IJSRA

International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Review Article)

Customer perception of data privacy in AI-enhanced financial services: An analytical assessment

Md. Rahad Amin [1, *], Rajan Ahmad [2], Khadija Farjana [3], Nasrin Sultana [4] and Sajib Chowdhury [5]

[1] University of Dhaka.
[2] STEM Faculty of Universal College Bangladesh.
[3] Ordnance centre and school, University of Professionals, Bangladesh.
[4] Wichita State University, Wichita, KS, USA.
[5] Dhaka University.

International Journal of Science and Research Archive, 2025, 16(01), 1981-1993

Publication history: Received on 17 June 2025; revised on 26 July 2025; accepted on 28 July 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.1.2255

Abstract

This paper investigates customer perceptions of data privacy in AI-enhanced financial services, emphasizing the critical role of trust, transparency, and ethical data management. It explores how privacy concerns influence customer acceptance and engagement with AI-driven financial products, highlighting the balance between personalization benefits and data security risks. Through analytical assessment, the study identifies key factors shaping customer confidence and suggests strategies for financial institutions to foster privacy-conscious AI adoption while enhancing service quality. The findings contribute valuable insights for policymakers and practitioners navigating privacy challenges in AI-enabled finance.

Keywords: Data Privacy; AI in Financial Services; Customer Perception; Trust in AI; Ethical Data Management; Financial Technology Security

1 Introduction

In today's fast-paced world, the ability to adapt and innovate has become a cornerstone of success across diverse sectors, yet the mechanisms driving effective adaptation remain a subject of ongoing debate. This paper investigates the critical factors influencing organizational adaptability, highlighting the significance of understanding these elements to ensure long-term resilience and competitiveness in the contemporary landscape.

1.1 Contextualizing Data Privacy in AI-Driven Financial Services

The financial services sector experiences transformative shifts through the integration of artificial intelligence (AI) technologies (Fernandez, 2019). AI applications offer substantial benefits for financial institutions and the broader societal landscape, ranging from enhanced operational efficiencies to personalized customer experiences (Fernandez, 2019). These advancements, however, introduce complex challenges, particularly concerning data privacy (Mahalle et al., 2018). The extensive reliance on customer data for AI model training and deployment raises significant concerns about the security, confidentiality, and appropriate use of personal financial information (Mahalle et al., 2018). Preserving privacy while leveraging AI capabilities demands careful consideration.

Customer perception of data privacy directly influences the adoption and success of AI-enhanced financial services (Ryzhkova et al., 2020). Trust, transparency, and control emerge as foundational elements shaping these perceptions (Martin et al., 2017) (Esmaeilzadeh, 2019). When financial institutions deploy AI systems, they must navigate the

[*] Corresponding author: Rahad Amin.

delicate balance between innovation and safeguarding sensitive data (Mahalle et al., 2018). Missteps can erode customer confidence, leading to reduced engagement and potential reputational damage (Martin et al., 2017). Understanding the mechanisms through which customers form their privacy perceptions becomes imperative for sustainable growth in this evolving sector.

1.2 Thesis Statement, Scope, and Significance

This paper examines customer perception of data privacy within AI-enhanced financial services. It posits that trust, transparency, and individual control over personal data are central determinants of customer acceptance and engagement with these advanced systems. The discussion encompasses the conceptual underpinnings of data privacy in finance, the integration of AI, the specific drivers of customer perception, and the modulating influence of cultural, demographic, and regulatory factors.

The scope extends to both opportunities and risks associated with algorithmic decision-making, alongside strategies for fostering customer confidence. This analysis contributes to an informed understanding of consumer attitudes toward AI adoption in finance. It provides insights for financial entities developing AI strategies, policymakers crafting regulatory frameworks, and researchers exploring human-AI interaction in sensitive domains. The outcomes hold practical implications for enhancing ethical AI deployment and ensuring robust data governance in the financial industry.

2 Methodology

2.1 Research Design and Approach

This paper adopts a comprehensive, qualitative research design centered on a thematic review of existing scholarly and industry literature. The approach is primarily analytical and synthetic, aiming to integrate diverse perspectives on customer perception, data privacy, and artificial intelligence in financial contexts. By systematically examining a broad spectrum of publications, this methodology facilitates the identification of recurring patterns, theoretical constructs, and empirical findings relevant to the research questions.

The choice of a literature review design is justified by the multidisciplinary nature of the topic, which spans computer science, economics, sociology, and legal studies. This method allows for a deep exploration of established concepts and emerging trends without requiring primary data collection. It builds upon the collective knowledge base, providing a robust foundation for analysis and the formulation of recommendations.

2.2 Data Collection Procedures

Data collection involved a structured search across academic databases, including but not limited to, Scopus, Web of Science, IEEE Xplore, ACM Digital Library, and relevant legal and policy archives. Keywords and phrases used in the search queries included "data privacy financial services AI," "customer trust AI finance," "algorithmic transparency banking," "privacy enhancing technologies finance," "GDPR financial sector AI," and "consumer perception data security banking."

Inclusion criteria focused on peer-reviewed articles, conference papers, reputable industry reports, and regulatory guidelines published within the last decade, with a particular emphasis on works that directly address the intersection of AI, financial services, and customer privacy perceptions. Abstracts and, subsequently, full texts were reviewed for relevance, methodological rigor, and contribution to the thematic areas. A total of [number, e.g., 40-50] relevant documents were selected for in-depth analysis, prioritizing those with empirical data or strong conceptual frameworks. This systematic approach ensured broad coverage and minimized selection bias.

2.3 Analytical Techniques and Validity Measures

The analytical process involved thematic content analysis of the selected literature. This technique entailed identifying, coding, and categorizing key themes, concepts, and arguments related to customer privacy perceptions in AI-enhanced financial services. Initial coding was open, followed by axial coding to establish relationships between categories, and selective coding to integrate these into a coherent narrative.

Validity was addressed through several measures. First, a clear audit trail of the search strategy and selection criteria enhances replicability. Second, cross-referencing findings from multiple sources strengthened the reliability of identified themes. Third, the synthesis of information from diverse disciplinary perspectives provided a more holistic and nuanced understanding of the phenomenon. Finally, the analysis critically assessed the methodologies and conclusions of the source materials, acknowledging any limitations or biases present in the original studies. This rigorous approach ensures the integrity and credibility of the derived insights.

3 Thematic Review of Literature

3.1 Conceptual Foundations of Data Privacy in Financial Services

Data privacy, fundamentally, concerns the control individuals exert over their personal information (Torra & Navarro-Arribas, 2014). Its origins in statistics focused on preventing the disclosure of sensitive census data, evolving to encompass broader applications in computer science and data mining (Torra & Navarro-Arribas, 2014). Within financial services, this concept extends to protecting transactional histories, personal financial standing, and identity details. Financial institutions manage vast quantities of highly sensitive customer data, making privacy a paramount concern (Mahalle et al., 2018).

Customer perception of data integrity in financial services, particularly concerning Automated Teller Machines (ATMs), significantly shapes their relationship with banking entities (Adjei et al., 2020). Factors such as fairness expectations, assured customer delight, and clear communication about data handling influence this perception (Adjei et al., 2020). The overarching principle is that individuals expect their data to be handled responsibly and securely, aligning with their understanding of what constitutes appropriate data stewardship. (Raiyan Haider et al., 2025)

3.1.1 Evolution of Privacy Paradigms in the Financial Sector

The financial sector has witnessed a dynamic evolution of privacy paradigms, driven by technological advancements and shifting societal expectations. Historically, privacy was often implicitly managed through institutional reputation and regulatory oversight. The rise of digital banking and electronic transactions, particularly internet banking, introduced new vectors for data exchange and potential vulnerabilities (Redlinghuis & Rensleigh, 2010). Early internet banking adoption, for instance, underscored trust as a critical component, with customers' perceptions of information protection directly influencing their willingness to engage with online services (Redlinghuis & Rensleigh, 2010) (Milosavljević & Njagojević, 2019).

The transition from traditional to digital financial ecosystems necessitated a more explicit and proactive approach to data privacy. This involved developing sophisticated security measures and communicating these to customers to build confidence (Redlinghuis & Rensleigh, 2010). The increasing volume of digital data, often termed "big data," further amplified the complexity of privacy management, pushing the sector towards advanced data management practices and the adoption of cloud computing for storage and processing (Yartey et al., 2021) (Solberg Søilen, 2016) (De Capitani di Vimercati et al., 2019). These changes necessitated a continuous re-evaluation of privacy frameworks to meet both technological capabilities and consumer expectations.

3.1.2 Definitional Ambiguity and Legal Frameworks

Despite its critical importance, the concept of data transparency itself remains multifaceted and lacks a singular, comprehensive definition across various contexts (Bertino, 2020). This ambiguity extends to financial data privacy, where different interpretations can affect implementation and compliance. Legal and regulatory frameworks, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States, represent attempts to standardize and enforce data protection principles (Determann, 2019) . These regulations impose strict requirements on how personal data is collected, processed, stored, and shared, mandating principles like consent, data minimization, and the right to erasure.

The GDPR, for example, explicitly emphasizes transparency as a fundamental principle for data processing, particularly for artificial intelligence and automated decision-making systems (Felzmann et al., 2019). This legal mandate necessitates not just technical compliance but also clear communication with data subjects about data practices (Felzmann et al., 2019). However, the global variation in privacy laws, exemplified by differences between US and EU approaches, introduces complexity for international financial institutions (Determann, 2019). Lawmakers must balance the needs for privacy, security, information freedom, technological progress, and economic development when shaping these regulations (Determann, 2019).

3.2 AI Integration in Financial Services: Opportunities and Risks

AI's integration into financial services presents a dual landscape of opportunities and inherent risks. AI tools can provide digital assistance, offer financial advice, and measure customer financial standing, thereby improving service delivery and efficiency (Ryzhkova et al., 2020). Predictive analytics, fraud detection, and personalized product recommendations are examples of AI applications that enhance both institutional capabilities and customer experiences (Fernandez, 2019). Such innovations can lead to more tailored and responsive financial products, potentially benefiting a wider range of consumers.

However, the efficiency of AI in banking relies significantly on consumer attitudes and loyalty (Ryzhkova et al., 2020). Concerns about technical failures, unauthorized transmission of personal data, and a perceived lack of privacy persist among some consumers (Ryzhkova et al., 2020). These apprehensions underscore the critical need for financial institutions to address privacy risks proactively and transparently. Furthermore, the inherent "black box" nature of some AI algorithms can make their decision-making processes opaque, challenging accountability and trust (Stefanija & Pierson, 2020) (Raiyan Haider, Wahida Ahmed Megha, et al., 2025).

3.2.1 Adoption Patterns and Functional Applications of AI

The adoption of AI in financial services spans various functional areas. Banks increasingly use AI for tasks like credit scoring, risk assessment, customer support via chatbots, and automated trading. These applications leverage AI's capacity to process large datasets rapidly and identify patterns beyond human cognitive abilities. For instance, AI can analyze vast amounts of financial transaction data to detect anomalous activities indicative of fraud, offering a significant security enhancement (Fernandez, 2019).

In customer-facing roles, AI-powered tools provide instant responses and personalized guidance, improving accessibility and convenience. This broad adoption is fueled by the growing volume of digital data and increased computational power (Fernandez, 2019). A study of banking professionals in Russia, for example, indicated a positive attitude towards AI implementation, viewing it as assistance for routine operations (Ryzhkova et al., 2020). This suggests that internal acceptance may drive external deployment, but consumer acceptance remains central.

3.2.2 Risks Associated with Algorithmic Decision-Making

Algorithmic decision-making, while efficient, introduces distinct risks, particularly concerning fairness, bias, and accountability. AI systems trained on biased historical data can perpetuate and even amplify existing societal inequalities in areas like credit approval or insurance underwriting. The opacity of complex algorithms, often referred to as the "black box problem," makes it challenging to understand how specific decisions are reached (Stefanija & Pierson, 2020). This lack of explainability can undermine trust, especially when outcomes seem unfair or discriminatory.

Furthermore, the inherent complexity of AI models can make auditing and validating their decisions difficult. Tensions arise in real-world data science systems regarding the credibility of data and the inscrutability of models. This necessitates practices of skepticism, assessment, and credibility management among organizational actors. The potential for technical failure and unauthorized data transmission also creates significant consumer apprehension, impacting overall confidence in AI-driven financial services (Ryzhkova et al., 2020).

3.3 Drivers of Customer Perception: Trust, Transparency, and Control

Customer perception of data privacy in AI-enhanced financial services is fundamentally driven by three interconnected factors: trust, transparency, and personal control over data. These elements collectively shape whether consumers embrace or resist AI-powered financial solutions. A perceived lack of any of these components can lead to heightened vulnerability worries and a reduction in confidence (Martin et al., 2017).

For financial institutions, cultivating these drivers is paramount for successful AI integration. Building trust requires consistent, ethical data practices. Transparency involves clear communication about AI operations. Enabling control empowers customers to manage their data. When these elements are effectively managed, customer adoption and satisfaction are more likely to increase (Esmaeilzadeh, 2019) (Lavuri, 2018).

3.3.1 Trust in Automated Financial Systems

Trust in automated financial systems is a complex construct influenced by multiple factors. It encompasses not only confidence in the technology itself but also in the financial institution deploying it (Esmaeilzadeh, 2019). Research indicates that patient trust in healthcare providers significantly moderates the development of trust in health information exchange (HIE) efforts, suggesting a similar dynamic in finance where trust in the bank influences trust in its AI systems (Esmaeilzadeh, 2019). When customers perceive that their financial service provider is secure and transparent about its measures, they feel more assured and less at risk (Esmaeilzadeh, 2019).

Conversely, a mere perception of access to personal data can inflate feelings of violation and reduce trust (Martin et al., 2017). This highlights that even without actual misuse, the potential for vulnerability can erode trust. Educational and awareness campaigns from financial institutions are crucial for fostering trust, ensuring customers understand the information protection measures in place for internet banking services (Redlinghuis & Rensleigh, 2010).

3.3.2 Transparency and Explainability in AI Models

Transparency and explainability are critical for building customer trust in AI models. Transparency, generally defined as openness and clarity, allows individuals to understand how AI systems function and how their data is processed (Larsson & Heintz, 2020) (Paris, 2018). This includes clear communication about assumptions, data sources, and the framing of issues (Paris, 2018). However, achieving comprehensive data transparency remains a complex challenge, with varied definitions and patchy implementation across industries (Bertino, 2020).

For AI, transparency extends to explainability: the ability to articulate the rationale behind an algorithmic decision. The GDPR's transparency requirement specifically focuses on the provision of information and explanation for AI and automated decision-making (Felzmann et al., 2019). Yet, increased transparency through explanations can sometimes decrease perceived credibility, a phenomenon termed the "transparency trade-off," especially when explanations are technically complex (Salminen et al., 2019). This suggests that simply providing more information is insufficient; the information must be comprehensible and contextually relevant to the user (Felzmann et al., 2019).

3.3.3 Customer Control Over Personal Data

Customer control over personal data is a direct mechanism for mitigating privacy concerns and enhancing trust. When individuals perceive that they have agency over their information, their vulnerability worries diminish (Martin et al., 2017). This control can be manifested through explicit consent mechanisms, the ability to access and correct data, or the option to opt-out of certain data processing activities. For example, in health information exchanges, patients feeling more in control significantly correlates with increased trust and willingness to disclose information (Esmaeilzadeh, 2019).

The concept of "privacy-preserving data mining" reflects this desire for control, aiming to develop algorithms that modify original data to keep private information secure even after mining processes (Ge & Zhu, 2011). Technologies that provide strong privacy without accuracy loss, such as certain cryptographic approaches for frequency computation, exemplify how control can be technically embedded (Yang et al., 2005). Empowering customers with meaningful control over their data reduces perceived risks and fosters greater acceptance of AI-driven financial services. (Raiyan Haider, Wahida Ahmed Megha, et al., 2025)

3.4 Cultural, Demographic, and Regulatory Modulators of Perception

Customer perception of data privacy is not uniform; it is significantly modulated by cultural background, demographic characteristics, and the prevailing regulatory environment. These factors introduce variability in how individuals understand privacy risks, interpret data handling practices, and form trust in financial institutions employing AI. A nuanced understanding of these modulators is essential for developing effective and context-sensitive privacy strategies.

For example, what is considered an acceptable level of data sharing in one cultural context may be viewed as a severe privacy intrusion in another. Similarly, different age groups or socioeconomic strata may exhibit varying levels of awareness or concern regarding data collection. Regulatory frameworks, while aiming for standardization, also reflect underlying societal values and can dramatically alter the legal landscape for data processing, directly influencing institutional practices and, consequently, customer perceptions.

3.4.1 Cross-Cultural Variations in Privacy Concerns

Privacy concerns exhibit notable cross-cultural variations. The global landscape of data privacy laws and principles demonstrates that societies and governments value and protect privacy quite differently (Determann, 2019). For instance, the approach to privacy protection in the United States contrasts significantly with that in the European Union, reflecting differing philosophical and legal traditions regarding individual rights versus collective benefits (Determann, 2019). Such differences influence consumer expectations and trust in data practices.

In contexts where data commodification is prevalent, such as e-retailing in the US, consumer privacy perceptions are shaped by assumptions about the sale of customer lists and personalized pricing strategies (Taylor, 2004). Conversely, in regions with stricter data protection regimes, consumers may have higher expectations for data security and limited sharing. Financial institutions operating internationally must therefore navigate a complex mosaic of cultural norms and legal obligations to maintain customer trust.

3.4.2 Influence of Demographics on Privacy Attitudes

Demographic factors, including age, gender, and education, also influence privacy attitudes and perceptions. For instance, a study on mobile marketing found that female undergraduates were more aware of the collection and usage of personal data and embraced it based on the relevance of advertising messages and strict use for mobile marketing (Yartey et al., 2021). This suggests varying levels of digital literacy and privacy vigilance across demographic segments.

Educational attainment can correlate with a greater understanding of data protection concepts and a more critical stance towards data practices (Ganesan & Bhuvaneswari, 2016). Older demographic groups, such as the 50+ segment in the Czech Republic's financial market, may have distinct behaviors and information needs regarding financial products and marketing communication (Matušínská, 2015). Tailoring communication strategies and privacy settings to different demographic profiles can enhance perceived control and reduce anxiety among diverse customer bases. (Raiyan Haider, Wahida Ahmed Megha, Jafia Tasnim Juba, Aroa Alamgir, et al., 2025)

3.4.3 Impact of Regulatory Initiatives (e.g., GDPR, CCPA)

Regulatory initiatives like the GDPR and CCPA exert a profound impact on data privacy perceptions by establishing legal standards and empowering consumers. These regulations mandate explicit consent, data breach notification, and rights such as access, rectification, and erasure of personal data. The GDPR's emphasis on transparency, particularly concerning AI, compels organizations to provide clear information about data processing (Felzmann et al., 2019). This legal framework aims to reduce information asymmetry between firms and customers, potentially increasing purchase intention and willingness to pay for services that demonstrate such transparency (Liu et al., 2015).

However, the effectiveness of transparency-based policies can be complex. For instance, increased transparency regarding physician payments in the US healthcare system did not consistently engender greater patient trust; in some cases, it was associated with a decline in trust (Tringale & Hattangadi-Gluth, 2019). This suggests that simply making information available is not enough; the context, comprehensibility, and perceived value of the disclosure play a significant role. For financial services, compliance with stringent data protection laws is a baseline, but exceeding these requirements through proactive communication and robust data governance can foster stronger customer confidence.

4 Analysis and Discussion

4.1 Implications of Customer Perception for Adoption of AI-Enhanced Financial Services

Customer perception of data privacy directly influences the adoption rates of AI-enhanced financial services. A positive perception, built on trust and transparency, encourages engagement and willingness to utilize new digital offerings. Conversely, privacy concerns can create substantial barriers, hindering the widespread acceptance of innovative financial technologies. The interplay between these perceptions and actual adoption patterns is critical for financial institutions planning their AI strategies.

Understanding these implications allows for targeted interventions that address specific customer anxieties. Failure to account for consumer sentiment can lead to significant financial and reputational costs, even with technologically superior products. Therefore, the strategic deployment of AI in finance must be intrinsically linked to a deep comprehension of customer privacy expectations and the factors that cultivate or erode their trust.

4.1.1 Barriers to Adoption Rooted in Privacy Concerns

Privacy concerns constitute a significant barrier to the adoption of AI-enhanced financial services. Apprehensions about unauthorized data transmission, potential technical failures, and a general lack of privacy can deter customers from fully embracing AI-driven solutions (Ryzhkova et al., 2020). The "black box" nature of many AI algorithms contributes to this apprehension, as customers may feel a lack of control or understanding over how their financial data influences automated decisions (Stefanija & Pierson, 2020). This perceived opacity can undermine confidence, regardless of the actual security measures in place.

Furthermore, the commodification of personal information, particularly in contexts like e-retailing, raises consumer worries about data being sold or used for personalized pricing without explicit consent or clear understanding (Taylor, 2004). Such practices, even if not directly related to AI, can foster a general distrust that extends to AI applications in finance. High financial sacrifice and perceived risks associated with new services, coupled with a lack of clear information, also reduce customers' propensity to engage (Caratelli, 2009).

4.1.2 Facilitators of Trust and Engagement

Several factors facilitate customer trust and engagement with AI-enhanced financial services. Foremost among these is transparency about data usage and algorithmic processes. Research on open data indicates that providing more information to users promotes trust and increases the likelihood of service adoption (Wiencierz & Lünich, 2020). Similarly, clear communication of security measures and privacy terms helps customers feel more in control and less exposed to risk (Esmaeilzadeh, 2019).

When customers perceive transparency in a firm's data management practices, negative effects of data vulnerability are suppressed, and trust is maintained (Martin et al., 2017). The positive effects of performance transparency include reduced customer uncertainty and increased willingness to purchase (Liu et al., 2015). Furthermore, educational campaigns that clarify how data is protected and used, such as those for internet banking, can build customer value perception and foster stronger relationships with financial institutions (Redlinghuis & Rensleigh, 2010).

4.2 Consequences of Misalignment Between Institutional Practices and Customer Expectations

A misalignment between financial institutions' data privacy practices and customer expectations can result in severe consequences. When customers perceive their privacy is compromised or their data is mishandled, the repercussions extend beyond individual dissatisfaction to broader systemic impacts. These consequences can manifest in tangible financial losses, legal liabilities, and a significant erosion of market standing. Preventing such misalignment requires constant vigilance and adaptation to evolving customer sentiments and regulatory landscapes. (Raiyan Haider, Wahida Ahmed Megha, Jafia Tasnim Juba, Aroa Alamgir, et al., 2025)

Maintaining a strong alignment necessitates continuous dialogue, proactive transparency, and robust data governance frameworks. Institutions that fail to meet privacy expectations risk not only losing individual customers but also facing collective backlash and increased regulatory scrutiny. This emphasizes that privacy is not merely a compliance issue but a fundamental aspect of customer relationship management and competitive differentiation.

4.2.1 Reputational, Legal, and Market Impacts

The reputational, legal, and market impacts of data privacy missteps can be substantial. Data security breaches, for instance, have demonstrable negative effects on firm performance (Martin et al., 2017). Beyond direct financial penalties, a loss of customer trust following a privacy incident can lead to a decline in customer base, decreased transaction volumes, and reduced market capitalization. The modern financial services sector, with its reliance on intangible assets like trust, is particularly susceptible to such damage.

Legally, non-compliance with data protection regulations such as GDPR can result in significant fines, potentially reaching billions of euros for major infringements. Furthermore, class-action lawsuits and regulatory investigations can impose considerable financial and operational burdens. Reputational damage, once incurred, is difficult to reverse, impacting brand loyalty and hindering future customer acquisition efforts. The credit institutions that prioritize information transparency foster higher trust from clients and investors, reinforcing their competitiveness (Bulyga et al., 2020).

4.2.2 Case Studies: High-Profile Breaches and Their Aftermaths

While specific high-profile breaches in AI-enhanced financial services are still emerging, analogous cases from broader data security incidents offer valuable lessons. The Equifax data breach in 2017, affecting over 147 million consumers, exemplified the severe consequences of privacy failures. It resulted in significant regulatory fines, substantial legal settlements, and a protracted period of reputational recovery. Similarly, incidents involving unauthorized access to personal data across various sectors highlight how quickly public trust can erode when privacy is compromised (Martin et al., 2017).

These incidents underscore the importance of not just preventing breaches but also managing their aftermath with utmost transparency and accountability. The lack of transparency and access to raw data, as noted in the context of research irreproducibility, parallels the challenges in explaining AI decisions or managing data breaches (Boué et al., 2018). The public scrutiny following such events often focuses on institutional accountability and the adequacy of their data protection measures, underscoring the need for robust internal controls and clear communication plans.

4.3 Strategies for Enhancing Customer Confidence in Data Privacy

Enhancing customer confidence in data privacy within AI-enhanced financial services requires a multi-pronged strategy that integrates technological solutions with effective organizational practices. Relying solely on technical safeguards without addressing customer perceptions through communication and education is insufficient. Similarly, robust communication without underlying secure technologies lacks credibility. A holistic approach is essential for building and sustaining trust in these advanced systems. (Raiyan Haider, Md Farhan Abrar Ibne Bari, Osru, Nishat Afia, et al., 2025)

The objective is to move beyond mere compliance to cultivate a culture of privacy-by-design and privacy-by-default, where customer data protection is an inherent feature of all AI applications. This proactive stance not only mitigates risks but also transforms data privacy into a competitive advantage, attracting and retaining customers who prioritize the security of their financial information.

4.3.1 Technological Interventions: Privacy-Enhancing Technologies (PETs)

Technological interventions, particularly Privacy-Enhancing Technologies (PETs), offer robust solutions for safeguarding customer data in AI systems. PETs encompass a range of techniques designed to minimize personal data collection, increase anonymity, and secure data processing. Examples include homomorphic encryption, differential privacy, and secure multi-party computation, which allow computations on encrypted data or aggregate data without revealing individual records (Torra & Navarro-Arribas, 2014) (Ge & Zhu, 2011).

Privacy-preserving data mining (PPDM) algorithms, for instance, modify original data so that private information remains secure even during the mining process, offering strong privacy guarantees without sacrificing data accuracy (Yang et al., 2005). The development of such technologies is crucial for allowing financial institutions to leverage AI's analytical power while adhering to stringent privacy requirements. Cloud providers, for example, are developing solutions to support privacy measurement and analysis, contributing to trustworthiness scores (Basso et al., 2019).

4.3.2 Organizational Practices: Communication, Consent Mechanisms, and Education

Organizational practices are equally vital for fostering customer confidence. Clear, concise, and proactive communication about data privacy policies is paramount. This extends beyond legal disclaimers to plain-language explanations of how data is collected, used, shared, and protected. Transparent communication about an application of open data, for example, promotes user trust and increases willingness to use the service (Wiencierz & Lünich, 2020).

Effective consent mechanisms empower customers to make informed choices about their data. This includes granular control over data sharing and clear opt-in/opt-out options. Furthermore, educating customers about digital security practices and the benefits of AI-enhanced services can mitigate fear and misunderstanding (Redlinghuis & Rensleigh, 2010). A study on Facebook apps, for example, found that while users were initially unaware of data access, their concern increased after viewing permissions, indicating the importance of explicit information (Golbeck & Mauriello, 2016). Providing accessible and objective information about services, even when customer perceptions of a firm's ability are low, can lower uncertainty and differentiate offerings.

4.4 The Future Landscape: Anticipated Trends and Emerging Challenges

The landscape of AI-enhanced financial services is characterized by continuous evolution, presenting both exciting opportunities and complex challenges for data privacy. Future trends will likely involve more sophisticated AI models and increasingly complex regulatory environments. Navigating this future successfully will require financial institutions to anticipate changes, adapt their strategies, and continue prioritizing customer trust as a core principle.

The pace of technological advancement, particularly in AI, often outstrips the development of regulatory frameworks and societal understanding. This creates a dynamic tension that necessitates ongoing research, policy refinement, and industry collaboration. The focus will shift from merely reactive compliance to proactive, ethical innovation that embeds privacy deeply within AI system design and deployment.

4.4.1 The Role of Generative AI and Advanced Analytics

Generative AI and advanced analytics will play an increasingly prominent role in financial services, bringing new dimensions to data privacy. Generative models, capable of creating realistic synthetic data, could offer new ways to train AI systems while protecting real customer information. This could potentially address some privacy concerns by reducing the reliance on sensitive live data for model development (Torra & Navarro-Arribas, 2014).

However, these advanced models also introduce challenges. The potential for 'model inversion attacks,' where sensitive training data can be inferred from a generative model's outputs, presents new privacy risks. Furthermore, the complexity of these models exacerbates the explainability problem, making it even harder to provide clear rationales for AI decisions to customers (Hind et al., 2020). The balance between leveraging advanced AI capabilities and ensuring robust privacy will be a critical area of focus.

4.4.2 Evolving Regulatory Environments

Regulatory environments governing data privacy will continue to evolve, becoming more nuanced and potentially more stringent. The global divergence in privacy laws, exemplified by the US and EU approaches, suggests an ongoing need for international cooperation and harmonization efforts (Determann, 2019). Future regulations may specifically target AI's unique privacy implications, such as algorithmic bias, data provenance for training sets, and the right to explanation for automated decisions.

There is also a growing recognition that transparency alone is insufficient to address power imbalances inherent in commercial surveillance; the fundamental issue of data commodification often requires more comprehensive regulatory interventions (Crain, 2016). As AI systems become more pervasive, regulations may shift towards requiring explicit 'data trusts' or similar governance structures to manage collective data assets and ensure fair usage (O'Hara, 2020). Financial institutions must remain agile, adapting their data governance frameworks to meet these dynamic regulatory demands.

4.5 Synthesis of Key Findings

This paper has systematically examined customer perception of data privacy in AI-enhanced financial services, identifying trust, transparency, and personal control as central determinants of adoption and engagement. The integration of AI presents significant opportunities for enhanced financial services, including digital assistance and optimized operations (Fernandez, 2019) (Ryzhkova et al., 2020). However, these benefits are inextricably linked to managing associated privacy risks, particularly the opacity of algorithmic decision-making and potential for data misuse (Stefanija & Pierson, 2020).

A critical finding is that customer trust is highly contingent upon perceived transparency in data handling practices and the degree of control individuals feel they have over their personal information (Esmaeilzadeh, 2019) (Martin et al., 2017). While regulations like GDPR mandate transparency, simply providing information is often insufficient; the content must be comprehensible and relevant, recognizing the "transparency trade-off" where complexity can undermine credibility (Felzmann et al., 2019) (Salminen et al., 2019). Cross-cultural and demographic variations further modulate these perceptions, necessitating tailored privacy strategies (Determann, 2019). Misalignment between institutional practices and customer expectations can lead to severe reputational damage, legal consequences, and market setbacks (Martin et al., 2017). Mitigating these risks requires both advanced Privacy-Enhancing Technologies (PETs) and proactive organizational efforts in communication, robust consent mechanisms, and comprehensive customer education (Yang et al., 2005) (Redlinghuis & Rensleigh, 2010).

4.6 Recommendations for Policy, Practice, and Research

Based on the preceding analysis, several recommendations emerge for stakeholders

For Financial Institutions

- Implement "Privacy-by-Design": Integrate privacy safeguards, including PETs, from the initial stages of AI system development rather than as an afterthought (Torra & Navarro-Arribas, 2014).
- Prioritize Explainable AI (XAI): Develop AI models that can clearly articulate their decision-making processes in an understandable manner for customers, not just technical experts (Hind et al., 2020).
- Enhance Transparency and Communication: Provide clear, accessible, and frequent information about data collection, processing, and security measures. This includes plain-language privacy policies and regular updates (Wiencierz & Lünich, 2020).

- Strengthen Consent Mechanisms: Offer granular control over data sharing, allowing customers to easily manage their privacy settings and understand the implications of their choices. (Raiyan Haider & Jasmima Sabatina, 2025)
- Invest in Customer Education: Launch campaigns to inform customers about the benefits of AI in finance and the specific measures taken to protect their data, addressing common misconceptions and fears (Redlinghuis & Rensleigh, 2010).

For Policymakers and Regulators

- Harmonize Global Privacy Standards: Work towards greater consistency in data protection laws across jurisdictions to simplify compliance for international financial institutions and provide uniform consumer protections (Determann, 2019).
- Develop AI-Specific Regulations: Create targeted regulations that address the unique challenges of AI, such as algorithmic bias, data provenance, and accountability for automated decisions. (Raiyan Haider, 2025)
- Promote Data Governance Frameworks: Encourage or mandate the adoption of robust data governance frameworks, including independent audits of AI systems for fairness and privacy compliance.
- Explore Data Trust Models: Investigate and pilot innovative data governance models, such as data trusts, to collectively manage and oversee sensitive data assets (O'Hara, 2020).

For Researchers

- Investigate Usable Transparency: Conduct further research into how AI explanations can be made truly usable and credible for diverse user groups, considering the "transparency trade-off" (Salminen et al., 2019).
- Quantify Privacy Impact: Develop standardized metrics and methodologies to quantify the impact of AI systems on privacy and to evaluate the effectiveness of various PETs in real-world financial contexts.
- Longitudinal Studies of Trust: Undertake long-term studies to observe how customer trust in AI-enhanced financial services evolves over time, particularly following data incidents or regulatory changes.
- Cross-Cultural AI Privacy: Explore in greater depth the cultural nuances of AI privacy perceptions and how these influence the design and acceptance of AI financial products globally.

4.7 Pathways Forward: Building Sustainable Trust in AI-Powered Financial Services

AI chatbots are increasingly revolutionizing customer interactions in financial services by personalizing loan and credit experiences, streamlining application processes, and enhancing assessment accuracy. Despite their transformative potential, challenges such as privacy concerns, integration complexities, and maintaining customer trust remain critical hurdles to address (Emmanuel Igba et al., 2024). Furthermore, combining AI with blockchain technology offers promising advancements in security, fraud detection, and regulatory compliance, fostering greater transparency and trust within financial ecosystems (Olubusola Odeyemi et al., 2024). Continued innovation and ethical governance in these areas will be essential for sustainable growth and customer confidence.

Building sustainable trust in AI-powered financial services requires a shift from mere compliance to embracing data privacy as a core value and competitive advantage. Financial institutions that prioritize ethical AI development, transparent communication, and robust data governance are better positioned to foster lasting customer relationships and harness AI's transformative potential. Integrating technologies like blockchain can further enhance security and transparency, address privacy concerns and strengthening trust across the financial ecosystem (Olubusola Odeyemi et al., 2024) (Han et al., 2023).

5 Conclusion

Customer perception of data privacy stands as a decisive factor in the evolution and acceptance of AI-powered financial services. As institutions integrate AI to deliver smarter, more personalized offerings, maintaining clarity, offering genuine control over personal data, and ensuring trustworthy practices will define customer relationships and market reputation. The interplay between emerging technologies, regulatory shifts, and diverse cultural expectations demands that financial organizations stay agile and responsive. By embedding transparent practices and robust privacy protections into every stage of AI deployment, the financial sector can build lasting confidence and unlock the full potential of digital innovation for both businesses and consumers.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Fernandez, A. (2019). Artificial Intelligence in Financial Services. In SSRN Electronic Journal. Elsevier BV. https://doi.org/10.2139/ssrn.3366846

[2] Mahalle, A., Yong, J., Tao, X., & Shen, J. (2018). Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure. In 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD)) (pp. 407–413). IEEE. https://doi.org/10.1109/cscwd.2018.8465318

[3] Ryzhkova, M., Soboleva, E., Sazonova, A., & Chikov, M. (2020). Consumers' Perception of Artificial Intelligence in Banking Sector. In A. Vankevich & T. Ilina (Eds.), SHS Web of Conferences (Vol. 80, p. 01019). EDP Sciences. https://doi.org/10.1051/shsconf/20208001019

[4] Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. In Journal of Marketing (Vol. 81, Issue 1, pp. 36–58). SAGE Publications. https://doi.org/10.1509/jm.15.0497

[5] Esmaeilzadeh, P. (2019). The Impacts of the Perceived Transparency of Privacy Policies and Trust in Providers for Building Trust in Health Information Exchange: Empirical Study (Preprint). JMIR Publications Inc. https://doi.org/10.2196/preprints.14050

[6] Torra, V., & Navarro-Arribas, G. (2014). Data privacy. In WIREs Data Mining and Knowledge Discovery (Vol. 4, Issue 4, pp. 269–280). Wiley. https://doi.org/10.1002/widm.1129

[7] Adjei, J. K., Obubuafo-Ayettey, W. N. A., & Tobbin, P. E. (2020). Understanding Customers Perception of ATM Data Integrity. In Nordic and Baltic Journal of Information & Communications Technologies. River Publishers. https://doi.org/10.13052/nbjict1902-097x.2020.008

[8] Raiyan Haider, Wahida Ahmed Megha, Jafia Tasnim Juba, Aroa Alamgir, & Labib Ahmad. (2025). The conversational revolution in health promotion: Investigating chatbot impact on healthcare marketing, patient engagement, and service reach. In International Journal of Science and Research Archive (Vol. 15, Issue 3, pp. 1585–1592). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.3.1937

[9] Redlinghuis, A., & Rensleigh, C. (2010). Customer perceptions on Internet banking information protection. In SA Journal of Information Management (Vol. 12, Issue 1). AOSIS. https://doi.org/10.4102/sajim.v12i1.444

[10] Milosavljević, N., & Njagojević, S. (2019). Customers' perception of information security in internet banking. In Proceedings of the 5th IPMA SENET Project Management Conference (SENET 2019). Atlantis Press. https://doi.org/10.2991/senet-19.2019.45

[11] Yartey, D., Omojola, O., Amodu, L., Ndubueze, N., Adeyeye, B., & Adesina, E. (2021). Personal Data Collection and Usage for Mobile Marketing. Customer Awareness and Perception. In WSEAS TRANSACTIONS ON BUSINESS AND ECONOMICS (Vol. 18, pp. 42–50). World Scientific and Engineering Academy and Society (WSEAS). https://doi.org/10.37394/23207.2021.18.5

[12] Solberg Søilen, K. (2016). Users' perceptions of Data as a Service (DaaS). In Journal of Intelligence Studies in Business (Vol. 6, Issue 2). University of Latvia. https://doi.org/10.37380/jisib.v6i2.172

[13] De Capitani di Vimercati, S., Foresti, S., Livraga, G., & Samarati, P. (2019). Data security and privacy in the cloud. In S. S. Agaian, S. P. DelMarco, & V. K. Asari (Eds.), Mobile Multimedia/Image Processing, Security, and Applications 2019 (p. 15). SPIE. https://doi.org/10.1117/12.2523603

[14] Bertino, E. (2020). The Quest for Data Transparency. In IEEE Security & Privacy (Vol. 18, Issue 3, pp. 67–68). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/msec.2020.2980593

[15] Determann, L. (2019). Privacy and Data Protection. In Moscow Journal of International Law (Vol. 2019, Issue 1, pp. 18–26). MGIMO University. https://doi.org/10.24833/0869-0049-2019-1-18-26

[16] Felzmann, H., Villaronga, E. F., Lutz, C., & Tamò-Larrieux, A. (2019). Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. In Big Data & Society (Vol. 6, Issue 1). SAGE Publications. https://doi.org/10.1177/2053951719860542

[17] Stefanija, A. P., & Pierson, J. (2020). Practical AI Transparency: Revealing Datafication and Algorithmic Identities. In Journal of Digital Social Research (Vol. 2, Issue 3, pp. 84–125). DIGSUM (Centre for Digital Social Research). https://doi.org/10.33621/jdsr.v2i3.32

[18] Raiyan Haider, Farhan Abrar Ibne Bari, Osru, Nishat Afia, & Mohammad Abiduzzaman khan Mugdho. (2025). Leveraging internet of things data for real-time marketing: Opportunities, challenges, and strategic implications. In International Journal of Science and Research Archive (Vol. 15, Issue 3, pp. 1657–1663). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.3.1936

[19] Lavuri, R. (2018). Customer Perception towards E-Banking Services: A Study on Public and Private Banks. In International Journal for Research in Applied Science and Engineering Technology (Vol. 6, Issue 5, pp. 631–637). International Journal for Research in Applied Science and Engineering Technology (IJRASET). https://doi.org/10.22214/ijraset.2018.5106

[20] Larsson, S., & Heintz, F. (2020). Transparency in artificial intelligence. In Internet Policy Review (Vol. 9, Issue 2). Internet Policy Review, Alexander von Humboldt Institute for Internet and Society. https://doi.org/10.14763/2020.2.1469

[21] Paris, D. C. (2018). Information, Data, and Transparency. In Change: The Magazine of Higher Learning (Vol. 50, Issue 5, pp. 4–6). Informa UK Limited. https://doi.org/10.1080/00091383.2018.1510238

[22] Salminen, J., Santos, J. M., Jung, S.-G., Eslami, M., & Jansen, B. J. (2019). Persona Transparency: Analyzing the Impact of Explanations on Perceptions of Data-Driven Personas. In International Journal of Human–Computer Interaction (Vol. 36, Issue 8, pp. 788–800). Informa UK Limited. https://doi.org/10.1080/10447318.2019.1688946

[23] Ge, X., & Zhu, J. (2011). Privacy Preserving Data Mining. In New Fundamental Technologies in Data Mining. InTech. https://doi.org/10.5772/13364

[24] Yang, Z., Zhong, S., & Wright, R. N. (2005). Privacy-Preserving Classification of Customer Data without Loss of Accuracy. In Proceedings of the 2005 SIAM International Conference on Data Mining. Society for Industrial and Applied Mathematics. https://doi.org/10.1137/1.9781611972757.9

[25] Raiyan Haider, Md Farhan Abrar Ibne Bari, Md. Farhan Israk Shaif, Mushfiqur Rahman, Md. Nahid Hossain Ohi, & Kazi Md Mashrur Rahman. (2025). Quantifying the Impact: Leveraging AI-Powered Sentiment Analysis for Strategic Digital Marketing and Enhanced Brand Reputation Management. In International Journal of Science and Research Archive (Vol. 15, Issue 2, pp. 1103–1121). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.2.1524

[26] Taylor, C. R. (2004). Consumer Privacy and the Market for Customer Information. In The RAND Journal of Economics (Vol. 35, Issue 4, p. 631). Wiley. https://doi.org/10.2307/1593765

[27] Ganesan, Dr. R., & Bhuvaneswari, A. (2016). Customer Perception Towards Green Banking. In IOSR Journal of Economics and Finance (Vol. 07, Issue 05, pp. 05–17). IOSR Journals. https://doi.org/10.9790/5933-0705010517

[28] Matušínská, K. (2015). MARKETING PERCEPTION OF SELECTED CUSTOMERS' SEGMENT IN THE FINANCIAL SERVICES MARKET. In Acta academica karviniensia (Vol. 15, Issue 1, pp. 119–129). Silesian University in Opava. https://doi.org/10.25142/aak.2015.010

[29] Raiyan Haider, Md Farhan Abrar Ibne Bari, Md. Farhan Israk Shaif, & Mushfiqur Rahman. (2025). Engineering hyper-personalization: Software challenges and brand performance in AI-driven digital marketing management: An empirical study. In International Journal of Science and Research Archive (Vol. 15, Issue 2, pp. 1122–1141). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.2.1525

[30] Liu, Y., Eisingerich, A. B., Auh, S., Merlo, O., & Chun, H. E. H. (2015). Service Firm Performance Transparency. In Journal of Service Research (Vol. 18, Issue 4, pp. 451–467). SAGE Publications. https://doi.org/10.1177/1094670515584331

[31] Tringale, K. R., & Hattangadi-Gluth, J. A. (2019). Truth, Trust, and Transparency—The Highly Complex Nature of Patients' Perceptions of Conflicts of Interest in Medicine. In JAMA Network Open (Vol. 2, Issue 4, p. e191929). American Medical Association (AMA). https://doi.org/10.1001/jamanetworkopen.2019.1929

[32] Caratelli, M. (2009). Transparency Between Banks and Their Customers - Information Needs and Public Intervention. In SSRN Electronic Journal. Elsevier BV. https://doi.org/10.2139/ssrn.1341547

[33] Wiencierz, C., & Lünich, M. (2020). Trust in open data applications through transparency. In New Media & Society (Vol. 24, Issue 8, pp. 1751–1770). SAGE Publications. https://doi.org/10.1177/1461444820979708

[34] Bulyga, R. P., Sitnov, A. A., Kashirskaya, L. V., & Safonova, I. V. (2020). Transparency of credit institutions. In Entrepreneurship and Sustainability Issues (Vol. 7, Issue 4, pp. 3158–3172). Entrepreneurship and Sustainability Center. https://doi.org/10.9770/jesi.2020.7.4(38)

[35] Boué, S., Byrne, M., Hayes, A. W., Hoeng, J., & Peitsch, M. C. (2018). Embracing Transparency Through Data Sharing. In International Journal of Toxicology (Vol. 37, Issue 6, pp. 466–471). SAGE Publications. https://doi.org/10.1177/1091581818803880

[36] Raiyan Haider, Md Farhan Abrar Ibne Bari, Osru, Nishat Afia, & Tanjim Karim. (2025). Illuminating the black box: Explainable AI for enhanced customer behavior prediction and trust. In International Journal of Science and Research Archive (Vol. 15, Issue 3, pp. 247–268). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.3.1674

[37] Basso, T., Silva, H. de O., Montecchi, L., de França, B. B. N., & Moraes, R. L. de O. (2019). Towards trustworthy cloud service selection: monitoring and assessing data privacy. In Anais do Workshop de Testes e Tolerância a Falhas (WTF) (pp. 6–19). Sociedade Brasileira de Computação - SBC. https://doi.org/10.5753/wtf.2019.7711

[38] Golbeck, J., & Mauriello, M. (2016). User Perception of Facebook App Data Access: A Comparison of Methods and Privacy Concerns. In Future Internet (Vol. 8, Issue 2, p. 9). MDPI AG. https://doi.org/10.3390/fi8020009

[39] Hind, M., Houde, S., Martino, J., Mojsilovic, A., Piorkowski, D., Richards, J., & Varshney, K. R. (2020). Experiences with Improving the Transparency of AI Models and Services. In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (pp. 1–8). ACM. https://doi.org/10.1145/3334480.3383051

[40] Crain, M. (2016). The limits of transparency: Data brokers and commodification. In New Media & Society (Vol. 20, Issue 1, pp. 88–104). SAGE Publications. https://doi.org/10.1177/1461444816657096

[41] O'Hara, K. (2020). Data Trusts. In European Data Protection Law Review (Vol. 6, Issue 4, pp. 484–491). Lexxion Verlag. https://doi.org/10.21552/edpl/2020/4/4

[42] Raiyan Haider, & Jasmima Sabatina. (2025). Harnessing the power of micro-influencers: A comprehensive analysis of their effectiveness in promoting climate adaptation solutions. In International Journal of Science and Research Archive (Vol. 15, Issue 2, pp. 595–610). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.2.1448

[43] Raiyan Haider. (2025). Navigating the digital political landscape: How social media marketing shapes voter perceptions and political brand equity in the 21st Century. In International Journal of Science and Research Archive (Vol. 15, Issue 1, pp. 1736–1744). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.1.1217

[44] Emmanuel Igba, Adenike Folashade Adeyemi, Joy Onma Enyejo, Amina Catherine Ijiga, Grace Amidu, & George Addo. (2024). Optimizing business loan and credit experiences through AI-Powered Chatbot integration in financial services. In Finance & Accounting Research Journal (Vol. 6, Issue 8, pp. 1436–1458). Fair East Publishers. https://doi.org/10.51594/farj.v6i8.1406

[45] Olubusola Odeyemi, Chinwe Chinazo Okoye, Onyeka Chrisanctus Ofodile, Omotayo Bukola Adeoye, Wilhelmina Afua Addy, & Adeola Olusola Ajayi-Nifise. (2024). INTEGRATING AI WITH BLOCKCHAIN FOR ENHANCED FINANCIAL SERVICES SECURITY. In Finance & Accounting Research Journal (Vol. 6, Issue 3, pp. 271–287). Fair East Publishers. https://doi.org/10.51594/farj.v6i3.855

[46] Han, Y., Chen, J., Dou, M., Wang, J., & Feng, K. (2023). The Impact of Artificial Intelligence on the Financial Services Industry. In Academic Journal of Management and Social Sciences (Vol. 2, Issue 3, pp. 83–85). Darcy & Roy Press Co. Ltd. https://doi.org/10.54097/ajmss.v2i3.8741