactions are lower. However, predictive analysis assesses a larger volume of data from various alternative sources (such as utility bill payment, mobile phone usage, and social media interactions) about the client to build a worthy credit profile. ^[52] . Likewise, start-up businesses and gig freelancers have difficulty accessing financing for their business enterprises and operations. Through big data analytics, entities and individuals in the gig economy can access inclusive financial services since AI can develop new credit scoring models and offer personalized financial advice. ^[53-54].

Traditional mathematical models are not able to deep-mine massive amounts of economic data for countries; China leverages the use of AI and predictive analytics to maintain the soundness of its economic system. ^[55] . Through data cleaning and fusion algorithms, predictive analytics has been a basis for early analysis of economic security and warns financial service providers to make necessary operational decisions. ^[55] . Markets also depend on predictive analytics to respond quickly to market movements, real-time data feeds help firms respond to uncertainties in turbulent markets to enhance operational resilience, reduce losses, and ensure compliance monitoring. ^[56].

3.2.2. Anomaly detection

Cyber threats keep evolving and threaten the integrity of security in banking and digital finance platforms. AI has made a transformative impact in detecting fraud and threats, hence offering innovative solutions to counter the threats. ^[57] . In particular, AI algorithms have been perfect in processing massive amounts of data to learn transactional and behavioral patterns. Through effective analytics, the systems can detect anomalies and profile the risk for prevention and investigation. The detection of anomalies is essential when detecting money laundering, fraud detection, malware, and ransomware activities. Deep learning anomaly detection and prevention have been employed to mitigate such risks. ^[57].

AI is specifically suited for anomaly detection; it employs the use of supervised and unsupervised learning to extract features from the data and classify the incoming transactions. The legitimate and fraudulent transactions can be filtered based on features such as device data (IP address), transaction data (order value, billing address), and user historical data. ^[58] . Other techniques in anomaly detection, such as Generative Adversarial Networks (GANs), have been effective for fraud detection in the Fin-Tech industry since they effectively discriminate between legitimate and fraudulent transactions, hence offering precise and efficient real-time identification of suspicious activities. Unfortunately, the black-box nature of GANs hinders transparency in the highly regulated finance industry. Posthoc analysis and feature-attribute techniques have been used to enhance the models to satisfy the transparency requirement ^[59].

Detection of threats from insiders is a global threat, some of the anomalies and fraud are perpetrated by the employees who understand the system. However, the use of AI can be an effective shield so that the controls are not bypassed by the system insiders. AI-powered threat detection reveals behavioral anomalies, predictive analysis of employee activities, and network behavior analysis to prevent fraud. ^[60].

3.2.3. Sentiment analysis

Sentiment analysis is effectively used for assessing social media platforms for real-time emotions, options, and the behavior of volatile digital finance markets that depend on social media [61]. Digital finance platforms overly depend on the market that spends time on social media, negative sentiments about a certain platform would negatively affect its client base, while positive feedback on social media platforms will have a positive impact on the operations. To prevent investment risks and operational risks, NLP is integrated into the analytics to guide portfolio assessment and forecasting operations. [61-62]. In a study on target-based emotion analysis on Twitter (currently X), it was found that finance-based emotions can make predictions on the performance of stock market assets to prevent high investment risks, unlike the traditional dividend or stock price models. Combining ML models and NLP models on social media messages can help in the detection of financial opportunities or precautions for investors [63].

AI is also effective in mining risk-related sentiments in corporate annual reports. Apart from the sentiment analysis in financial reports, the risk-related sentiments in the top management speech can be used to effectively assess the risks such as the company debt, bankruptcy risk, market value, and profitability. [64]. For those working in investment and algorithmic trading firms, social media sentiment analytics is critical to providing stock price prediction and investment management. The open-ended interviews are harnessed as data sources to effectively show the operational risks before investments. [65]. Sentiment analysis is also used as a supplementary tool for traditional surveys, which are time-consuming and costly. It is also used for pattern analysis in the event of security breaches to prevent further risk since it raises public awareness and action can be taken to remediate it on time. [66].

3.2.4. Credit scoring

The use of AI in the credit scoring of clients presents a timely and accurate method of assessing trends and patterns in prospective client financial positions. The use of AI minimizes bias since it assesses vast amounts of data that rate the client. [67]. Traditional systems often introduce bias of judgment based on various features such as geographical location, ethnicity, volume, and value of historical transactions. For example, individuals or entities who have no history of a volume or value of transactions are less likely to receive credit. That has often hindered many seed companies that would have accessed credit and began on a high note to be profitable ventures, but due to lack of enough capital, they may begin and not break even due to operating under capacity. To ease the burden on seed financing, the use of AI in credit score assessment conducts the right analytics to determine the score and credit facility that can be advanced.

The conditions in the industry and market conditions are also critical to the credit facilities that can be advanced. Monetary and fiscal policies can be effectively assessed to determine the credit that can be advanced to firms, this complies with the regulations as instituted by the statutory agencies to achieve the desired effects in the economy. Thus, AI enhances compliance and explainability of every action taken by both the government agencies and the client. [68].

The risk with traditional credit scoring is a wrong judgment based on bias and lack of clear assessment of the economic conditions and market conditions. Large companies may be assumed to be financially secure when they are highly leveraged and lower their creditworthiness. However, based on the volume and value of transactions, the credit assessor may make wrong judgments and make the wrong strategic decisions. Thus, the use of AI reduces the instances of such wrong decisions and biases since the right analytics will give the right credit score to the clients of digital finance firms. [69].

3.3. Challenges in implementing AI for risk evaluation

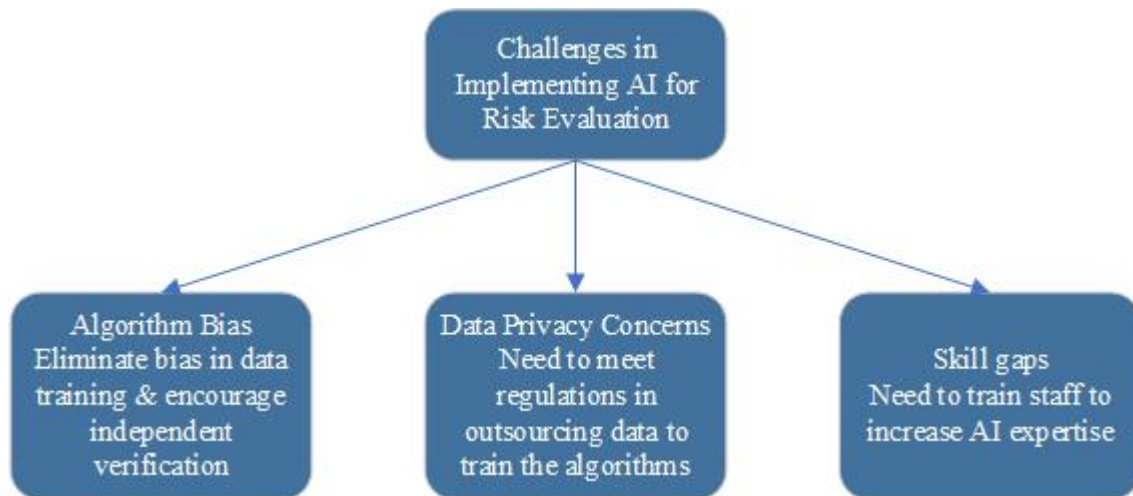


Figure 4. The identified challenges in solutions in AI implementation.

The challenges in using AI are algorithm bias, data privacy issues, regulatory compliance, and skill gaps. These are discussed below.

3.3.1. Bias

Bias in AI algorithms interferes with the outcome of the data analysis. The source of bias is generally from the training of the dataset and the algorithm bias. [70].

Data bias training: AI systems are trained on past data; they may contain inherent biases from past human decisions or social anomalies. For example, some populations may be underrepresented or have different coincidence structures for the model's target variables, leading to distorted results.[71].

Algorithmic bias: Characteristics of the methods used in an AI system can also introduce bias. For example, a machine learning model can create a bias if its training data is biased. [72]. Similarly, logic-based AI systems can be biased if the knowledge engineer's vision is distorted.

Financial institutions can use several strategies to address these issues:

Pre-modeling interpreter: This involves analyzing the dataset before building the model to eliminate any potential bias. This helps ensure that the data used for training is representative and unbiased [73].

Post-Model Interpretation: Interpreting complex models is important in understanding how decisions are made after the model has been developed. This helps to identify and correct biases that may occur during the modeling process. [73].

Independent verification: Third-party organizations are required to verify and certify the objectivity of the model. This ensures that unintended bias is identified and eliminated. [72].

Diverse teams: It is important to promote diversity within teams that develop and manage AI algorithms. Diverse teams are more likely to identify and address biases that may occur during development. And provide a different perspective on how bias can creep in.

3.3.2. Data privacy

AI systems analyze large datasets to get information about the company, clients, and any other related financial platforms before they can guide in making informed findings. Assessment of the datasets may breach some data privacy regulations. [74]. The AI systems analyze personal data in social media, bank

information, and credit scores in independent platforms to make the right predictive analytics on the phenomena under study. This implies that data in the platforms is not fully secured against the access of the AI algorithms so that they can access the data. For example, if an AI algorithm has to assess text messages and social media platforms to give a credit score, this implies the private texts on the phone are not secure from AI. [75]. While the client consents to such when using digital finance platforms, the only hope is their private information is not leaked to the supposed secure AI systems.

3.3.3. Regulatory compliance

Most digital finance platforms are cross-country, and payment platforms are developed to gain application in various countries. While some countries have high standards of ethical practice on data privacy, some countries do not have laws and policies on the regulation of private data on digital platforms. [76]. To comply with the various regulations in monetary policies, data privacy, and other ethical practices, bespoke digital platforms are often created to match a country's or region's law requirements. [77]. This prevents gaps that would lead to legal litigations.

3.3.4. Skill gaps

The lack of expertise in digital data science and AI hinders the implementation of the digital platform requirements. [78]. The decline in staffing and personnel is overcome by training staff in AI expertise, and developing and hosting the platforms to meet the labor demands.

4. Future trends

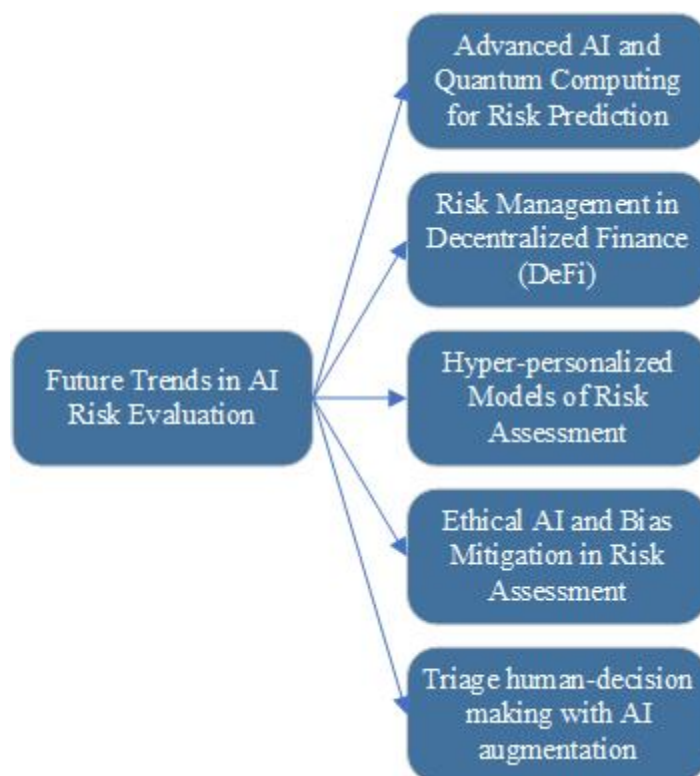


Figure 5. The future trends in AI for financial risk evaluation.

Risk Prediction with Advanced AI & Quantum Computing: Quantum computing will find ways to analyze tons of information related to risk at the speed of light. Predictive analytics will be more granular in testing financial systems, hence higher efficiency than the current algorithms.

Risk Management in Decentralized Finance (DeFi): AI will be integrated into smart contracts and help in the prevention of any fraudulent activity in the DeFi transactions. Banks and fintech firms will use federated learning to enhance risk models without transferring any sensitive data. AI will also analyze decentralized data silos without exposing sensitive customer data.

Hyper-Personalized Models of Risk: AI will customize risk analysis based on personal spending trends rather than solely on traditional metrics. This will help in personalized lending, insurance, and investment products.

Ethical AI & Bias Mitigation: With pressure to eliminate the lack of transparency and bias in AI algorithms, AI developers will focus efforts on mitigating bias in risk assessment models. The evaluation of financial risk will be guided by ethical AI frameworks.

Triage human decision-making with AI-augmented intelligence: Financial risk analysts will not be replaced by AI but will benefit from deeper, data-driven insights to make better decisions. A human-in-the-loop AI will ensure risk decisions are as data-based and context-conscious as possible.

5. Conclusion

The review paper investigated the role of AI in financial risk evaluation in digital finance platforms. The common financial risks evaluated by AI include market risks, operational risks, compliance risks, credit risks, and fraud risks. The AI systems can speedily analyze vast amounts of structured and unstructured data to help the firm mitigate the probable financial risks it faces. The key AI capabilities that enable the detection and prevention of such risks are predictive analytics, anomaly detection, sentiment analysis, and credit scoring capabilities. The identified challenges in the implementation of AI are algorithm bias, data privacy concerns, regulatory compliance, and skill gaps. Improvement of the system in the future will enhance the efficiency of AI for use in digital financial platforms in various economic sectors in the world.

Acknowledgment

We would like to express our sincere gratitude to Mr. HUANG Shuoteng (Edwin Ng), a PhD candidate at aSSIST University, for his invaluable contributions throughout the development and writing of this article. Although Mr. Huang Shuoteng (Edwin Ng) is not listed as an author, his significant involvement in the selection of the research topic, literature review, and writing process was indispensable. His scholarly input, meticulous literature searches, and thoughtful contributions to the writing played a crucial role in the successful completion of this study.

Conflict of interest

The authors declare no conflict of interest.

References

1. M. Bouchetara, M. Zerouti, and A. R. Zouambi, "LEVERAGING ARTIFICIAL INTELLIGENCE (AI) IN PUBLIC SECTOR FINANCIAL RISK MANAGEMENT: INNOVATIONS, CHALLENGES, AND FUTURE DIRECTIONS," *EDPACS*, vol. 69, no. 9, pp. 124–144, Sep. 2024, doi: 10.1080/07366981.2024.2377351.
2. L. Vanneschi, D. M. Horn, and M. Castelli, "An artificial intelligence system for predicting customer default in e-commerce," *Expert Syst Appl*, vol. 104, no. 8, pp. 1–21, 2018.
3. X. Yu and Y. Peng, "Application and Challenges of Artificial Intelligence in Financial Risk Management," *Southern Finance*, no. 9, p. 5, 2017.
4. F. Butaru, Q. Chen, B. Clark, S. Das, A. W. Lo, and A. Siddique, "Risk and risk management in the credit card industry," *J Bank Financ*, vol. 72, pp. 218–239, Nov. 2016, doi: 10.1016/J.JBANKFIN.2016.07.015.
5. Y. Ma, H. Liu, G. Zhai, and Z. Huo, "Financial Risk Early Warning Based on Wireless Network Communication and the Optimal Fuzzy SVM Artificial Intelligence Model," *Wirel Commun Mob Comput*, vol. 2021, no. 1, p. 7819011, Jan. 2021, doi: 10.1155/2021/7819011.

6. X. Hua and Y. Huang, "Understanding China's fintech sector: development, impacts and risks," *European Journal of Finance*, vol. 27, no. 4–5, pp. 321–333, 2021, doi: 10.1080/1351847X.2020.1811131.
7. P. J. Morgan, "Assessing the Risks Associated with Green Digital Finance and Policies for Coping with Them," *Economics, Law, and Institutions in Asia Pacific*, pp. 51–68, 2022, doi: 10.1007/978-981-19-2662-4_3.
8. D. A. Zetsche, W. A. Birdthistle, D. W. Arner, and R. P. Buckley, "Digital Finance Platforms: Toward a New Regulatory Paradigm," *University of Pennsylvania Journal of Business Law*, vol. 23, 2020, Accessed: Jan. 10, 2025. [Online]. Available: <https://heinonline.org/HOL/Page?handle=hein.journals/upjlel23&id=277&div=&collection=>
9. M. Zhao, "Research on Financial Risk Assessment Based on Artificial Intelligence," *SHS Web of Conferences*, vol. 151, p. 01017, 2022, doi: 10.1051/SHSCONF/202215101017.
10. K. Du, F. Xing, R. Mao, and E. Cambria, "Financial Sentiment Analysis: Techniques and Applications," *ACM Comput Surv*, vol. 56, no. 9, p. 220, Oct. 2024, doi: 10.1145/3649451/ASSET/C6E561D5-EB82-4402-9140-444D133B3216/ASSETS/GRAPHIC/CSUR-2022-0579-F02.JPG.
11. Z. Jiang, D. Xu, and J. Liang, "A Deep Reinforcement Learning Framework for the Financial Portfolio Management Problem," Jun. 2017, Accessed: Jan. 10, 2025. [Online]. Available: <http://arxiv.org/abs/1706.10059>
12. S. W. K. Chan and M. W. C. Chong, "Sentiment analysis in financial texts," *Decis Support Syst*, vol. 94, pp. 53–64, Feb. 2017, doi: 10.1016/J.DSS.2016.10.006.
13. M. Kraus and S. Feuerriegel, "Decision support from financial disclosures with deep neural networks and transfer learning," *Decis Support Syst*, vol. 104, pp. 38–48, Dec. 2017, doi: 10.1016/j.dss.2017.10.001.
14. V. Siva and P. Nimmagadda, "AI-Powered Predictive Analytics for Credit Risk Assessment in Finance: Advanced Techniques, Models, and Real-World Applications," *Distributed Learning and Broad Applications in Scientific Research*, vol. 5, pp. 251–286, Jul. 2019, doi: 10.3115/v1/d14-1181.
15. K. R. Jammalamadaka and S. Itapu, "Responsible AI in automated credit scoring systems," *AI and Ethics* 2022 3:2, vol. 3, no. 2, pp. 485–495, Jun. 2022, doi: 10.1007/S43681-022-00175-3.
16. M. Faheem, "AI-Driven Risk Assessment Models: Revolutionizing Credit Scoring and Default Prediction," 2021, Accessed: Jan. 06, 2025. [Online]. Available: https://www.researchgate.net/profile/Muhammad-Ashraf-Faheem/publication/385074551_AI-Driven_Risk_Assessment_Models_Revolutionizing_Credit_Scoring_and_Default_Prediction/links/6713e02e035917754c09413e/AI-Driven-Risk-Assessment-Models-Revolutionizing-Credit-Scoring-and-Default-Prediction.pdf
17. V. Siva and P. Nimmagadda, "AI-Powered Predictive Analytics for Credit Risk Assessment in Finance: Advanced Techniques, Models, and Real-World Applications," *Distributed Learning and Broad Applications in Scientific Research*, vol. 5, pp. 251–286, Jul. 2019, doi: 10.3115/v1/d14-1181.
18. M. H. BARI, "A SYSTEMATIC LITERATURE REVIEW OF PREDICTIVE MODELS AND ANALYTICS IN AI-DRIVEN CREDIT SCORING," *SSRN Electronic Journal*, Oct. 2024, doi: 10.2139/SSRN.5050068.
19. C. Chen, K. Lin, C. Rudin, Y. Shaposhnik, S. Wang, and T. Wang, "An Interpretable Model with Globally Consistent Explanations for Credit Risk," Nov. 2018, Accessed: Jan. 09, 2025. [Online]. Available: <http://arxiv.org/abs/1811.12615>
20. P. Golbayani, D. Wang, and I. Florescu, "Application of Deep Neural Networks to assess corporate Credit Rating," Mar. 2020, Accessed: Jan. 09, 2025. [Online]. Available: <http://arxiv.org/abs/2003.02334>
21. L. Marceau, L. Qiu, N. Vandewiele, and E. Charton, "A comparison of Deep Learning performances with other machine learning algorithms on credit scoring unbalanced data," Jul. 2019, Accessed: Jan. 09, 2025. [Online]. Available: <http://arxiv.org/abs/1907.12363>
22. S. Shi, R. Tse, W. Luo, S. D'Addona, and G. Pau, "Machine learning-driven credit risk: a systemic review," *Neural Comput Appl*, vol. 34, no. 17, pp. 14327–14339, Sep. 2022, doi: 10.1007/S00521-022-07472-2/TABLES/6.
23. A. M. Rahmani, B. Rezazadeh, M. Haghparast, W. C. Chang, and S. G. Ting, "Applications of Artificial Intelligence in the Economy, Including Applications in Stock Trading, Market Analysis, and Risk Management," *IEEE Access*, vol. 11, pp. 80769–80793, 2023, doi: 10.1109/ACCESS.2023.3300036.
24. P. Cerchiello and P. Giudici, "Big data analysis for financial risk management," *J Big Data*, vol. 3, no. 1, pp. 1–12, Dec. 2016, doi: 10.1186/S40537-016-0053-4/FIGURES/3.
25. Q. Zhang, K. J. Wu, and M. L. Tseng, "Exploring Carry Trade and Exchange Rate toward Sustainable Financial Resources: An application of the Artificial Intelligence UKF Method," *Sustainability*, vol. 11, no. 12, p. 3240, 2019.
26. F. G. D. C. Ferreira, A. H. Gandomi, and R. T. N. Cardoso, "Artificial Intelligence Applied to Stock Market Trading: A Review," *IEEE Access*, vol. 9, pp. 30898–30917, 2021, doi: 10.1109/ACCESS.2021.3058133.
27. V. M. Sangala, S. Alamanda, and P. Tirumalareddy, "AI-Infused Finance: Predicting Stock Prices Through News and Market Data Analysis," *Lecture Notes in Networks and Systems*, vol. 1049 LNNS, pp. 390–403, 2024, doi: 10.1007/978-3-031-64779-6_38.

28. F. Alharbi and A. I. Al-Alawi, "Labor Market Prediction Using Machine Learning Methods: A Systematic Literature Review," 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems, ICETSSIS 2024, pp. 478–482, 2024, doi: 10.1109/ICETSSIS61505.2024.10459632.
29. D. Acemoglu, D. Autor, J. Hazell, and P. Restrepo, "Artificial intelligence and jobs: evidence from online vacancies," *J Labor Econ*, vol. 40, no. S1, pp. S293–S340, Apr. 2022, doi: 10.1086/718327.
30. O. Melnychenko, "Is Artificial Intelligence Ready to Assess an Enterprise's Financial Security?," *Journal of Risk and Financial Management* 2020, Vol. 13, Page 191, vol. 13, no. 9, p. 191, Aug. 2020, doi: 10.3390/JRFM13090191.
31. A. K. Mishra, S. Anand, N. C. Debnath, P. Pokhariyal, and A. Patel, "Artificial Intelligence for Risk Mitigation in the Financial Industry," *Artificial Intelligence for Risk Mitigation in the Financial Industry*, pp. 1–355, Jan. 2024, doi: 10.1002/9781394175574.
32. C. Maple et al., "The AI Revolution: Opportunities and Challenges for the Finance Sector," Aug. 2023, Accessed: Jan. 10, 2025. [Online]. Available: <https://arxiv.org/abs/2308.16538v1>
33. M. Ahmed Salamkar and S. J. Associate at Morgan Chase, "Real-time Analytics: Implementing ML algorithms to analyze data streams in real-time," *Journal of AI-Assisted Scientific Discovery*, vol. 3, no. 2, pp. 587–612, Sep. 2023, Accessed: Jan. 10, 2025. [Online]. Available: <https://scienceacadpress.com/index.php/jaasd/article/view/223>
34. V. Baulkaran and P. Jain, "Behavioral Biases of Financial Planners: The Case of Retirement Funding Recommendations," *Journal of Behavioral Finance*, 2024, doi: 10.1080/15427560.2024.2305412.
35. V. S. Athota, V. Pereira, Z. Hasan, D. Vaz, B. Laker, and D. Reppas, "Overcoming financial planners' cognitive biases through digitalization: A qualitative study," *J Bus Res*, vol. 154, p. 113291, Jan. 2023, doi: 10.1016/J.JBUSRES.2022.08.055.
36. C. Rastogi, Y. Zhang, D. Wei, K. R. Varshney, A. Dhurandhar, and R. Tomsett, "Deciding Fast and Slow: The Role of Cognitive Biases in AI-assisted Decision-making," *Proc ACM Hum Comput Interact*, vol. 6, no. CSCW1, Apr. 2022, doi: 10.1145/3512930.
37. R. K. Inampudi, T. Pichaimani, and Y. Surampudi, "AI-Enhanced Fraud Detection in Real-Time Payment Systems: Leveraging Machine Learning and Anomaly Detection to Secure Digital Transactions," *Australian Journal of Machine Learning Research & Applications*, vol. 2, no. 1, pp. 483–523, Mar. 2022, Accessed: Jan. 10, 2025. [Online]. Available: <https://sydneyacademics.com/index.php/ajmlra/article/view/189>
38. R. T. Potla, "AI in Fraud Detection: Leveraging Real-Time Machine Learning for Financial Security," *Journal of Artificial Intelligence Research and Applications*, vol. 3, no. 2, pp. 534–549, Oct. 2023, Accessed: Jan. 10, 2025. [Online]. Available: <https://aimlstudies.co.uk/index.php/jaira/article/view/189>
39. O. A. Bello, A. Ogundipe, D. Mohammed, F. Adebola, and O. A. Alonge, "AI-Driven Approaches for Real-Time Fraud Detection in US Financial Transactions: Challenges and Opportunities," 2023, Accessed: Jan. 10, 2025. [Online]. Available: <https://ejournals.org/ejcsit/>
40. J. Rashid, T. Mahmood, M. W. Nisar, and T. Nazir, "Phishing Detection Using Machine Learning Technique," *Proceedings - 2020 1st International Conference of Smart Systems and Emerging Technologies, SMART-TECH 2020*, pp. 43–46, Nov. 2020, doi: 10.1109/SMART-TECH49988.2020.00026.
41. O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," *Expert Syst Appl*, vol. 117, pp. 345–357, Mar. 2019, doi: 10.1016/J.ESWA.2018.09.029.
42. M. Noor and U. Milon, "Gravitating towards Artificial Intelligence on Anti-Money Laundering A PRISMA Based Systematic Review," *International Journal of Religion*, vol. 5, no. 7, pp. 303–315, May 2024, doi: 10.61707/PY0FE669.
43. L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, and T. Newe, "Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review," *Sensors* 2023, Vol. 23, Page 1151, vol. 23, no. 3, p. 1151, Jan. 2023, doi: 10.3390/S23031151.
44. O. O. Adeyelu, C. E. Ugochukwu, and M. A. Shonibare, "AUTOMATING FINANCIAL REGULATORY COMPLIANCE WITH AI: A REVIEW AND APPLICATION SCENARIOS," *Finance & Accounting Research Journal*, vol. 6, no. 4, pp. 580–601, Apr. 2024, doi: 10.51594/FARJ.V6I4.1035.
45. S. Patel and A. Rahman, "Data Privacy in the Digital Age: Navigating Compliance and Ethical Challenges," *Baltic Multidisciplinary Research Letters Journal*, vol. 1, no. 3, pp. 13–24, Nov. 2024, Accessed: Jan. 10, 2025. [Online]. Available: <https://www.bmlrj.com/index.php/Baltic/article/view/21>
46. D. Banciu and C. E. Cirnu, "AI Ethics and Data Privacy compliance," 2022 14th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2022, 2022, doi: 10.1109/ECAI54874.2022.9847510.
47. S. Gupta, S. Bagga, and D. K. Sharma, "Intelligent Data Analysis," *Intelligent Data Analysis*, pp. 1–15, Jun. 2020, doi: 10.1002/9781119544487.CH1.
48. G. Deipenbrock, "Artificial intelligence and machine learning in the financial sector: Legal-methodological challenges of steering towards a regulatory 'whitebox,'" *Routledge Handbook of Financial Technology and Law*, pp. 3–26, Jan. 2021, doi: 10.4324/9780429325670-1/ARTIFICIAL-INTELLIGENCE-MACHINE-LEARNING-FINANCIAL-SECTOR-GUDULA-DEIPENBROCK.

49. P. Wirawan, "Leveraging Predictive Analytics in Financing Decision-Making for Comparative Analysis and Optimization," *Advances in Management & Financial Reporting*, vol. 1, no. 3, pp. 157–169, Sep. 2023, doi: 10.60079/AMFR.V1I3.209.
50. T. D. Olorunyomi, I. C. Okeke, O. G. Ejike, and A. G. Adeleke, "Using Fintech innovations for predictive financial modeling in multi-cloud environments," *Computer Science & IT Research Journal*, vol. 5, no. 10, pp. 2357–2370, 2024.
51. F. Ekundayo, I. Atoyebi, A. Soyele, and E. Ogunwobi, "Predictive Analytics for Cyber Threat Intelligence in Fintech Using Big Data and Machine Learning," *Int J Res Publ Rev*, vol. 5, no. 11, pp. 1–15, 2024.
52. A. O. Abhulimen, E. E. Agu, A. Nkemchor Obiki-Osafiele, O. S. Osundare, I. A. Adeniran, and C. P. Efunniyi, "4 Nigeria Inter-bank Settlement System Plc (NIBSS). 5 International Association of Computer Analysts and Researchers," *UK. International Journal of Frontline Research in Multidisciplinary Studies*, vol. 2024, no. 02, pp. 20–029, 2024, doi: 10.56355/ijfrms.2024.3.2.0026.
53. B. Jadhav, A. Kulkarni, P. Kulkarni, and S. Kulkarni, "Artificial Intelligence and Big Data Analytics in Digital Gig Finance," *Synergy of AI and Fintech in the Digital Gig Economy*, pp. 96–108, Sep. 2024, doi: 10.1201/9781032720104-6.
54. A. Khang, B. Jadhav, V. Abdullayev Hajimahmud, and I. Satpathy, "Synergy of AI and Fintech in the Digital Gig Economy," *Synergy of AI and Fintech in the Digital Gig Economy*, Aug. 2024, doi: 10.1201/9781032720104/SYNERGY-AI-FINTECH-DIGITAL-GIG-ECONOMY.
55. Y. Liang, D. Quan, F. Wang, X. Jia, M. Li, and T. Li, "Financial big data analysis and early warning platform: A case study," *IEEE Access*, vol. 8, pp. 36515–36526, 2020, doi: 10.1109/ACCESS.2020.2969039.
56. N. R. Boinapalli, "AI-Driven Predictive Analytics for Risk Management in Financial Markets," *Silicon Valley Tech Review*, vol. 2, no. 1, pp. 41–53, 2023.
57. A. Zainal, "Role of Artificial Intelligence and Big Data Technologies in Enhancing Anomaly Detection and Fraud Prevention in Digital Banking Systems," *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, vol. 7, no. 12, pp. 1–10, Dec. 2023, Accessed: Jan. 06, 2025. [Online]. Available: <https://theaffine.com/index.php/IJACSTA/article/view/2023-12-04>
58. S. R. Gayam, "AI-Driven Fraud Detection in E-Commerce: Advanced Techniques for Anomaly Detection, Transaction Monitoring, and Risk Mitigation," *Distributed Learning and Broad Applications in Scientific Research*, vol. 6, pp. 124–151, Nov. 2020, Accessed: Jan. 06, 2025. [Online]. Available: <https://dlabi.org/index.php/journal/article/view/108>
59. S. Dixit, "Advanced Generative AI Models for Fraud Detection and Prevention in FinTech: Leveraging Deep Learning and Adversarial Networks for Real-Time Anomaly Detection in Financial Transactions," *Journal of Artificial Intelligence Research*, vol. 4, no. 2, pp. 51–77, Oct. 2024, Accessed: Jan. 06, 2025. [Online]. Available: <https://nucleuscorp.org/JAIR/article/view/402>
60. S. Agrawal, "Enhancing Payment Security Through AI-Driven Anomaly Detection and Predictive Analytics," *International Journal of Sustainable Infrastructure for Cities and Societies*, vol. 7, no. 2, pp. 1–14, Apr. 2022, Accessed: Jan. 06, 2025. [Online]. Available: <https://vectoral.org/index.php/IJSICS/article/view/99>
61. J. Liu, F. Xu, and X. Liu, "Financial Market Sentiment Analysis and Investment Strategy Formulation Based on Social Network Data," *J. Electrical Systems*, vol. 20, no. 9, pp. 655–660, 2024.
62. N. R. Mitta, "Leveraging Natural Language Processing (NLP) for AI-Based Sentiment Analysis in Financial Markets: Real-Time Insights for Trading Strategies and Risk Management," *African Journal of Artificial Intelligence and Sustainable Development*, vol. 3, no. 2, pp. 398–434, Dec. 2023, Accessed: Jan. 06, 2025. [Online]. Available: <https://africansciencegroup.com/index.php/AJAISD/article/view/209>
63. S. García-Méndez, F. de Arriba-Pérez, A. Barros-Vila, and F. J. González-Castaño, "Targeted aspect-based emotion analysis to detect opportunities and precaution in financial Twitter messages," *Expert Syst Appl*, vol. 218, p. 119611, May 2023, doi: 10.1016/J.ESWA.2023.119611.
64. S. G. Anton and A. E. A. Nucu, "Firm value and corporate cash holdings. Empirical evidence from the Polish listed firms," *E a M: Economie a Management*, vol. 22, no. 3, pp. 121–134, 2019, doi: 10.15240/TUL/001/2019-3-008.
65. K. B. Hansen and C. Borch, "Alternative data and sentiment analysis: Prospecting non-standard data in machine learning-driven finance," <https://doi.org/10.1177/20539517211070701>, vol. 9, no. 1, Jan. 2022, doi: 10.1177/20539517211070701.
66. C. Xiang, J. Zhang, F. Li, H. Fei, and D. Ji, "A semantic and syntactic enhanced neural model for financial sentiment analysis," *Inf Process Manag*, vol. 59, no. 4, p. 102943, Jul. 2022, doi: 10.1016/J.IPM.2022.102943.
67. M. A. Faheem, "AI-Driven Risk Assessment Models: Revolutionizing Credit Scoring and Default Prediction," 2021.
68. F. Doshi-Velez and B. Kim, "Towards A Rigorous Science of Interpretable Machine Learning," Feb. 2017, Accessed: Jan. 10, 2025. [Online]. Available: <http://arxiv.org/abs/1702.08608>

69. S. Putha, "AI-Enabled Predictive Analytics for Enhancing Credit Scoring Models in Banking," *Journal of Artificial Intelligence Research and Applications*, vol. 1, no. 1, pp. 290–330, Feb. 2021, Accessed: Jan. 09, 2025. [Online]. Available: <https://aimlstudies.co.uk/index.php/jaira/article/view/200>
70. M. T. Ribeiro, S. Singh, and C. Guestrin, "'Why should i trust you?' Explaining the predictions of any classifier," *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, vol. 13-17-August-2016, pp. 1135–1144, Aug. 2016, doi: 10.1145/2939672.2939778.
71. H. Cramer, J. Garcia-Gathright, A. Springer, and S. Reddy, "Assessing and addressing algorithmic bias in practice," *Interactions*, vol. 25, no. 6, pp. 58–63, Nov. 2018, doi: 10.1145/3278156.
72. D. Roselli, J. Matthews, and N. Talagala, "Managing bias in AI," *The Web Conference 2019 - Companion of the World Wide Web Conference, WWW 2019*, pp. 539–544, May 2019, doi: 10.1145/3308560.3317590.
73. L. H. Nazer et al., "Bias in artificial intelligence algorithms and recommendations for mitigation," *PLOS Digital Health*, vol. 2, no. 6, p. e0000278, Jun. 2023, doi: 10.1371/JOURNAL.PDIG.0000278.
74. A. Oseni, N. Moustafa, H. Janicke, P. Liu, Z. Tari, and A. Vasilakos, "Security and Privacy for Artificial Intelligence: Opportunities and Challenges," Feb. 2021, Accessed: Jan. 10, 2025. [Online]. Available: <http://arxiv.org/abs/2102.04661>
75. K. R. Gade, "Data Analytics: Data Privacy, Data Ethics, Data Monetization," *MZ Computing Journal*, vol. 1, no. 1, Apr. 2020, Accessed: Jan. 10, 2025. [Online]. Available: <https://mzjournal.com/index.php/MZCJ/article/view/409>
76. N. I. Qureshi, S. S. Choudhuri, Y. Nagamani, R. A. Varma, and R. Shah, "Ethical Considerations of AI in Financial Services: Privacy, Bias, and Algorithmic Transparency," *2024 International Conference on Knowledge Engineering and Communication Systems, ICKECS 2024*, 2024, doi: 10.1109/ICKECS61492.2024.10616483.
77. V. Bharath Munagandla, S. Surya, V. Dandyala, and B. Chandra Vadde, "The Future of Data Analytics: Trends, Challenges, and Opportunities," *Revista de Inteligencia Artificial en Medicina*, vol. 13, no. 1, pp. 421–442, Nov. 2022, Accessed: Jan. 10, 2025. [Online]. Available: <https://redcrevistas.com/index.php/Revista/article/view/171>
78. L. Pham, B. O'Sullivan, T. Scantamburlo, and T. Mai, "Addressing Digital and AI Skills Gaps in European Living Areas: A Comparative Analysis of Small and Large Communities," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 38, no. 21, pp. 23119–23127, Mar. 2024, doi: 10.1609/AAAI.V38I21.30357.