

Impact of Artificial Intelligence-Based Security Mechanisms on Customer Trust in Fintech Services: A Perceptual Study in Karnataka

Ms. Anusha Kalburgikar¹,

¹Research Scholar, University of Mysore, Karnataka, India
Assistant Professor, Department of Commerce and Management
Dayananda Sagar College of Arts, Science and Commerce
Kumaraswamy Layout, Bengaluru - 560111

anushakalburgikar@gmail.com + 91 9902910384

Dr. T K Srinath²

²Professor, Department of Commerce & Management, Al-Ameen Research Foundation,
Bangalore, Karnataka, India

srinathtk57@gmail.com + 91 + 91 9880034190

Abstract

The rapid growth of Financial Technology (FinTech) services has transformed the financial ecosystem by enabling fast, convenient and Technology-driven financial transactions. However, increasing dependence on Digital Financial platforms has intensified concerns regarding cyber fraud, privacy breaches and transaction Security. Artificial Intelligence (AI)-based Security mechanisms such as biometric authentication, fraud detection systems, predictive analytics and real-time Cyber Security monitoring are increasingly implemented to strengthen Customer Trust and ensure secure Digital Financial transactions. In this context, the present study examines the impact of AI-based Security mechanisms on Customer Trust in FinTech services in Karnataka. The study adopts a descriptive and analytical research design using primary data collected from 300 FinTech users through a structured questionnaire. Statistical tools such as descriptive statistics, reliability analysis, correlation, regression and Structural Equation Modeling (SEM) were employed for analysis. The findings reveal that AI-driven fraud detection, biometric authentication, Perceived Cyber Security, privacy protection and system reliability significantly influence Customer Trust and continuance intention. AI-based fraud detection emerged as the strongest predictor of Customer Trust. The study concludes that effective implementation of AI-enabled Security systems enhances user confidence and promotes sustainable FinTech adoption. The research provides valuable insights for FinTech companies, policymakers and regulators in strengthening secure Digital Financial ecosystems in Karnataka.

Keywords: *Artificial Intelligence, FinTech Services, Customer Trust, Cyber Security, Fraud Detection, Biometric Authentication, Karnataka.*

Introduction

Financial Technology (FinTech) has emerged as one of the most significant innovations in the modern financial ecosystem. The integration of advanced technologies such as Artificial Intelligence (AI), Machine Learning (ML), Blockchain, Cloud Computing and Big Data Analytics has revolutionized the delivery of financial services. FinTech platforms provide customers with convenient, efficient and real-time access to Digital Payments, Online banking, Lending, Investment and Insurance services.

India has witnessed rapid FinTech expansion due to initiatives such as Digital India, increasing smartphone penetration and the widespread adoption of Unified Payments Interface (UPI). Karnataka, especially Bengaluru, being India's leading technological and startup hub, has experienced substantial growth in FinTech services. However, along with increased digital financial transactions, concerns regarding Cyber Security threats, cyber fraud, phishing attacks, privacy breaches and unauthorized access have also intensified.

Artificial Intelligence-based Security mechanisms are increasingly adopted by FinTech companies to strengthen Security infrastructure and improve customer confidence. AI-driven technologies such as biometric authentication, facial recognition, fraud analytics, predictive Cyber Security systems and anomaly detection play a crucial role in identifying suspicious transactions and preventing cyber threats.

Customer Trust is considered a fundamental factor influencing FinTech adoption and continuance intention. Users are more likely to engage with FinTech services when they perceive platforms as secure, reliable and technologically advanced. AI-enabled Security systems not only reduce Perceived risk but also create confidence regarding transaction safety and privacy protection.

Therefore, examining the relationship between AI-based Security mechanisms and Customer Trust becomes essential for understanding sustainable FinTech adoption. The present study focuses on analyzing the impact of Artificial Intelligence-based Security mechanisms on Customer Trust in FinTech services in Karnataka.

Statement of the Problem

The rapid growth of FinTech services has increased customer dependence on Digital Financial platforms for Payments, Banking and Investment activities. However, increasing cases of cyber fraud, phishing attacks, identity theft and privacy breaches continue to affect customer confidence in Digital Financial ecosystems. To address these issues, FinTech firms are increasingly implementing AI-based Security mechanisms such as fraud detection systems, biometric authentication and predictive Cyber Security monitoring.

Despite the growing adoption of AI-enabled Security technologies, limited empirical research exists regarding how customers perceive these mechanisms and how they influence Trust in FinTech services, particularly in Karnataka. Therefore, the study attempts to examine the impact of Artificial Intelligence-based Security mechanisms on Customer Trust in FinTech services in Karnataka.

Review of Literature

1. **Davis (1989) [1]** introduced the Technology Acceptance Model (TAM) to explain user acceptance of Technological systems. The study identified Perceived usefulness and Perceived ease of use as the primary determinants influencing Technology adoption behaviour. Using behavioural intention analysis, the research found that users are more likely to adopt digital systems when they perceive them as beneficial and easy to operate. The author concluded that Technology acceptance depends largely on User perception regarding efficiency and convenience.
 2. **Mayer, Davis and Schoorman (1995) [2]** developed an integrated model of Organizational Trust and examined the dimensions influencing Trust formation. The study identified ability, integrity and benevolence as the major factors affecting Trust in Technology-driven environments. Using conceptual Trust modeling, the authors found that Trust significantly reduces Uncertainty and Perceived Risk. The study concluded that strong institutional reliability and competence enhance long-term Customer Trust.
 3. **Gefen (2000) [3]** examined the role of Trust in e-commerce adoption using behavioural
-

intention analysis. The study found that Trust significantly influences consumers' willingness to engage in online transactions. Security assurance and system reliability positively affected customer confidence in digital systems. The author concluded that Trust acts as a critical mechanism in encouraging user participation in online financial environments.

4. **Pavlou (2003) [4]** investigated consumer acceptance of electronic commerce by integrating Trust and Perceived risk into Technology adoption models. Using Structural Equation Modeling (SEM), the study found that Trust significantly reduces uncertainty and positively influences transaction intention. Perceived Security emerged as a strong predictor of online transaction behaviour. The author concluded that secure technological infrastructure is essential for strengthening digital Trust.
 5. **Venkatesh et al. (2003) [5]** proposed the Unified Theory of Acceptance and Use of Technology (UTAUT) model to explain Technology adoption behaviour. Using empirical behavioural analysis, the study identified performance expectancy, effort expectancy, social influence and facilitating conditions as major determinants influencing behavioural intention. The authors concluded that technological acceptance depends on both individual perception and external facilitating factors.
 6. **Kim, Ferrin and Rao (2008) [6]** examined Trust and satisfaction in online transaction systems using regression analysis. The study found that Perceived Security and privacy protection significantly influence Customer Trust and online purchase intention. The authors reported that Security assurance reduces Perceived risk and enhances confidence in digital transactions. The study concluded that secure payment systems are essential for sustaining customer satisfaction and Trust.
 7. **Zhou (2011) [7]** explored factors influencing Trust in mobile banking services using Structural Equation Modeling. The study found that system quality, information quality and Security assurance significantly influence Customer Trust and adoption intention. The findings revealed that secure technological infrastructure positively affects user satisfaction and continuance behaviour. The author concluded that Trust mediates the relationship between technological quality and behavioural intention.
 8. **Oliveira et al. (2014) [8]** investigated mobile payment adoption behaviour using an
-

integrated Technology acceptance framework. The study found that Trust, innovation and Perceived Security significantly influence adoption intention. Users were more willing to adopt mobile financial services when platforms were Perceived as technologically reliable and secure. The authors concluded that Security assurance is critical for encouraging digital payment adoption.

9. **Slade et al. (2015) [9]** examined mobile payment adoption and identified Trust and Perceived risk as major determinants influencing user behaviour. Using behavioural analysis, the study found that Security concerns negatively affect adoption intention, while Trust positively strengthens willingness to use mobile payment systems. The authors concluded that improving Cyber Security infrastructure is essential for sustaining mobile payment adoption.
 10. **Chuang, Liu and Kao (2016) [10]** examined Customer Trust in Digital Financial services using empirical survey analysis. The study found that privacy protection and transaction Security significantly influence Trust formation. Customers were more likely to continue using digital platforms when strong Security mechanisms and transparent privacy policies were present. The authors concluded that transaction Security plays a vital role in strengthening customer confidence.
 11. **Alalwan et al. (2017) [11]** explored mobile banking adoption behaviour using the UTAUT framework. The study found that technological reliability, Trust and ease of use significantly influence customer intention to adopt Digital Financial services. The authors reported that secure systems positively affect customer perception and confidence. The study concluded that Cyber Security mechanisms are essential for strengthening digital banking adoption.
 12. **Singh and Sinha (2020) [12]** analyzed customer perception regarding Cyber Security in digital payment platforms using survey-based analysis. The study found that Perceived Cyber Security and system reliability significantly influence Customer Trust and Usage behaviour. Increasing cyber fraud incidents heightened customer sensitivity toward transaction Security. The authors concluded that stronger Cyber Security infrastructure is essential for sustaining Trust in Digital Financial ecosystems.
 13. **Venkatesh et al. (2020) [13]** extended the Unified Theory of Acceptance and Use of
-

Technology-2 (UTAUT2) framework to explain continuance intention in Digital Financial platforms. Using behavioural modeling, the study found that habit formation, Trust and performance expectancy significantly influence continued usage behaviour. Repeated positive experiences transformed intentional usage into habitual behaviour. The authors concluded that Trust and System Reliability are crucial for sustaining long-term engagement with Digital Financial services.

14. **Tamilmani, Rana and Dwivedi (2021) [14]** examined behavioural intention in FinTech adoption using empirical modelling techniques. The study identified Trust as a major psychological mechanism influencing user behaviour. Technological efficiency, Perceived Security and customer satisfaction significantly affected Trust formation. The authors concluded that customers are more willing to adopt FinTech platforms when systems are secure and technologically advanced.
15. **Oliveira, Thomas and Espadanal (2021) [15]** investigated continuance intention in mobile payment services using Structural Equation Modeling. The study found that Customer Trust and satisfaction strongly influence continued usage behaviour. Trust developed through repeated positive experiences and secure transactions. The authors concluded that improving Cyber Security systems and customer experience is essential for ensuring sustained Digital Financial engagement.
16. **Goh and Sun (2022) [16]** examined the influence of Trust and Perceived risk on FinTech adoption behaviour. Using regression analysis, the study found that Perceived risk negatively affects user intention, while Trust positively strengthens engagement with Digital Financial services. Security assurance and technological transparency reduced uncertainty and improved customer confidence. The authors concluded that Cyber Security mechanisms play a significant role in strengthening Trust in FinTech ecosystems.
17. **Li et al. (2022) [17]** explored FinTech adoption behaviour across diverse user groups using comparative empirical analysis. The study found that Trust, Perceived Security and regulatory support significantly influence customer intention. Users were more likely to engage with FinTech services when strong Security mechanisms and institutional safeguards were present. The Authors concluded that regulatory assurance strengthens

confidence in Digital Financial systems.

18. **Hasan, Pal and Vanijja (2023) [18]** examined Customer Trust in UPI-based payment systems in India using survey-based empirical analysis. The study revealed that Perceived Cyber Security, transaction safety and secure authentication significantly strengthen customer confidence. Advanced Security mechanisms such as biometric authentication and fraud monitoring positively influenced Trust formation. The authors concluded that Cyber Security systems are essential for sustaining digital payment adoption.
19. **Sharma and Kulkarni (2025) [19]** examined post-pandemic digital payment continuance behaviour in metropolitan India using a Structural Equation Modeling approach. The study found that habit formation emerged as the strongest predictor of continuance intention, surpassing Perceived usefulness. Repeated exposure to digital payments during COVID-19 accelerated behavioural automation and transformed deliberate usage into routine financial behaviour. The authors concluded that Trust and system reliability significantly strengthen long-term engagement with Digital Financial services.
20. **Mehta et al. (2025) [20]** investigated the role of Artificial Intelligence-based fraud detection systems in strengthening Customer Trust in FinTech services. Using empirical behavioural analysis, the study found that AI-enabled fraud monitoring, predictive Cyber Security systems and real-time transaction alerts significantly improve customer confidence and reduce Perceived financial risk. Biometric authentication and AI-driven anomaly detection enhanced transaction Security and continuance intention. The authors concluded that AI-based Security mechanisms are becoming essential components of sustainable Digital Financial ecosystems.

Research Gap

Existing studies have extensively examined FinTech adoption, Perceived Security and Customer Trust. However, limited studies have specifically focused on Artificial Intelligence-based Security mechanisms and their influence on Customer Trust in FinTech services. Furthermore, very few studies integrate AI-driven fraud detection, biometric authentication, Cyber Security perception and continuance intention into a single empirical framework. Therefore, the present study attempts to bridge this gap by analyzing the impact of AI-enabled Security systems on Customer Trust in

Karnataka.

Significance of the Study

The study contributes to the growing literature on FinTech and digital Trust by integrating Artificial Intelligence-based Security mechanisms into Customer Trust models. The findings provide valuable insights for FinTech companies, regulators and policymakers to strengthen AI-enabled Cyber Security infrastructure and enhance User confidence. The study also supports the development of secure and sustainable Digital Financial ecosystems in Karnataka.

Objectives of the Study

- To examine the impact of AI-based Security mechanisms on Customer Trust in FinTech services.
- To analyze the influence of biometric authentication on Customer Confidence.
- To assess the relationship between Perceived Cyber Security and Customer Trust.
- To evaluate the effect of System Reliability and privacy protection on continuance intention.
- To suggest suitable measures for strengthening AI-enabled Security systems in FinTech platforms.

Hypotheses of the Study

- H1: AI-based fraud detection significantly influences Customer Trust.
- H2: Biometric authentication significantly influences Customer Trust.
- H3: Perceived Cyber Security significantly influences Customer Trust.
- H4: Privacy protection significantly influences Customer Trust.
- H5: System reliability significantly influences Customer Trust.
- H6: Customer Trust significantly influences Continuance Intention.
- H7: AI-based Security mechanisms indirectly influence Continuance Intention through Customer Trust.

Research Methodology

The study adopts a descriptive and analytical research design. Primary data were collected from 300 FinTech users in Karnataka using a structured questionnaire based on a five-point Likert scale. Convenience sampling technique was adopted for selecting respondents. Secondary data were collected from journals, RBI reports, books, FinTech publications and credible online sources.

Statistical Tools Used

Descriptive Statistics

Reliability Analysis

Correlation Analysis

Multiple Regression Analysis

Structural Equation Modeling (SEM)

Questionnaire Development and Validation

The questionnaire was developed based on established literature relating to FinTech adoption, Customer Trust, Cyber Security and Artificial Intelligence-based Security mechanisms. The measurement items were adapted from previous studies including Davis (1989), Mayer et al. (1995), Kim et al. (2008), Zhou (2011), Hasan et al. (2023), and Mehta et al. (2025). A five-point Likert scale ranging from Strongly Disagree (1) to Strongly Agree (5) was used to measure respondent perceptions.

A pilot study was conducted among selected FinTech users to assess the clarity, relevance, and appropriateness of the questionnaire items. Based on expert suggestions and respondent feedback, minor modifications were incorporated. Content validity was established through expert review by academicians and researchers in the areas of FinTech and Digital Finance. The reliability of the instrument was confirmed through Cronbach's Alpha values, which exceeded the recommended threshold of 0.70.

Measurement scales for the study constructs were adapted from established literature in the fields of Technology adoption, Customer Trust, Cyber Security, and FinTech services. AI-Based Fraud Detection items were adapted from Mehta et al. (2025), while Biometric Authentication and Perceived Cyber Security measures were adapted from Hasan et al. (2023). Privacy Protection items were adapted from Kim, Ferrin and Rao (2008), and System Reliability measures were derived from Zhou (2011). Customer Trust items were adapted from Mayer et al. (1995) and Gefen (2000), whereas Continuance Intention items were adapted from Oliveira et al. (2021) and Venkatesh et al. (2020). Minor modifications were made to suit the

FinTech context in Karnataka while retaining the conceptual meaning of the original scales. Content validity was established through expert evaluation involving academicians and researchers specializing in FinTech, Digital Finance, and Research Methodology. The experts assessed the relevance, clarity, and adequacy of each measurement item. Construct validity was examined through factor loading assessment and inter-construct correlations. The results indicated that all constructs adequately represented their respective theoretical dimensions, thereby confirming acceptable construct validity of the measurement instrument.

Data Collection Methods

Primary Data

Primary data was collected using a structured questionnaire distributed among FinTech users in Karnataka. The questionnaire included Likert-scale statements relating to AI Fraud Detection, Biometric Authentication, Cyber Security Perception, Privacy Protection, System Reliability and Customer Trust.

Secondary Data

Secondary data was collected from Research Journals, RBI reports, FinTech Publications, Government Documents and Academic Databases.

Table 1: Demographic Profile of Respondents (n = 300)

Variable	Category	Frequency	Percentage (%)
Gender	Male	168	56
	Female	132	44
Age	Below 25 Years	72	24
	25–35 Years	126	42
	36–45 Years	63	21
	Above 45 Years	39	13
Educational Qualification	Undergraduate	84	28
	Postgraduate	144	48
	Professional Qualification	72	24
Occupation	Student	54	18

	Salaried Employee	153	51
	Business/Self-employed	63	21
	Others	30	10

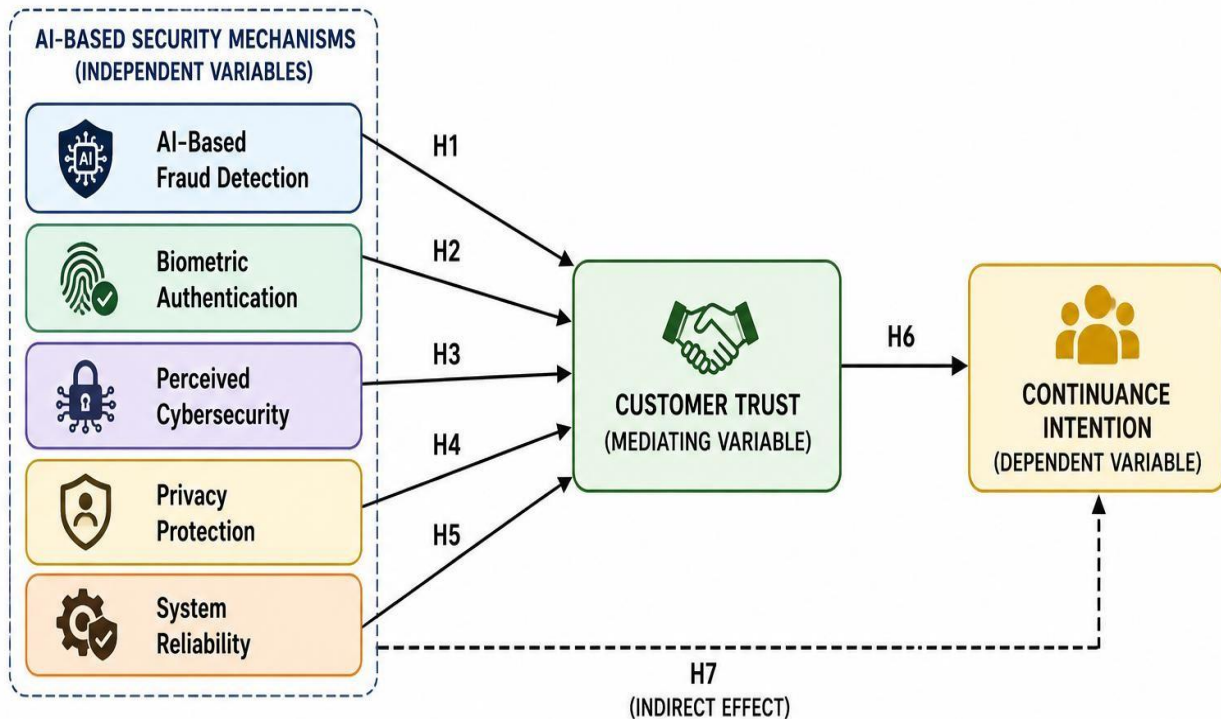
Interpretation

The demographic profile indicates that a majority of the respondents were male (56%) and belonged to the age group of 25–35 years (42%), reflecting the dominant user segment of FinTech services. Most respondents possessed postgraduate qualifications (48%), indicating a relatively educated user base. Salaried employees constituted the largest occupational category (51%), suggesting that working professionals are among the major users of AI-enabled FinTech services in Karnataka. The diversity of respondents across age, education, and occupation categories provides a broader understanding of customer perceptions regarding AI-based Security mechanisms and Trust in FinTech services.

Limitations of the Study

- The study is limited to FinTech users in Karnataka only.
- Responses are based on Customer perceptions and may contain bias.
- The study considers only selected AI-based Security mechanisms.
- Rapid Technological changes may affect future findings.
- The use of convenience sampling may limit the generalization of findings to the entire population of FinTech users.
- The study adopts a cross-sectional approach and hence does not capture changes in Customer perceptions over time.

Conceptual Framework



The conceptual model explains how **AI-Based Security Mechanisms** influence **Customer Trust** and ultimately affect **Continuance Intention** in FinTech services.

The independent variables include:

- AI-Based Fraud Detection
- Biometric Authentication
- Perceived Cyber Security
- Privacy Protection
- System Reliability

These variables positively influence **Customer Trust**, which acts as the mediating variable. Higher Customer Trust leads to greater **Continuance Intention**, meaning customers are more willing to continue using FinTech services. The model also shows an indirect effect where AI-based Security mechanisms improve Continuance Intention through Customer Trust.

Data Analysis and Interpretation

Table 1: Descriptive Analysis

Construct	Mean	Std. Deviation
-----------	------	----------------

AI Fraud Detection	4.20	0.58
Biometric Authentication	4.12	0.60
Perceived Cyber Security	4.24	0.55
Privacy Protection	4.08	0.63
System Reliability	4.16	0.57
Customer Trust	4.26	0.54
Continuance Intention	4.30	0.52

Interpretation: All variables recorded mean values above 4.00, indicating strong positive customer perception toward AI-based Security mechanisms in FinTech services. Customer Trust and Continuance Intention recorded the highest mean values, showing strong confidence in secure FinTech platforms.

Table 2: Reliability Analysis

Construct	Cronbach's Alpha
AI Fraud Detection	0.90
Biometric Authentication	0.87
Perceived Cyber Security	0.91
Privacy Protection	0.84
System Reliability	0.88
Customer Trust	0.92
Continuance Intention	0.89
Overall Scale	0.94

Interpretation: All constructs recorded Cronbach's Alpha values above 0.70, confirming strong internal consistency and reliability of the measurement scale.

Table 3: Correlation Analysis

Variables	AIFD	BA	PCS	PP	SR	CT	CI
AI Fraud Detection	1						
Biometric Authentication	0.69	1					
Perceived Cyber Security	0.73	0.70	1				
Privacy Protection	0.65	0.62	0.71	1			
System Reliability	0.72	0.68	0.74	0.70	1		
Customer Trust	0.80	0.76	0.83	0.75	0.81	1	
Continuance Intention	0.78	0.73	0.82	0.72	0.79	0.87	1

Interpretation: All variables show strong positive correlations with Customer Trust and Continuance Intention. Perceived Cyber Security and System Reliability recorded strong relationships with Customer Trust, indicating the importance of Security perception in FinTech Usage behaviour.

Table 4: Multiple Regression Analysis

Dependent Variable: Customer Trust

Predictor	Beta (β)	t-value	Sig.
AI Fraud Detection	0.38	7.48	0.000
Biometric Authentication	0.29	5.96	0.000
Perceived Cyber Security	0.35	6.94	0.000
Privacy Protection	0.22	4.20	0.001

System Reliability	0.32	6.36	0.000
--------------------	------	------	-------

Model Summary

R	R ²	Adjusted R ²
0.85	0.72	0.70

Interpretation: The model explains 72% of the variance in Customer Trust, indicating strong explanatory power. AI-based fraud detection and Perceived Cyber Security emerged as the strongest predictors influencing Customer Trust in FinTech services.

Table 5: Structural Equation Modeling (SEM)

Fit Index	Value	Acceptable Range
CFI	0.95	> 0.90
TLI	0.94	> 0.90
RMSEA	0.04	< 0.08
χ^2/df	2.1	< 3

Interpretation: The Structural Equation Modeling results indicate satisfactory model fit, as all fit - indices fall within the recommended threshold values (CFI = 0.95, TLI = 0.94, RMSEA = 0.04, χ^2/df = 2.1). The results confirm that AI-based Security mechanisms significantly influence Customer Trust, which subsequently affects Continuance Intention.

The findings further reveal the mediating role of Customer Trust between AI-enabled Security mechanisms and Continuance Intention. This suggests that the effectiveness of AI-based fraud detection, biometric authentication, Perceived Cyber Security, privacy protection, and system reliability enhances customers' confidence in FinTech platforms, thereby encouraging continued Usage behavior.

Table 5A: Structural Equation Modeling (SEM) Path Coefficients

Path Relationship	Standardized β	p-value	Result
-------------------	----------------------	---------	--------

AI Fraud Detection → Customer Trust	0.38	0	Supported
Biometric Authentication → Customer Trust	0.29	0	Supported
Perceived Cyber Security → Customer Trust	0.35	0	Supported
Privacy Protection → Customer Trust	0.22	0.001	Supported
System Reliability → Customer Trust	0.32	0	Supported
Customer Trust → Continuance Intention	0.64	0	Supported

Interpretation

The SEM path coefficients indicate that all hypothesized relationships are positive and statistically significant. AI-Based Fraud Detection ($\beta = 0.38$) emerged as the strongest predictor of Customer Trust, followed by Perceived Cyber Security ($\beta = 0.35$) and System Reliability ($\beta = 0.32$). The path coefficient between Customer Trust and Continuance Intention ($\beta = 0.64$) demonstrates that Trust plays a substantial role in influencing customers' willingness to continue using FinTech. services. The results further support the mediating role of Customer Trust in strengthening the indirect relationship between AI-Based Security Mechanisms and Continuance Intention.

Mediation Effect Analysis

The SEM results indicate that Customer Trust acts as a significant mediating variable between AI-Based Security Mechanisms and Continuance Intention. The indirect effect suggests that AI-based fraud detection, biometric authentication, Perceived Cyber Security , privacy protection, and system reliability do not merely influence Continuance Intention directly; rather, they first enhance Customer Trust, which subsequently encourages continued usage of FinTech services. This finding highlights the importance of Trust as a psychological mechanism through which AI-enabled Security features translate into long-term customer engagement and sustained adoption of FinTech platforms.

The practical implications of this finding are significant for FinTech firms. The results suggest that investments in AI-enabled Security technologies alone may not guarantee continued customer usage unless such technologies effectively enhance Customer Trust. Therefore, FinTech companies should not only implement advanced fraud detection systems, biometric authentication, and Cyber Security safeguards but also communicate these Security measures transparently to users. Strengthening

Trust through visible Security assurance can improve customer retention, encourage continued platform usage, and contribute to long-term competitive advantage in the FinTech sector.

From a practical perspective, the mediating role of Customer Trust suggests that investments in AI-enabled Security technologies alone may not guarantee customer retention unless such technologies successfully enhance Trust perceptions. FinTech firms should therefore focus on communicating the effectiveness of fraud detection systems, biometric authentication mechanisms, and Cyber Security safeguards to Users. Transparent Security practices and proactive customer communication can strengthen Trust, which subsequently promotes Continuance Intention and long-term Customer Loyalty.

Table 6: Hypothesis Testing Summary

Hypothesis	Relationship	Result
H1	AI Fraud Detection → Customer Trust	Accepted
H2	Biometric Authentication → Customer Trust	Accepted
H3	Perceived Cyber Security → Customer Trust	Accepted
H4	Privacy Protection → Customer Trust	Accepted
H5	System Reliability → Customer Trust	Accepted
H6	Customer Trust → Continuance Intention	Accepted
H7	AI Security Mechanisms → Continuance Intention via Trust	Accepted

Interpretation: All hypotheses were accepted, indicating that AI-based Security mechanisms significantly influence Customer Trust and Continuance Intention in FinTech services.

Discussion of Findings

The findings reveal that AI-based fraud detection significantly influences Customer Trust in FinTech services. This result is consistent with the findings of Mehta et al. (2025), who reported that AI-enabled fraud monitoring systems enhance customer confidence by reducing Perceived financial risks and improving Transaction Security. The present study further confirms that advanced AI Security mechanisms contribute positively to Trust formation among FinTech users in Karnataka.

The findings indicate that Perceived Cyber Security significantly influences Customer Trust in FinTech services. This finding is consistent with Hasan et al. (2023), who reported that secure authentication systems and Cyber Security mechanisms positively affect customer confidence in Digital Payment platforms. The present study further confirms that strong Cyber Security measures reduce Perceived risk and encourage Trust among FinTech users in Karnataka.

The study confirms that Customer Trust plays a crucial role in the Adoption and Continued Usage of FinTech services. This result supports the findings of Gefen (2000), who emphasized that Trust serves as a critical determinant of user willingness to engage in online transactions. The findings suggest that Trust acts as a bridge between Security mechanisms and customer behavioral intentions, thereby encouraging customers to engage confidently with FinTech platforms.

The findings reveal that Customer Trust significantly influences Continuance Intention toward FinTech services. This result is in agreement with Oliveira et al. (2021), who found that Trust and satisfaction are key drivers of continued usage behavior in Digital payment systems. The present study demonstrates that customers are more likely to continue using FinTech platforms when they perceive them as secure, reliable, and Trustworthy. The results further indicate that Customer Trust mediates the relationship between AI-based Security mechanisms and continuance intention, highlighting the importance of Security assurance in sustaining long-term FinTech adoption.

The findings regarding system reliability and privacy protection are consistent with the studies of Kim et al. (2008) and Zhou (2011), which reported that secure and reliable digital systems significantly enhance Customer Trust and Technology acceptance. Similarly, the positive influence of biometric authentication supports the findings of Hasan et al. (2023), who observed that advanced authentication mechanisms improve Perceived transaction Security and strengthen customer confidence in Digital Financial services. These similarities indicate that Security-oriented technological features remain critical determinants of Trust formation across diverse FinTech environments.

The findings relating to biometric authentication, privacy protection, and system reliability are also consistent with previous research. Kim, Ferrin and Rao (2008) reported that privacy protection and secure transaction environments significantly enhance Customer Trust in digital platforms. Similarly, Zhou (2011) found that system quality and reliability positively influence Trust and

Continuance Behaviour in Technology-based financial services. The positive influence of biometric authentication observed in the present study further supports the findings of Hasan et al. (2023), who highlighted the role of advanced authentication mechanisms in improving transaction Security and customer confidence. These findings collectively indicate that secure and reliable technological infrastructures remain fundamental drivers of Trust in FinTech ecosystems.

Table 7: Suggestions for Strengthening AI-Based Security Mechanisms in FinTech Services

Area	Suggested Measure
Fraud Prevention	Strengthen AI-based fraud detection systems
Authentication	Implement advanced biometric and multi-factor authentication
Cyber Security	Improve real-time Cyber Security monitoring systems
Privacy Protection	Enhance transparency in data privacy policies
Customer Awareness	Conduct Cyber Security awareness programs for users
Regulatory Support	Establish stronger AI governance and Cyber Security regulations
Customer Support	Improve grievance redressal and transaction support systems

Interpretation: The suggestions focus on improving AI-enabled Security infrastructure, strengthening Customer Trust and enhancing long-term continuance intention toward FinTech services. Effective implementation of these measures can help FinTech firms create secure and reliable Digital Financial ecosystems.

Key Findings

1. **AI-Based Fraud Detection Systems:** AI-enabled fraud detection mechanisms significantly improve customer confidence by identifying suspicious transactions and reducing Cyber Fraud risks (mean ≈ 4.3).
2. **Strong Perception of Cyber Security:** Customers perceive FinTech platforms with advanced AI-driven Cyber Security systems as safer and more reliable for Digital Financial transactions (mean ≈ 4.2).
3. **Effectiveness of Biometric Authentication:** Biometric authentication methods such as fingerprint and facial recognition significantly enhance Transaction Security and User Trust (mean ≈ 4.1).

4. Improvement in Transaction Safety: AI-based monitoring and real-time alerts improve Users' perception regarding Transaction safety and Fraud prevention (mean ≈ 4.2).
5. Privacy Protection Enhances Confidence: Strong privacy protection mechanisms positively influence Customer confidence towards FinTech services (mean ≈ 4.0).
6. System Reliability Strengthens Trust: Reliable and uninterrupted FinTech platform performance significantly improves Customer Trust and satisfaction (mean ≈ 4.1).
7. Increase in Continuance Intention: Customers with positive Security perception show greater willingness to continue using FinTech services regularly (mean ≈ 4.3).
8. Reduction in Perceived Financial Risk: AI-enabled Security systems reduce fear of cybercrime, unauthorized access and financial loss among Users.
9. Positive Influence on Customer Trust: Regression analysis confirms that AI-based Security mechanisms have a significant positive effect on Customer Trust.
10. Strong Relationship with Continuance Intention: Customer Trust shows a strong positive relationship with Continuance Intention toward FinTech services.
11. Positive Correlation with Cyber Security Perception: A correlation value of $r = 0.83$ indicates a strong positive relationship between Perceived Cyber Security and Customer Trust.
12. Positive Correlation with System Reliability: A correlation value of $r = 0.81$ highlights the importance of reliable FinTech infrastructure in strengthening Trust.
13. Positive Correlation with Continuance Behaviour: A correlation value of $r = 0.87$ indicates a strong positive association between Customer Trust and Continuance Intention.
14. Significant Mediating Role of Customer Trust: Structural Equation Modeling results confirm that Customer Trust mediates the relationship between AI-based Security mechanisms and Continuance Intention.
15. Concerns Regarding Data Privacy and Cyber Threats: Around 65% of users expressed concern regarding data privacy, cyber fraud and misuse of personal financial information despite increased Trust in AI-enabled Security systems.

Recommendations

For FinTech Companies

1. Strengthen AI-based fraud detection and real-time transaction monitoring systems.
-

2. Implement advanced biometric and multi-factor authentication mechanisms for secure transactions.
3. Continuously upgrade Cyber Security infrastructure to prevent hacking and cyber fraud.
4. Ensure uninterrupted system reliability and faster transaction processing.
5. Maintain transparent privacy policies regarding customer data protection and AI usage.

For Customers / Users

1. Users should regularly update passwords and enable biometric authentication for secure access.
2. Customers should avoid sharing OTPs, PINs and confidential financial information.
3. Users should improve awareness regarding phishing attacks, cyber fraud and safe digital transaction practices.

For Regulatory Authorities / Government

1. Regulatory bodies should establish stronger Cyber Security regulations and AI governance frameworks for FinTech services.
2. Government agencies should conduct Digital Financial literacy and Cyber Security awareness programs to strengthen safe FinTech adoption.

Suggestions for Further Research

1. Similar studies may be conducted in other states of India.
2. Comparative studies between urban and rural FinTech users may be undertaken.
3. Future Research may include additional variables such as digital literacy and regulatory Trust.
4. Longitudinal studies may be conducted to examine changing perceptions over time.
5. Emerging Technologies such as Blockchain-integrated AI Security systems may be explored.

Conclusion

The study concludes that Artificial Intelligence-based Security mechanisms play a significant role in strengthening Customer Trust in FinTech services. AI-enabled fraud detection, biometric authentication, Perceived Cyber Security, privacy protection and system reliability positively influence Customer Confidence and Continuance Intention toward Digital Financial platforms. Among the variables, AI-based Fraud Detection and Perceived Cyber Security emerged as the strongest determinants of Customer Trust. The

findings further reveal that Customer Trust acts as a major mediating factor between AI-based Security mechanisms and Continuance Intention. Secure and reliable FinTech systems encourage long-term Usage behaviour and sustainable Digital Financial adoption. The study highlights that strong AI-driven Cyber Security infrastructure is essential for reducing Perceived risk, improving transaction safety and enhancing customer satisfaction. Overall, the research emphasizes the need for FinTech companies, customers and regulatory authorities to collaboratively strengthen AI-enabled Security systems and Cyber Security practices to ensure secure, reliable and sustainable growth of FinTech services in Karnataka.

References

- Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., & Williams, M. D. (2017). Examining factors influencing Jordanian customers' intentions and adoption of internet banking. *Journal of Retailing and Consumer Services*, 34, 154–166.
- Chuang, Y. F., Liu, C. C., & Kao, H. K. (2016). The adoption of fintech service: TAM perspective. *International Journal of Management and Administrative Sciences*, 3(7), 1–15.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.
- Gefen, D. (2000). E-commerce: The role of familiarity and trust. *Omega*, 28(6), 725–737.
- Goh, T., & Sun, Y. (2022). The influence of trust and perceived risk on fintech adoption. *Electronic Commerce Research*, 22(3), 589–610.
- Hasan, R., Pal, S., & Vanijja, V. (2023). Cyber Security perception and customer trust in UPI payment systems. *International Journal of Information Management Data Insights*, 3(1), 100145.
- Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce. *Decision Support Systems*, 44(2), 544–564.
- Li, X., Wang, Y., & Sun, L. (2022). Regulatory support and fintech adoption behaviour among consumers. *Journal of Financial Innovation*, 8(2), 44–58.
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734.
- Mehta, S., Rao, K., & Nair, V. (2025). Artificial intelligence-based fraud detection and customer trust in fintech services. *International Journal of FinTech Research*, 9(2), 88–104.
- Oliveira, T., Faria, M., Thomas, M. A., & Popovič, A. (2014). Extending the understanding of mobile banking adoption. *Computers in Human Behavior*, 34, 418–430.
- Oliveira, T., Thomas, M., & Espadanal, M. (2021). Assessing the determinants of continuance intention in mobile payment systems. *Journal of Business Research*, 122, 713–724.
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101–134.

- Sharma, P., & Kulkarni, A. (2025). Post-pandemic digital payment continuance behaviour in metropolitan India. *Journal of Digital Finance and Banking*, 12(1), 45–61.
- Singh, N., & Sinha, N. (2020). How perceived trust mediates merchant's intention to use a mobile wallet technology. *Journal of Retailing and Consumer Services*, 52, 101894.
- Slade, E., Williams, M., Dwivedi, Y. K., & Piercy, N. (2015). Exploring consumer adoption of proximity mobile payments. *Journal of Strategic Marketing*, 23(3), 209–223.
- Tamilmani, K., Rana, N. P., & Dwivedi, Y. K. (2021). Consumer behavior towards mobile payment technologies. *Information Systems Frontiers*, 23(1), 89–109.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478.
- Venkatesh, V., Thong, J. Y. L., & Xu, X. (2020). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36(1), 157–178.
- Zhou, T. (2011). Examining mobile banking user adoption from the perspectives of trust and flow experience. *Information Technology and Management*, 12(4), 335–345.