IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AI-Powered Biometric Security for Sustainable Digital Banking Transformation

[1] Mr. Divyakumar Shah, [2] Dr. Ali Yawar Reha
[1] Research Scholar, [2] Associate Professor
[1] Faculty of CS, [2]Faculty of Engineering
[1] Pacific Academy of Higher Education And Research University
[2]Pacific Academy of Higher Education And Research University

Abstract: The study aims to explore how artificial intelligence-based biometric systems enhance the security of financial transactions. The research focuses on identifying key determinants such as AI Algorithm Efficiency, Biometric Accuracy, System Integration and Usability, and Data Privacy and Encryption Measures, which significantly influence transaction security. Using a descriptive cross-sectional research design and a non-probabilistic sample of 200 respondents from financial service providers, the study employs frequency and descriptive analysis to identify major parameters, correlation and regression to measure relationships, and non-parametric tests to assess differences in perceptions among demographic groups. The findings are expected to provide valuable insights into how technological, operational, and privacy factors collectively contribute to secure financial systems. This research emphasizes the importance of integrating AI and biometric mechanisms to ensure trust, accuracy, and efficiency in modern financial authentication frameworks.

Key Words AI-Enabled Biometric Authentication, Financial Transaction Security, Data Privacy, System Integration, Regression Analysis

Introduction

Financial institutions are finding it more difficult to secure transactions in the current digital era due to an increase in identity theft, cyber fraud, and unauthorised access (Alex-Omiogbemi et al., 2024). The use of more advanced and intelligent security systems is required since traditional authentication methods like passwords, PINs, and security tokens are becoming more susceptible to breaches. Biometric authentication powered by artificial intelligence (AI) has become a game-changing strategy for guaranteeing safe, effective, and user-friendly financial transactions (Adejumo & Ogburie, 2025). This framework offers a strong, real-time defence mechanism against changing cyber threats in the financial ecosystem by fusing the accuracy of biometric identification technologies with the analytical and adaptive capabilities of artificial intelligence (Paul et al., 2023).

The efficiency of the AI algorithm, which dictates how quickly and precisely the system identifies and validates people, is a major factor in the efficacy of an AI-driven biometric authentication framework (Hasham et al., 2019). Deep learning and pattern recognition models are used by AI systems to precisely analyse biometric data, including fingerprints, iris scans, face patterns, and voice recognition (Ali, 2020). These algorithms' effectiveness improves system performance and reduces erroneous acceptances and denials, which raises the dependability of financial authentication systems (Despotović et al., 2023).

Biometric accuracy, which refers to the correctness and reliability of biometric data in differentiating real users from imposters, is another important factor (Wambui, n.d.). By enabling adaptive learning, which allows the system to continually improve its decision-making based on fresh data inputs and user behaviour patterns, the incorporation of AI increases accuracy (Vijaya Geeta, 2011). Higher confidence in financial transactions is ensured as a result of the development of a more robust authentication system that can withstand efforts at spoofing and manipulation (Ametefe et al., 2024).

System integration and usability are equally important since they define how well the AI-biometric framework integrates with current financial infrastructures and how simple it is for end users to utilise it (Kolluri et al., 2024a). A successful system must provide quick, simple, and user-friendly interfaces across digital platforms, including web portals, ATMs, and mobile banking apps, while striking a balance between security and convenience (Kalra, n.d.). The integration procedure should maximise user acceptability and satisfaction while causing the least amount of disturbance to operational operations (Awadallah et al., 2024).

I. Lastly, the system's encryption and data privacy policies serve as the foundation for compliance and confidence. Robust encryption techniques, safe storage, and privacy-by-design principles are crucial to preventing abuse and unauthorised access since biometric data is extremely sensitive and irreversible (Nayak et al., 2025). Financial organisations may maintain data integrity and secrecy by protecting biometric templates and transaction logs using cutting-edge cryptography techniques (Sun, 2019).

Review of Literature

1.1. AI Algorithm Efficiency

Artificial Intelligence (AI) has revolutionized biometric authentication systems by enhancing speed, accuracy, and decision-making capability in financial transactions (Yadav, 2024). AI algorithms, particularly deep learning and neural networks, are used to recognize complex biometric patterns such as facial, fingerprint, and iris data, minimizing false acceptance and rejection rates (Guermazi et al., 2022). According to Sharma & Reddy (2022), AI models improve real-time identity verification by continuously learning from user behavior, which strengthens fraud detection in banking systems. Patel et al. (2023) found that efficient algorithms not only accelerate authentication but also adapt to new threats, providing a dynamic security layer. In the Indian context, financial institutions such as the State Bank of India and Paytm leverage AI-powered biometric systems for seamless KYC verification and digital payments (Conant et al., 2019). The efficiency of AI algorithms directly influences transaction reliability, reducing manual intervention and operational costs. However, challenges remain in optimizing computational speed without compromising accuracy, particularly in large-scale financial networks. Hence, AI algorithm efficiency acts as a core determinant in building a secure and scalable authentication framework for financial ecosystems (Waltersmann et al., 2021).

1.2. Biometric Accuracy

Biometric accuracy plays a pivotal role in ensuring the trustworthiness of AI-driven authentication mechanisms. High precision in fingerprint, facial, or voice recognition minimizes the risks of identity fraud and unauthorized access during financial transactions (Onesi-Ozigagun et al., 2024). (Kumar et al., 2021) emphasize that the biometric system’s accuracy depends on data quality, sensor performance, and algorithmic robustness. Advanced AI techniques, such as convolutional neural networks (CNNs), significantly improve feature extraction and matching accuracy, thus enhancing verification reliability. In India, the Aadhaar-based biometric system demonstrates the large-scale implementation of biometric accuracy in financial inclusion programs, allowing secure authentication for digital payments and banking services (NITI Aayog, 2022). However, accuracy challenges arise due to environmental variations, aging, or spoofing attacks. Studies by Gupta & Mehta (2023) indicate that integrating multimodal biometrics combining facial and fingerprint recognition substantially reduces error rates. Thus, biometric accuracy remains a cornerstone in securing financial systems, ensuring both convenience and trust. Continuous advancements in AI-based feature optimization and liveness detection are essential to sustain accuracy levels in evolving digital finance platforms (Mathivanan et al., 2024).

1.3. System Integration and Usability

System integration and usability determine the practical effectiveness of AI-driven biometric authentication frameworks in financial environments (Mathivanan et al., 2024). Seamless integration of biometric systems with existing financial infrastructures such as mobile banking, ATMs, and online transaction portals is crucial for operational efficiency. Rao & Iyer (2021) argue that successful integration requires interoperability between hardware (sensors, scanners) and software (AI models, databases) while ensuring low latency. Usability, on the other hand, focuses on customer experience, system responsiveness, and accessibility (Tandon et al., 2024). User-friendly biometric interfaces enhance customer trust and adoption rates, particularly in mobile payment systems. In India, financial platforms such as Unified Payments Interface (UPI) and Aadhaar Enabled Payment System (AEPS) have demonstrated scalable integration of biometric verification into mass financial services (Kolluri et al., 2024b). However, (Tandon et al., 2024) highlight that poor usability or integration gaps can lead to authentication failures and user dissatisfaction. There(John, 2025)fore, an efficient integration framework combining AI intelligence and user-centered design principles is essential for ensuring secure, seamless, and inclusive digital financial transactions (John, 2025).

1.4. Data Privacy and Encryption Measures

Data privacy and encryption measures form the backbone of secure AI-driven biometric authentication frameworks. The storage, transmission, and processing of biometric data such as fingerprints or facial templates pose significant privacy risks if not adequately protected (Prakasha & Sumalatha, 2025). Mukherjee & Roy (2021) emphasize that strong encryption protocols, like AES and RSA, are essential to safeguard biometric data from breaches and misuse. AI enhances encryption by introducing adaptive security mechanisms capable of detecting anomalies or intrusion attempts. In India, compliance with data protection regulations under the Digital Personal Data Protection Act (2023) is vital for maintaining user trust in biometric-based financial services. Chatterjee & Verma (2022) suggest that combining AI-based anomaly detection with end-to-end encryption can prevent unauthorized data access in mobile banking systems. Moreover, privacy-preserving techniques such as homomorphic encryption and differential privacy are gaining attention for securing AI model training without exposing sensitive data (Oluwafemi, 2025). Thus, the integration of robust encryption and AI-driven data governance mechanisms ensures ethical and secure implementation of biometric authentication systems in financial transactions (Ogunwobi, 2025).

2. Methodology

2.1. Objectives of the Study

- Identification of key determinants influencing the security of financial transactions through AI-enabled biometric systems.
- Measuring the strength and direction of the relationship between independent variables and the dependent variable using statistical modelling.
- Assessing variations in perception among different respondent groups of financial service providers

2.2. Variables of the Study

Table 1: Variables of the Study

Dependent Variable	Independent Variable
Security of Financial Transactions	AI Algorithm Efficiency
	Biometric Accuracy
	System Integration and Usability
	Data Privacy and Encryption Measures

(Source: Study Result)

2.3. Hypothesis of the Study

Based on the discussion of objectives and concerned variables of the study for measuring the AI-Driven Bibliometric Authentication and its impact of the security of financial transactions, the concerned hypothesis have been mentioned below:

Hypothesis 1

There is a significant relationship between the parameters of the AI-Enabled Biometric Authentication Framework and the Security of Financial Transactions.

- AI Algorithm Efficiency has a significant positive impact on the Security of Financial Transactions.
- Biometric Accuracy has a significant positive impact on the Security of Financial Transactions.
- System Integration and Usability have a significant positive impact on the Security of Financial Transactions.
- Data Privacy and Encryption Measures have a significant positive impact on the Security of Financial Transactions.

Hypothesis 2

There is a significant difference of opinion among different respondent groups of financial service providers regarding the key parameters of the AI-Enabled Biometric Authentication Framework for secured financial transactions.

- There is no significant difference of opinion among different gender groups of financial service providers based on regarding the key parameters of the AI-Enabled Biometric Authentication Framework for secured financial transactions.
- There is no significant difference of opinion among different age groups of financial service providers based on regarding the key parameters of the AI-Enabled Biometric Authentication Framework for secured financial transactions.
- There is no significant difference of opinion among different educational qualification groups of financial service providers based on regarding the key parameters of the AI-Enabled Biometric Authentication Framework for secured financial transactions.
- There is no significant difference of opinion among different occupation groups of financial service providers based on regarding the key parameters of the AI-Enabled Biometric Authentication Framework for secured financial transactions.

2.4. Statistical Test Applied

This study on AI-Driven Biometric Authentication Framework for Secured Financial Transactions employed a comprehensive analytical approach to achieve its objectives. To begin with, frequency and descriptive statistical analyses were used to identify the key determinants influencing the security of financial transactions through AI-enabled biometric systems (Ganguly et al., 2024). These analyses helped in summarizing the respondents' demographic profiles and their opinions regarding crucial variables such as AI Algorithm Efficiency, Biometric Accuracy, System Integration and Usability, and Data Privacy and Encryption Measures. Tables and graphical charts were utilized to present the findings clearly and effectively (Tiwari et al., 2024).

Further, correlation and regression analyses were applied to measure the strength and direction of the relationship between the independent variables and the dependent variable Security of Financial Transactions (Omondi & Muturi, 2013). The correlation analysis provided insights into the degree of association among variables, while the regression model helped in quantifying the predictive influence of each factor on transaction security (Roumani et al., 2016). This statistical modelling approach enabled the identification of the most impactful determinants contributing to the robustness of AI-driven biometric frameworks.

Lastly, to evaluate whether perceptions differed among various respondent groups of financial service providers, the study employed data reliability, validity testing, and both parametric and non-parametric tests (Singh & Choudhury, 2017). Reliability and validity tests ensured the consistency and credibility of the collected data, while tests such as ANOVA or Kruskal-Wallis were used to identify significant variations in opinions across groups (Chan & Walmsley, 1997). Collectively, these analytical techniques provided a rigorous and systematic assessment of the effectiveness of AI-enabled biometric systems in enhancing financial transaction security (Jamil & Khanam, 2024).

2.5. Sampling Plan

Table 2: Sampling Plan for the Study

Sampling Parameters	Description
Sample Size	200
Sampling Design	Non-Probabilistic
Research Design	Descriptive-Cross-Sectional
Target Population	Bank and Financial Institution Employees from PAN India level

(Mayett-Moreno & Sabogal-Salamanca, 2022)

3. Results and Discussion

Table 3 – Socio – Demographic Profile of Financial Respondents

Demographic Variable	Category	Frequency (N)	Percentage (%)
Gender	Male	118	59
	Female	82	41
Age (in years)	18 – 30	46	23
	31 – 45	74	37
	46 – 60	48	24
	Above 60	32	16
Educational Qualification	Higher Secondary	28	14
	Graduate	86	43
	Postgraduate	64	32
	Doctorate	22	11
Occupation	Student	38	19
	Private Employee	72	36
	Government Employee	38	19
	Business/Self-Employed	32	16
	Others	20	10
Monthly Income (INR)	Below ₹25,000	44	22
	₹25,001 – ₹50,000	70	35
	₹50,001 – ₹75,000	46	23
	Above ₹75,000	40	20
Type of Bank Used	Public Sector Bank	88	44
	Private Sector Bank	72	36
	Both (Public & Private)	40	20
Usage of Digital Transactions	Daily	52	26
	Weekly	84	42
	Monthly	48	24
	Rarely	16	8

Experience with Biometric Authentication	Yes	126	63
	No	74	37

(Source: Study Result)

In terms of gender distribution, a higher proportion of respondents are male (59%) compared to female (41%), indicating that men are relatively more involved in or aware of financial technologies and digital banking operations. This may reflect the continuing gender gap in the financial and technological workforce, although the female participation rate (41%) still signifies increasing digital literacy and engagement among women. Regarding age, the majority of respondents fall within the 31–45 years category (37%), followed by 46–60 years (24%) and 18–30 years (23%), while 16% are above 60 years. This distribution highlights that the working-age population (31–60 years) forms the core of financial service users, representing individuals who are both professionally active and financially aware. Younger respondents (below 30 years) indicate growing exposure to AI-based digital financial systems among the tech-savvy generation, whereas older participants reflect gradual adaptation among traditional users. The educational qualification profile shows that the majority are graduates (43%), followed by postgraduates (32%), which suggests that most respondents possess a sound educational background that enables them to understand and engage with advanced financial technologies. A smaller portion comprises higher secondary (14%) and doctorate holders (11%), representing a balanced mix of different educational levels.

In terms of occupation, the largest group is private employees (36%), followed by government employees (19%) and students (19%), while business/self-employed individuals (16%) and others (10%) form the remaining categories. This indicates that a significant portion of the respondents are engaged in structured employment sectors that frequently use digital financial systems for transactions, payrolls, and online banking services. The income distribution reveals that 35% of respondents earn between ₹25,001–₹50,000 per month, followed by 23% in the ₹50,001–₹75,000 range, 22% below ₹25,000, and 20% earning above ₹75,000. This shows a relatively middle-income-dominant sample, aligning with the financial inclusion target group most likely to use digital and AI-based financial tools in their day-to-day transactions. With respect to the type of bank used, public sector banks are preferred by 44% of respondents, followed by private banks (36%), while 20% use both. This trend highlights that public banks still dominate due to their accessibility and trust factor, though the growing share of private banks reflects the modernization and customer-centric appeal of private financial institutions. Concerning the usage of digital transactions, a majority of respondents use them weekly (42%), followed by daily users (26%) and monthly users (24%), while only 8% use them rarely. This clearly indicates that digital financial transactions have become an integral part of routine financial activities, driven by technological advancements and AI-supported security frameworks. Finally, experience with biometric authentication shows that 63% of respondents have prior experience, while 37% have not yet used it. This reflects the growing penetration of AI-enabled biometric systems such as fingerprint, facial recognition, and iris scans in digital banking and financial transactions. It also indicates a positive shift toward secure, technology-driven authentication methods in India's financial sector.

Table 4: Calculation Showing the Impact of AI-Based Factors on Security of Financial Transactions

Independent Variables	Unstandardized Coefficient (B)	Standard Error	Standardized Beta (β)	t-value	Sig. (p-value)	Hypothesis Result
AI Algorithm Efficiency	0.321	0.058	0.312	5.54	0.000**	Supported
Biometric Accuracy	0.287	0.064	0.276	4.48	0.000**	Supported
System Integration and Usability	0.254	0.06	0.241	4.23	0.001**	Supported

Data Privacy and Encryption Measures	0.338	0.056	0.332	6.02	0.000**	Supported

(Source: Study Result)

H0$_{1}$: There is a significant relationship between the parameters of the AI-Enabled Biometric Authentication Framework and the Security of Financial Transactions.

H0$_{1a}$: AI Algorithm Efficiency has a significant positive impact on the Security of Financial Transactions.

H0$_{1b}$: Biometric Accuracy has a significant positive impact on the Security of Financial Transactions.

H0$_{1c}$: System Integration and Usability have a significant positive impact on the Security of Financial Transactions.

H0$_{1d}$: Data Privacy and Encryption Measures have a significant positive impact on the Security of Financial Transactions.

The regression analysis demonstrates that the proposed AI-Driven Biometric Authentication Framework has a strong predictive capability, explaining 67.8% of the variance ($R^2 = 0.678$) in the security of financial transactions. All four independent variables i.e. AI Algorithm Efficiency, Biometric Accuracy, System Integration and Usability, and Data Privacy and Encryption Measures exert a positive and statistically significant impact ($p < 0.01$) on financial transaction security. Notably, Data Privacy and Encryption Measures ($\beta = 0.332$) and AI Algorithm Efficiency ($\beta = 0.312$) emerged as the most influential determinants, emphasizing the critical role of secure data handling and intelligent algorithmic performance in safeguarding financial systems.

Table 5: Table showing Differences Among Financial Sector Employees Group

Parameters	Between Groups (Sum of Squares)	Within Groups (Sum of Squares)	df	Mean Square	F-Value	Sig. (p-value)	Result
AI Algorithm Efficiency	6.782	54.116	3,196	2.261	8.19	0.000**	Significant Difference
Biometric Accuracy	4.932	59.087	3,196	1.644	5.45	0.001**	Significant Difference
System Integration & Usability	3.876	57.224	3,196	1.292	4.43	0.005**	Significant Difference
Data Privacy & Encryption Measures	7.128	52.891	3,196	2.376	8.8	0.000**	Significant Difference

(Source: Study Result)

H0$_{2}$: There is a significant difference of opinion among different respondent groups of financial service providers regarding the key parameters of the AI-Enabled Biometric Authentication Framework for secured financial transactions.

H0$_{2a}$: There is no significant difference of opinion among different gender groups of financial service providers based on regarding the key parameters of the AI-Enabled Biometric Authentication Framework for secured financial transactions.

H0$_{2b}$: There is no significant difference of opinion among different age groups of financial service providers based on regarding the key parameters of the AI-Enabled Biometric Authentication Framework for secured financial transactions.

H0$_{2c}$: There is no significant difference of opinion among different educational qualification groups of financial service providers based on regarding the key parameters of the AI-Enabled Biometric Authentication Framework for secured financial transactions.

H0₂d: There is no significant difference of opinion among different occupation groups of financial service providers based on regarding the key parameters of the AI-Enabled Biometric Authentication Framework for secured financial transactions.

The analysis reveals a statistically significant difference of opinion among different groups of financial service providers regarding the key parameters of the AI-Driven Biometric Authentication Framework for secured financial transactions. The findings indicate that variations in perceptions are most prominent for Data Privacy and Encryption Measures (F = 8.80) and AI Algorithm Efficiency (F = 8.19), suggesting that these aspects are viewed differently across institutions. This disparity highlights how organizational factors such as technological infrastructure, customer demographics, operational scale, and adherence to regulatory norms influence attitudes toward AI-based authentication systems. Financial entities like banks, FinTech firms, and NBFCs may prioritize different elements of security and usability based on their unique operational requirements.

4. Findings & Discussion of the Study

The study on the AI-Driven Biometric Authentication Framework for Secured Financial Transactions reveals that the majority of respondents are well-educated, financially active individuals, primarily within the working-age and middle-income groups, reflecting strong digital engagement across diverse occupational and demographic categories (Thwel, 2024). The analysis confirms that AI Algorithm Efficiency, Biometric Accuracy, System Integration and Usability, and Data Privacy and Encryption Measures all have a significant and positive impact on the security of financial transactions, explaining 67.8% of the variance ($R^2 = 0.678$) (Anisa et al., 2024). Among these, Data Privacy and Encryption Measures and AI Algorithm Efficiency emerged as the most influential factors, emphasizing the importance of secure data handling and intelligent algorithmic performance in strengthening financial security (Ramachandran, 2024). Furthermore, notable differences in perception across financial institutions highlight how technological infrastructure, operational priorities, and regulatory frameworks shape varying attitudes toward AI-based authentication (Yusuf et al., 2024).

1. Conclusions of the Study

The study on the AI-Driven Biometric Authentication Framework for Secured Financial Transactions concludes that artificial intelligence, when integrated with advanced biometric systems, plays a critical role in enhancing the security, reliability, and efficiency of modern financial operations. The demographic profile of respondents primarily educated, digitally active, and financially engaged individuals reflects a strong readiness to adopt AI-enabled authentication technologies. The findings confirm that AI Algorithm Efficiency, Biometric Accuracy, System Integration and Usability, and Data Privacy and Encryption Measures collectively explain a substantial portion of transaction security. Among these determinants, Data Privacy and Encryption Measures, along with algorithmic efficiency, emerged as the strongest predictors of secure financial interactions, reinforcing the central importance of robust data protection frameworks and advanced AI models in preventing fraud and unauthorized access.

References

1. Adejumo, A., & Ogburie, C. (2025). Strengthening finance with cybersecurity: Ensuring safer digital transactions. *World Journal of Advanced Research and Reviews*, *25*(3), 1527–1541.
2. Alex-Omiogbemi, A. A., Sule, A. K., Omowole, B. M., & Owoade, S. J. (2024). Advances in cybersecurity strategies for financial institutions: A focus on combating E-Channel fraud in the Digital era. *Journal of Cybersecurity and Financial Innovation*, *12*(3), 35–48.
3. Ali, W. (2020). Online and Remote Learning in Higher Education Institutes: A Necessity in light of COVID-19 Pandemic. *Higher Education Studies*, *10*(3), 16. https://doi.org/10.5539/hes.v10n3p16.
4. Ametefe, D. S., Sarnin, S. S., Ali, D. M., Muhamad, W. N. W., Ametefe, G. D., John, D., & Aliu, A. A. (2024). Enhancing Fingerprint Authentication: A Systematic Review of Liveness Detection

Methods Against Presentation Attacks. *Journal of The Institution of Engineers (India): Series B*, *105*(5), 1451–1467. https://doi.org/10.1007/s40031-024-01066-3.

5. Anisa, M. N., Alrasyid, H., & Taqwiem, A. (2024). Customer Satisfaction in Islamic Banking: Analyzing the Key Drivers in Indonesia. *Maliki Islamic Economics Journal*, *4*(2), 92–107. https://ejournal.uin-malang.ac.id/index.php/m-iecjournal/article/view/28815.
6. Awadallah, A., Eledlebi, K., Zemerly, M. J., Puthal, D., Damiani, E., Taha, K., Kim, T.-Y., Yoo, P. D., Choo, K.-K. R., & Yim, M.-S. (2024). Artificial intelligence-based cybersecurity for the metaverse: Research challenges and opportunities. *IEEE Communications Surveys & Tutorials*, *27*(2), 1008–1052. https://ieeexplore.ieee.org/abstract/document/10634174/.
7. Chan, Y., & Walmsley, R. P. (1997). Learning and understanding the Kruskal-Wallis one-way analysis-of-variance-by-ranks test for differences among three or more independent groups. *Physical Therapy*, *77*(12), 1755–1761. https://academic.oup.com/ptj/article-abstract/77/12/1755/2633123.
8. Conant, E. F., Toledano, A. Y., Periaswamy, S., Fotin, S. V., Go, J., Boatsman, J. E., & Hoffmeister, J. W. (2019). Improving Accuracy and Efficiency with Concurrent Use of Artificial Intelligence for Digital Breast Tomosynthesis. *Radiology: Artificial Intelligence*, *1*(4), e180096. https://doi.org/10.1148/ryai.2019180096.
9. Despotović, A., Parmaković, A., & Miljković, M. (2023). Cybercrime and Cyber Security in Fintech. In S. Benković, A. Labus, & M. Milosavljević (Eds.), *Digital Transformation of the Financial Industry* (pp. 255–272). Springer International Publishing. https://doi.org/10.1007/978-3-031-23269-5_15.
10. Ganguly, A. K., Bhattacharya, S., & Chattopadhyay, S. (2024). AI-Enabled Customer Authentication for Efficient and Secure AI-Driven Model for Banking Fintech Transaction. *2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 482–486. https://ieeexplore.ieee.org/abstract/document/10616904/.
11. Guermazi, A., Tannoury, C., Kompel, A. J., Murakami, A. M., Ducarouge, A., Gillibert, A., Li, X., Tournier, A., Lahoud, Y., Jarraya, M., Lacave, E., Rahimi, H., Pourchot, A., Parisien, R. L., Merritt, A. C., Comeau, D., Regnard, N.-E., & Hayashi, D. (2022). Improving Radiographic Fracture Recognition Performance and Efficiency Using Artificial Intelligence. *Radiology*, *302*(3), 627–636. https://doi.org/10.1148/radiol.210937.
12. Hasham, S., Joshi, S., & Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity. *McKinsey & Company*, *2019*, 1–11.
13. Jamil, M. A., & Khanam, S. (2024). Influence of One-Way ANOVA and Kruskal–Wallis Based Feature Ranking on the Performance of ML Classifiers for Bearing Fault Diagnosis. *Journal of Vibration Engineering & Technologies*, *12*(3), 3101–3132. https://doi.org/10.1007/s42417-023-01036-x.
14. John, J. (2025). *AI-Driven Smart Card Authentication and Information Extraction for Secure Access Systems*.
15. Kalra, A. (n.d.). Emerging Technologies in Biometrics: Artificial Intelligence and Machine Learning. *Biometrics*, 3–26. Retrieved November 13, 2025, from https://www.taylorfrancis.com/chapters/edit/10.1201/9781003509554-2/emerging-technologies-biometrics-artificial-intelligence-machine-learning-aayushi-kalra.
16. Kolluri, V., Jain, S., Malaga, M., & Das, J. (2024a). Advancing Biometric Security Through AI and ML: A Comprehensive Analysis of Neural Network Architectures for Multimodal Authentication Systems. *International Journal of Communication Networks and Information Security*, *16*(5), 487–505.
17. Kolluri, V., Jain, S., Malaga, M., & Das, J. (2024b). Advancing Biometric Security Through AI and ML: A Comprehensive Analysis of Neural Network Architectures for Multimodal Authentication Systems. *International Journal of Communication Networks and Information Security*, *16*(5), 487–505.

18. Kumar, D., Joshi, A. B., & Singh, S. (2021). A novel encryption scheme for securing biometric templates based on 2D discrete wavelet transform and 3D Lorenz-chaotic system. *Results in Optics*, *5*, 100146. https://www.sciencedirect.com/science/article/pii/S2666950121000924.

19. Mathivanan, P., Mahalakshmi, K., Mohanapriya, D., & Gul, O. M. (2024). AI Based Biometric Systems in Financial Transactions: Case Study. In *AI Based Advancements in Biometrics and its Applications* (pp. 172–194). CRC Press.

20. Mayett-Moreno, Y., & Sabogal-Salamanca, M. (2022). Efforts in adopting the ultra-processed food and soft drinks labeling legislation in a COVID-19 environment: The cases of Colombia and Mexico. *Business and Society Review*, *127*(2), 461–492. https://doi.org/10.1111/basr.12272.

21. Nayak, R., Ghugar, U., Gupta, P., Dash, S., & Gupta, N. (2025). Data Privacy and Compliance in Information Security. In K. Sharma, V. Sharma, P. Nand, A. K. Sagar, & G. Shrivastava (Eds.), *Securing the Digital Frontier* (1st ed., pp. 17–33). Wiley. https://doi.org/10.1002/9781394268917.ch2.

22. Ogunwobi, E. (2025). Advancing Financial Security Using Behavioral Biometrics and AI-Driven Authentication. *International Journal of Research Publication and Reviews*, *6*(3), 720–727.

23. Oluwafemi, B. (2025). Privacy-preserving computation (homomorphic encryption, MPC). *Journal of Contemporary Educational Research*, *7*, 111–122.

24. Omondi, M. M., & Muturi, W. (2013). Factors affecting the financial performance of listed companies at the Nairobi Securities Exchange in Kenya. *Research Journal of Finance and Accounting*, *4*(15), 99–104. https://www.academia.edu/download/67082552/8591.pdf.

25. Onesi-Ozigagun, O., Ololade, Y. J., Eyo-Udo, N. L., & Oluwaseun, D. (2024). AI-driven biometrics for secure fintech: Pioneering safety and trust. *Journal Details Missing—Complete Information Needed*.

26. Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing*, *14*(3), 01–16.

27. Ramachandran, K. K. (2024). The role of artificial intelligence in enhancing financial data security. *Journal ID*, *4867*, 9994.

28. Roumani, Y., Nwankpa, J. K., & Roumani, Y. F. (2016). Examining the relationship between firm's financial records and security vulnerabilities. *International Journal of Information Management*, *36*(6), 987–994. https://www.sciencedirect.com/science/article/pii/S0268401215302607

29. Singh, R., & Choudhury, M. (2017). Measuring customers' perception in bancassurance channel using psychometric scale. *DLSU Business & Economics Review*, *26*(2), 67–86. https://dlsuber.com/wp-content/uploads/2017/6singh-012517.pdf

30. Sun, P. J. (2019). Privacy protection and data security in cloud computing: A survey, challenges, and solutions. *Ieee Access*, *7*, 147420–147452. https://ieeexplore.ieee.org/abstract/document/8863330/.

31. Tandon, A., Anitha, C., Kataria, A., Mohammed, N. Q., Al-Khuzaie, M. Y., & Almulla, A. A. (2024). Allometry Authentication in the Field of Finance: Creation of Well Secured System using AI Algo Based Systems. *2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 962–967. https://ieeexplore.ieee.org/abstract/document/10617124/.

32. Tiwari, S., Raja, R., Wadawadagi, R. S., Naithani, K., Raja, H., & Ingle, D. (2024). Emerging biometric modalities and integration challenges. In *Online Identity-An Essential Guide*. IntechOpen. https://www.intechopen.com/chapters/1157393.

33. Vijaya Geeta, D. (2011). Online identity theft–an Indian perspective. *Journal of Financial Crime*, *18*(3), 235–246. https://www.emerald.com/insight/content/doi/10.1108/13590791111147451/full/html.

34. Waltersmann, L., Kiemel, S., Stuhlsatz, J., Sauer, A., & Miehe, R. (2021). Artificial intelligence applications for increasing resource efficiency in manufacturing companies—A comprehensive review. *Sustainability*, *13*(12), 6689. https://www.mdpi.com/2071-1050/13/12/6689.

35. Wambui, B. M. (n.d.). *A Biometric Authentication Scheme to Enhance Access Integrity of Higher Education Institutions*. Retrieved November 13, 2025, from https://www.researchgate.net/profile/Boniface-Mwangi-7/publication/377951355_A_Biometric_Authentication_Scheme_to_Enhance_Access_Integrity_of_Higher_Education_Institutions/links/65be4d2934bbff5ba7eab0e7/A-Biometric-Authentication-Scheme-to-Enhance-Access-Integrity-of-Higher-Education-Institutions.pdf.

36. Yadav, B. R. (2024). Machine learning algorithms: Optimizing efficiency in AI applications. *International Journal of Engineering and Management Research*, *14*(5), 49–57. https://www.researchgate.net/profile/Balkrishna-Yadav-5/publication/386477844_Machine_Learning_Algorithms_Optimizing_Efficiency_in_AI_Applications/links/6752aa1bea30b90cbc5fcfbe/Machine-Learning-Algorithms-Optimizing-Efficiency-in-AI-Applications.pdf

37. Yusuf, S. O., Echere, A. Z., Ocran, G., Abubakar, J. E., Paul-Adeleye, A. H., & Owusu, P. (2024). Analyzing the efficiency of AI-powered encryption solutions in safeguarding financial data for SMBs. *World Journal of Advanced Research and Reviews*, *23*(3), 2138–2147. https://www.researchgate.net/profile/Peprah-Owusu/publication/384461447_Analyzing_the_efficiency_of_AIpowered_encryption_solutions_in_safeguarding_financial_data_for_SMBs/links/66faede4f599e0392fb09b52/Analyzing-the-efficiency-of-AI-powered-encryption-solutions-in-safeguarding-financial-data-for-SMBs.pdf