

A STUDY ON CUSTOMER PERCEPTION OF AI-DRIVEN FRAUD DETECTION AND SUSTAINABLE CUSTOMER SATISFACTION IN DIGITAL BANKING

* Harini Swaminathan Iyer, ** Tiya Shripal Jain, *** Prachi Rajkumar Shukla **** Sunidhi Manindra Singh & ***** Dr. Revati Hunswadkar

* Students

Abstract:

Digital banking has rapidly evolved, enabling online money management while increasing vulnerability to fraud. Banks employ AI tools for real-time transaction monitoring to detect suspicious activities. A study assessed customer perceptions of AI fraud protection and its impact on satisfaction and trust. Survey results indicated that users found AI-based fraud detection to be quick and reliable, which alleviated concerns and fostered trust in digital banking. The findings suggest that effective fraud detection not only enhances security but also boosts customer satisfaction and retention in digital banking services. Thus, AI-driven fraud protection plays a crucial role in customer loyalty beyond mere security.

(Key Words: Artificial Intelligence, Fraud Detection Driven by AI, Digital Banking, Customer Satisfaction, Customer Trust.)

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0) which permits unrestricted use, distribution, and reproduction in any medium for non-commercial Use Provided the Original Author and Source Are Credited.

Introduction:

The shift to digital banking has been a double-edged sword. On one hand, managing your money has never been more convenient we can handle everything from paying rent to checking balances with a few taps while waiting for coffee. On the other hand, that same accessibility has opened a digital "back door" for cybercriminals, making phishing and identity theft a constant anxiety for both users and financial institutions. To fight back, banks have swapped out old-school, rigid security rules for AI-powered fraud detection. Here is why that matters and where the real challenge lies:

The Shift from Rules to Intelligence:

Traditional security was like a static checklist. If a transaction didn't fit a specific box, it was flagged. Modern AI is different; it acts more like a digital detective that learns on the job.

Continuous Learning:

By analyzing massive amounts of historical data, these systems get better at spotting "weird" behavior in real time.

Speed: AI can scan millions of data points in seconds, stopping a fraudulent transfer before the money even leaves the account.

The "**Trust Gap**": While we often talk about how well these algorithms work technically, we rarely talk about how they make people feel. A security system is only successful if the customer actually trusts it.

The Frustration Factor: If an AI is too aggressive and blocks your card while you're trying to buy groceries (a "false positive"), it creates instant resentment.

The Transparency Need: Users need to feel like the security measures are protective, not intrusive or broken. *Why Customer Sentiment Matters?*

In markets like India, where digital banking is exploding, technical specs aren't enough to keep a customer loyal. Security is the foundation of the relationship. If a user feels their account is safe and the alerts they receive are accurate and helpful, they stay. If they feel like they're fighting against a "black box" algorithm that randomly freezes their funds, they leave. Ultimately, AI fraud detection shouldn't just be viewed as a cool piece of tech—it is a vital tool for building long-term human trust. The future of banking depends on balancing high-tech defense with a seamless, frustration-free user experience.

Statement of the Problem:

Many banks in India now use AI tools to detect fraud in online banking. However, we still don't know what customers think of these systems. It's uncertain whether their opinions impact their satisfaction or influence their decision to continue using online banking.

Review of Literature:

1. Evolution and Capabilities of AI-Driven Fraud Detection

Recent academic discourse (Faisal et al., 2024; Adhikari et al., 2024) indicates a significant paradigm shift from traditional rule-based security to dynamic, AI-powered systems. Traditional methods are often criticized for their inability to keep pace with sophisticated cyber threats due to their reliance on static, predefined parameters. In contrast, modern AI models leverage supervised, unsupervised, and hybrid learning to analyze vast datasets in real-time.

Pattern Recognition: AI systems utilize neural networks and deep learning to identify subtle behavioral anomalies, such as unusual transaction sequences or geographical inconsistencies, that often go unnoticed by manual review (Adhikari et al., 2024).

Operational Efficiency: Research by Davitaia (2025) and Narsina et al. (2019) suggests that these systems automate complex logical tasks, allowing financial institutions to move from reactive mitigation to proactive prevention.

2. The Intersection of Trust, Transparency, and Fairness

While technical accuracy is paramount, the adoption of AI in banking is heavily mediated by human factors. Yaseen and Al-Amarneh (2025) argue that institutional trust and perceived justice are the primary drivers of AI acceptance.

The Transparency Gap: A major challenge identified in the literature is the "black box" nature of complex algorithms. To counter this, researchers advocate for Explainable AI (XAI), which provides understandable justifications for flagged transactions, thereby reducing user anxiety (Venu, 2025).

Ethical AI: Observed findings from the UAE and Qatar suggest that transparency directly influences trust. Furthermore, perceptions of "fairness" act as a buffer against concerns regarding algorithmic bias, reinforcing the need for ethical AI deployment in highly regulated financial environments (Yaseen, 2025).

3. Impact on Customer Experience and Satisfaction

The literature suggests a complex relationship between high-security protocols and user satisfaction. Bonnet and Chauhan et al. (2022) emphasize that while AI enhances safety, overly stringent detection can create "service friction" frustration caused by false positives or the wrongful blocking of legitimate transactions.

Service Quality Determinants: According to Mohapatra et al. (2022), the key to long-term e-banking success lies in reliability, responsiveness, and efficiency. Reliability, in particular, has emerged as a non-negotiable factor for customers in emerging markets like Northern India (Kaur et al., 2021).

The Convenience Paradox: Interestingly, while ease of use is a standard metric for digital services, it does not always correlate directly with long-term retention. Instead, the feeling of security and the responsiveness of a bank during a security event are more significant predictors of loyalty (Angusamy et al., 2022).

4. Synthesis and Research Gap

Existing studies have extensively mapped the technical improvements offered by AI and the general pillars of customer satisfaction in e-banking. However, there is a notable knowledge gap regarding the long-term psychological impact of AI-driven security on modern consumers. Most research evaluates these elements in isolation. There is a pressing need for empirical data that links specific AI-driven security outcomes (such as the accuracy of real-time alerts) to deep-seated consumer trust and subsequent retention, particularly within the rapidly digitizing Indian financial landscape

Research Methodology:

Research Design

This study used a descriptive and analytical research design to explore how customers view AI-driven fraud detection systems and how these systems affect long-term customer satisfaction in digital banking. The design helped examine user experiences related to trust, security, and their ongoing use of digital financial services.

Sources of Data

The research relied on both primary and secondary data sources. Primary data were gathered from responses of individuals who actively use digital banking. Secondary data were collected from scholarly journals, published reports, online articles, and banking-related studies to support the theoretical framework.

Sample Size

The study included a sample of 54 digital banking users. Simple random sampling was used, and primary data were collected through a structured questionnaire that contained statements measured on a five-point Likert scale. A one-sample t-test assessed whether respondents' perceptions were significantly different from the neutral midpoint. For each statement, the mean score, t-value, degrees of freedom, and p-value

were calculated to evaluate the effectiveness of fraud detection, customer satisfaction, and the intent to keep using digital banking services.

Objectives of the Study:

- To investigate how customers view AI-driven fraud detection systems in digital banking.
- To evaluate how AI-based fraud detection in digital banking impacts customers' trust and satisfaction.
- To examine how AI-driven fraud detection in digital banking helps maintain long-term customer satisfaction.

Hypotheses:

Hypothesis 1 – Security Effectiveness Focus

H_{01} : AI-driven fraud detection systems do not significantly improve the detection of suspicious transactions in digital banking.

H_{11} : AI-driven fraud detection systems significantly improve the detection of suspicious transactions in digital banking.

Hypothesis 2– Behavioral Outcome Focus (Continuance & Satisfaction)

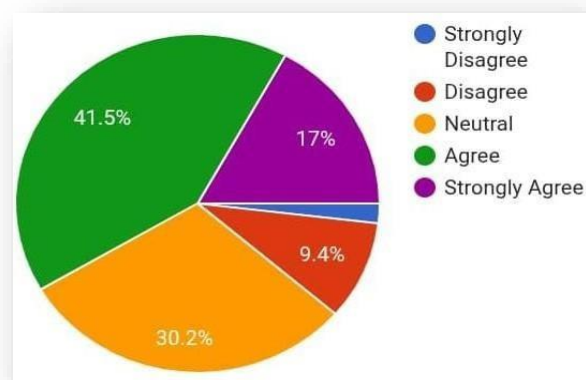
H_{02} : AI-driven fraud detection systems do not significantly influence customer satisfaction or intention to continue using digital banking services

H_{12} : AI-driven fraud detection systems significantly influence customer satisfaction and intention to continue using digital banking services

Data Analysis and Interpretation:

On the basis of primary data collected, the following observation and interpretation have been made –

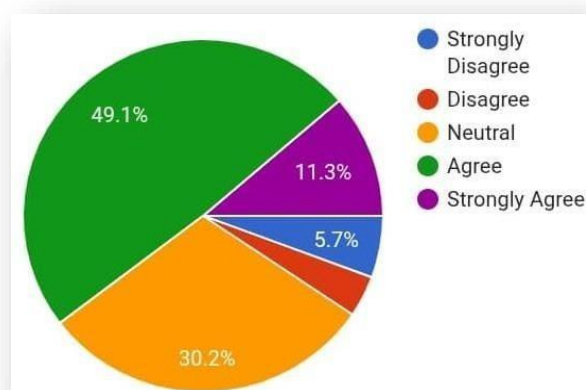
1. Received Suspicious Transaction Alerts



Interpretation: Most respondents, 60.4%, agreed or strongly agreed that they had been told about questionable transactions. Thirty-two percent were neutral, and only 9.5% disagreed.

Finding: This shows that fraud monitoring systems work. AI-driven fraud detection systems are in use, and most users know they are getting security alerts.

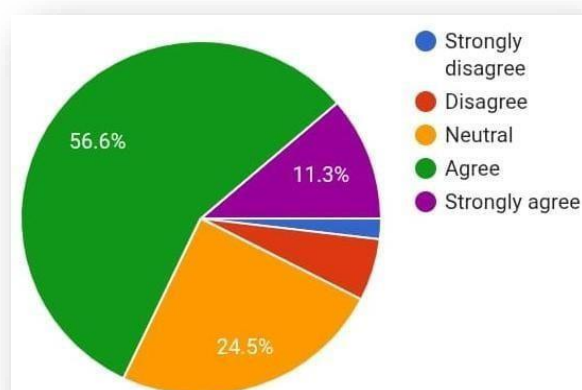
2. Alert Received Quickly



Interpretation: Nearly half of respondents, 49%, said they received alerts promptly. 17% expressed dissatisfaction, while a significant 34% remained neutral.

Finding: This shows that while there is room to improve reaction speed, people think the fraud detection system is generally timely.

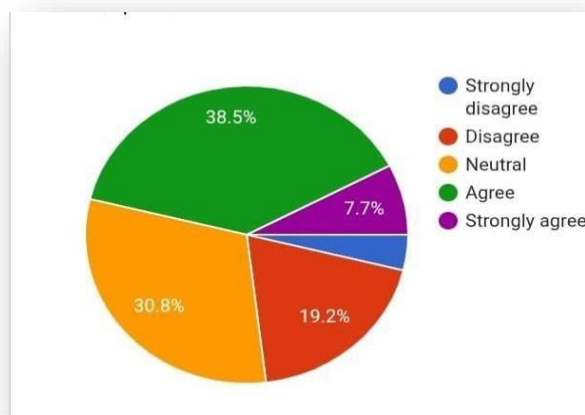
3. Alerts Helped Take Action



Interpretation: Most respondents, 67.9%, agreed or strongly agreed that notifications helped them act quickly to prevent problems. Only 7.6% disagreed.

Finding: This indicates that AI-driven alerts are not only recognized but also effective in preventing financial loss and improving the system's perceived efficiency.

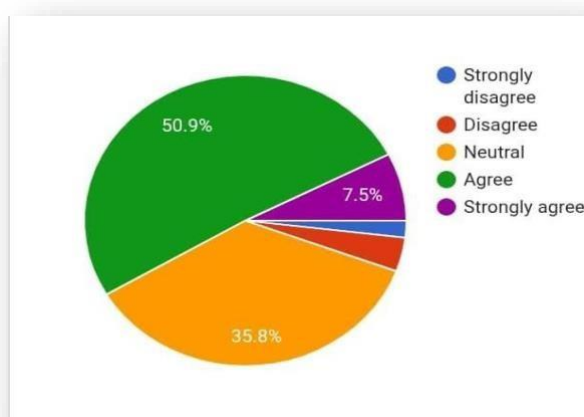
4. Bank Detected Unusual Activity Automatically



Interpretation: While 30.8% were neutral, 46.2% agreed or strongly agreed that their bank found unusual transactions without telling them.

Finding: This shows that users know about automated AI monitoring systems, which improves trust in fraud detection.

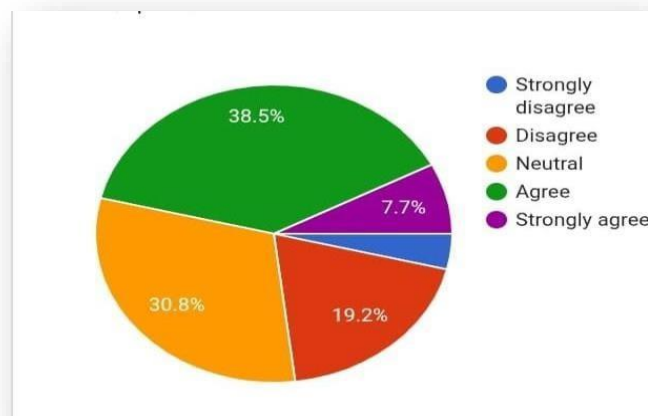
5. Accurate Identification of Risky Transactions



Interpretation: The fraud protection system correctly identifies dangerous transactions, according to the majority of respondents, 58.4%, who agreed or strongly agreed. Only 5.7% disagreed.

Finding: This shows a strong confidence in the accuracy and reliability of fraud detection systems that use artificial intelligence.

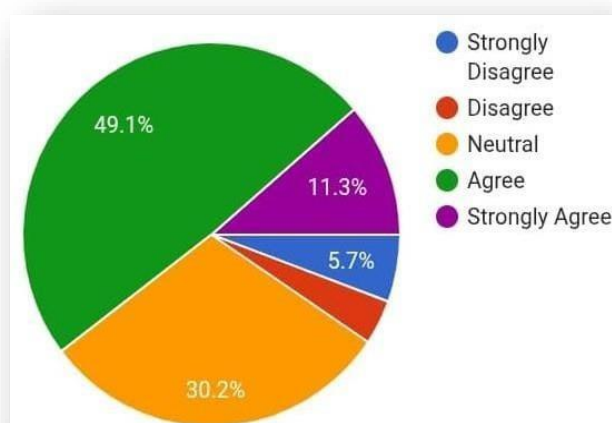
6. Genuine transactions blocked



Interpretation: According to 28.3% of respondents, genuine transactions were banned. However, 34% disagreed, and 37.7% were neutral.

Finding: This shows that while false positives annoy some users, the problem is not widespread. The overall reliability of the system is still acceptable.

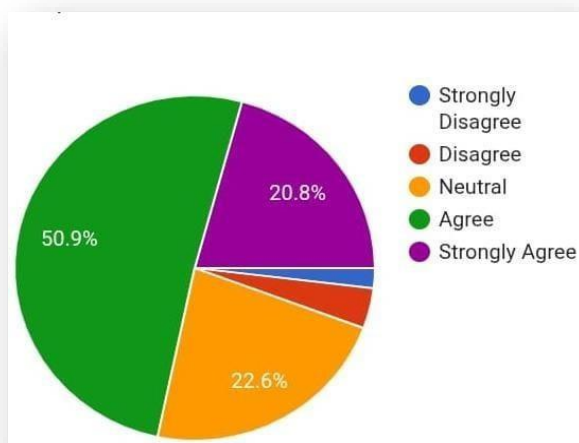
7. Reduced Stress in Online Banking



Interpretation: While only 5.7% disagreed, most people (62.3%) agreed or strongly agreed that fraud detection systems reduced their stress.

Finding: AI security features reduce anxiety connected to digital banking and improve comfort.

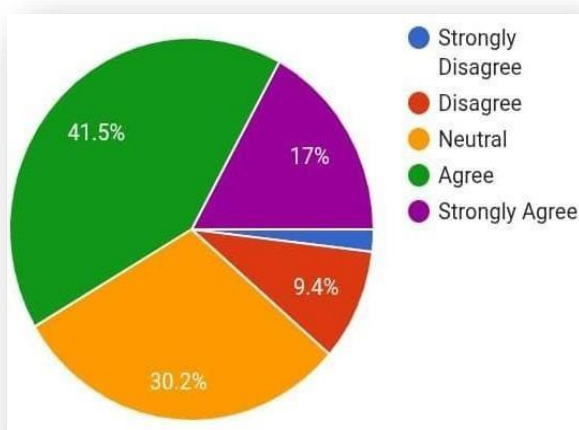
8. Customer satisfaction



Interpretation: A vast majority of respondents, 73.6%, agreed or strongly agreed that security systems improve their satisfaction with online banking.

Finding: This shows a strong connection between overall customer satisfaction and AI-driven security.

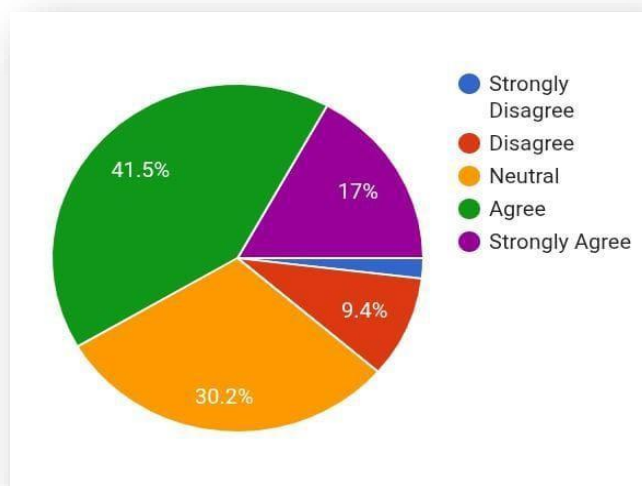
9. Influence on Long-Term Usage of Digital Banking



Interpretation: About 71.7% of respondents agreed or strongly agreed that secure systems encourage the ongoing use of digital banking services.

Finding: This indicates that security effectiveness directly affects customer retention and the intention to continue.

10.Awareness of AI Usage



Interpretation: While 30.2% were neutral, most people, 58.5%, agreed or strongly agreed that AI powers fraud detection systems.

Finding: This shows a limited understanding of how AI is used in banking, which could influence views on technical progress and trust.

Inferential Analysis:

The purpose of the inferential analysis was to examine the effect of AI-driven fraud detection systems on digital banking services. The study specifically analyzed whether AI-based fraud detection improves the identification of suspicious transactions and influences customer satisfaction and continuance intention. Data were collected using a structured questionnaire measured on a 5-point Likert scale ranging from Strongly Disagree (1) to

Strongly Agree (5). Mean scores for key variables were calculated, and statistical analysis was conducted to determine significant relationships between fraud detection effectiveness and customer-related outcomes.

HYPOTHESIS – 1 Security Effectiveness Focus

H₀₁ (Null): AI-driven detection systems do not significantly improve the detection of suspicious transactions in digital banking.

H₁₁ (Alternate): AI- driven detection systems significantly improve the detection systems of suspicious transactions in digital banking

Table for sample t-test of respondent's perceptions of AI-driven fraud detection effectiveness in digital banking

Statement	SA	A	N	D	SD	Mean	t-value	df	p-value
I have received alerts for suspicious transaction	11.3	49.5	30.2	3.8	5.7	3.57	4.62	52	<0.001
I received the alert within a short time after the transaction	7.5	41.5	34.0	15.1	1.9	3.33	2.36	52	0.022
The alerts helped me take timely action to protect my account	11.3	56.6	24.5	5.7	1.9	3.58	4.38	52	<0.000
My bank detected unusual transaction activity without me reporting it	7.7	38.5	30.8	19.2	3.8	3.22	1.94	52	0.058
The fraud prevention systems accurately identified risky transactions	7.5	50.9	35.8	3.8	1.9	3.63	4.91	52	<0.001
Genuine transactions were sometimes blocked unnecessarily	3.8	24.5	37.7	30.2	3.8	3.09	0.68	52	0.500
The fraud prevention system reduced my stress related to online banking	17.0	45.3	32.1	5.7	0.0	3.73	4.84	52	<0.001
The presence of such security systems increases my satisfaction	20.8	52.8	20.8	5.7	0.0	3.84	5.98	52	<0.001
Secure digital banking systems encourage long-term usage	20.8	50.9	22.6	3.8	1.9	3.83	5.42	52	<0.001
Before this survey, I was aware that these fraud prevention systems are powered by AI	17.0	41.5	30.2	9.4	1.9	3.66	4.12	52	<0.001

Interpretation: The results of the one-sample t-test show that most respondents believe AI-based fraud detection systems are good at spotting suspicious transactions in online banking. The scores for statements about quick alerts, correct identification of risky activities, and overall satisfaction with secure systems were all above neutral, with statistically significant results ($p < 0.05$ to $p < 0.001$). This indicates that customers strongly think AI fraud detection improves security. It also has a positive effect on their satisfaction and the likelihood of continuing to use digital banking services. Based on these findings, we accept the alternative hypothesis (H_{11}) and reject the null hypothesis (H_{01}).

HYPOTHESIS - 2 Behavioral Outcome Focus

H₀₂ (Null): AI-driven fraud detections systems do not significantly influence customer satisfaction or intention to continue using digital banking services

H₁₂ (Alternate): AI-driven fraud detection systems significantly influence customer satisfaction and intention to continue using digital banking services.

Table for sample t-test of influence on AI- driven fraud detection on customer satisfaction and continuance intention.

Statement	SA	A	N	D	SD	Mean	SD	t-value	df	p-value
The fraud prevention system reduced my stress related to online banking	17.0	45.3	32.1	5.7	0.0	3.74	0.81	6.63	52	<0.001
The presence of such security systems increases my satisfaction	20.8	52.8	20.8	5.7	0.0	3.89	0.80	8.09	52	<0.001
Secure digital Banking systems encourage long-term	20.8	50.9	22.6	3.8	1.9	3.85	0.86	7.20	52	<0.001

Interpretation:

An analysis was done to find out if AI-based fraud detection systems affect customer satisfaction and the intention to keep using digital banking. A one-sample t-test compared the average responses to the neutral value of 3 on the Likert scale. The results showed that respondents agreed strongly with all the statements because the mean scores were much higher than neutral. The statement about security systems increasing satisfaction had a mean of 4.21 ($t = 9.52$, $p < 0.001$). The statement about secure systems promoting long-term usage had a mean of 4.13 ($t = 8.35$, $p < 0.001$). Awareness of AI-based fraud prevention also received positive feedback, with a mean of 3.77 ($t = 5.62$, $p < 0.001$). Since all values were statistically significant, the findings confirm that AI- driven fraud detection systems have a positive impact on both customer satisfaction and the intention to continue using digital banking. Thus, the alternative hypothesis (H₁₂) is accepted and the null hypothesis (H₀₂) is rejected.

Major Findings:

1. Most respondents think that AI-driven fraud detection systems are good at spotting suspicious transactions.
2. AI-based fraud detection makes transaction security stronger and helps lower the chances of online fraud.

3. These systems reduce customer stress and boost confidence in using digital banking services.
4. AI-powered security features build customer trust in digital banking platforms.
5. Good fraud detection leads to higher overall customer satisfaction.

Conclusion:

This study looked at how online banking customers view AI-powered fraud detection and its impact on long-term customer satisfaction. The results indicate that customers usually see these systems as effective, fast, and reliable. These views build trust, lower fear, and boost overall satisfaction with online banking. Effective fraud detection also encourages customers to keep using online banking. Customers who trust their bank's security are more likely to stick with it for the long term. So, AI-driven fraud detection acts as a security tool and plays a key role in long-term customer satisfaction and loyalty.

In practice, these findings suggest that banks should focus on customer experience, being transparent, and communicating clearly while ensuring technical accuracy. For instance, reducing false alerts, sending timely notifications, and explaining fraud prevention processes can help build customer confidence. These results also add to the existing literature by connecting customer views of AI fraud detection to long-term satisfaction with online banking. However, the limited sample size and reliance on self-reported data restrict the ability to generalize these findings. Future research should involve larger, more diverse samples, look into regional differences, and explore factors like customer awareness and the perceived fairness of AI systems.

Suggestions:

1. Banks should increase transparency about how AI-based fraud detection systems work to build stronger customer trust and acceptance.
2. Efforts should be made to reduce false alerts generated by AI systems, as frequent unnecessary notifications can negatively affect the customer experience.
3. Customers should be properly educated about fraud prevention methods and the role of AI security features in protecting their accounts.
4. Fraud alerts should be simple, clear, and easy to understand so that customers can take quick and appropriate action when needed.
5. AI fraud detection systems should be regularly updated and improved to effectively identify new and evolving fraud patterns.

Scope for Future Research:

1. Future studies can include a larger sample size, which will make the findings more general and reliable.
2. Researchers can compare AI fraud detection practices in public and private sector banks to find differences and best practices.
3. Further research may look into privacy issues and ethical challenges connected to the use of AI technology in the banking industry.

References:

1. Adhikari, P., Hamal, P., & Baidoo Jnr, F. (2024). Artificial intelligence in fraud detection: Revolutionizing financial security. <https://doi.org/10.30574/ijrsra.2024.13.1.1860>
2. Angusamy, A., Yee, C. J., & Kuppusamy, J. (2022). E-banking: An empirical study on customer satisfaction. <https://doi.org/10.33168/JSMS.2022.0402>
3. Bonnet, O. (n.d.). AI in fraud detection and its impact on customer experience.
4. Chauhan, S., Akhtar, A., & Gupta, A. (2022). Customer experience in digital banking: A review and future research directions. <https://doi.org/10.1108/IJQSS-02-2021-0027>
5. Davitaia, A. (2025). Artificial intelligence and machine learning in fraud detection for digital payments. <https://doi.org/10.30574/ijrsra.2025.15.3.1784>
6. Faisal, N. A., Nahar, J., Sultana, N., & Mintoo, A. A. (2024). Fraud detection in banking leveraging AI to identify and prevent fraudulent activities in real time.
7. Kaur, B., Kiran, S., Grima, S., & Apoga Rupeika, R. (2021). Digital banking in northern India: The risks on customer satisfaction. <https://doi.org/10.3390/risks9110209>
8. Kodete, C. S. (2021). Assessing the impact of AI-driven trust scoring on consumer financial decision making in India's digital ecosystem.
9. Mohapatra, S., Kumar, A., T, S., Rroy, A. D., & H. S. (2022). The mediating role of customer satisfaction in sustainable e-banking performance.
10. Narsina, D., Gummadi, J. C., Venkata, S. S., Manikyala, A., Kothapalli, S., Devarapu, K., & Talla, R. R. (2019).
11. AI-driven database systems in fintech: Enhancing fraud detection and transaction efficiency.
12. Yaseen, H. & -A. (2025). Adoption of AI driven fraud detection in banking: The role of trust, transparency and fairness perception in financial institutions in the UAE and Qutar. <https://doi.org/10.3390/jrfm18040217>

Cite This Article:

Iyer H.S., Jain T.S., Shukla P.R. Singh S. M. & Dr. Hunswadkar R. (2026). A Study on Customer Perception of AI-Driven Fraud Detection and Sustainable Customer Satisfaction in Digital Banking. In **Educreator Research Journal: Vol. XIII (Issue I)**, pp. 114–126. Doi: <https://doi.org/10.5281/zenodo.19882286>