Eduvest – Journal of Universal Studies
Volume 5 Number 9, September, 2025
p- ISSN 2775-3735- e-ISSN 2775-3727

Facial Recognition Resistance in Banking: Analyzing Risk Through Technology Readiness, Regulation and Trust

Rika Ayu Haryanti, Dewi Hanggraeni
Universitas Indonesia, Indonesia
Email: haryanti.rikaayu@gmail.com, dewi_hanggraeni@yahoo.com

ABSTRACT

The rapid digitalization of Indonesia's banking sector has driven widespread adoption of biometric authentication, particularly facial recognition (FR) technology, to enhance security and user experience. However, user resistance remains a barrier, especially in light of concerns about privacy, regulatory trust, and technological readiness. This study investigates the influence of individual technology readiness, perceived risk, perceived trust, and regulation and compliance on resistance to FR technology in mobile banking. Using a quantitative survey method and Partial Least Squares Structural Equation Modeling (PLS-SEM), data were collected from 200 Indonesian mobile banking users familiar with FR technology. The findings reveal that digital literacy and personal innovativeness significantly enhance technology readiness, which, in turn, increases users' sensitivity to perceived risk. Perceived risk was found to be the strongest predictor of resistance, while trust reduced perceived risk but did not directly reduce resistance. Regulatory compliance directly enhanced trust and reduced resistance but did not moderate the influence of risk or trust. Mediation analysis showed that perceived risk fully mediates the relationship between technology readiness and resistance. These findings highlight the paradox that tech-ready users may still resist FR due to heightened awareness of data security concerns. The study suggests that reducing perceived risk and reinforcing data transparency through effective regulatory frameworks are critical to fostering public trust and adoption of FR technologies in digital banking.

KEYWORDS Facial recognition, perceived risk, biometric authentication, user resistance, technology readiness, data privacy

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International

INTRODUCTION

The Indonesian banking sector is undergoing a significant digital transformation to enhance service efficiency and accessibility (Sugihyanto & Arsjah, 2023). By the third quarter of 2024, digital banking transactions reached approximately 1.8 billion, driven by the increasing adoption of smartphones and continuous advancements in digital banking services (Bank Indonesia, 2024). However, this rapid digitalization has been accompanied by a notable increase in cyber fraud incidents, particularly involving social engineering techniques such as SIM swap fraud, which enables unauthorized access to customer accounts. The Ministry of Communication and Information Technology (*Kominfo*) has issued warnings regarding the rising threat of SIM swap fraud in Indonesia, emphasizing the need for heightened vigilance and improved cybersecurity measures.

In response to these security challenges, financial institutions are increasingly adopting *Facial Recognition* (FR) technology as a biometric authentication method. FR systems utilize artificial intelligence (AI) to analyze unique facial features, offering a more secure alternative to traditional authentication mechanisms such as Personal Identification Numbers (PINs) and One-Time Passwords (OTPs), while also enhancing user experience and operational efficiency (Zhang & Zhang, 2024; Lim et al., 2024).

The integration of FR technology within Indonesia's banking sector primarily occurs through two avenues: government-backed services facilitated by the Directorate General of Population and Civil Registration (*Dukcapil*), which authenticate biometric data against national databases, and commercial third-party providers offering electronic Know Your Customer (e-KYC) and transaction authentication solutions. However, the ransomware attack on Indonesia's Temporary National Data Center (*PDNS*) in June 2024 exposed significant cybersecurity vulnerabilities, disrupting over 200 government services and raising concerns about the potential misuse of biometric data, especially in light of advancing deepfake technologies. Deepfake technology, which employs AI to create highly realistic synthetic media, poses a growing threat to biometric authentication systems, as it can be used to spoof facial recognition mechanisms.

To address escalating concerns over data privacy and security, the Indonesian government enacted the *Personal Data Protection Law* (UU PDP) on October 17, 2022. Following a two-year transitional period, the law became fully enforceable on October 17, 2024, mandating all entities processing personal data to comply with its provisions. The UU PDP strictly governs the collection, processing, and storage of personal data, including biometric information, aligning Indonesia's data protection practices with international standards such as the European Union's General Data Protection Regulation (GDPR). Compliance with this regulation is mandatory for banks and public institutions, enhancing user trust and significantly reducing the potential for data breaches and privacy violations.

Globally, advanced economies such as China, Japan, the United States, and Singapore have widely adopted FR technology for public security, digital payments, and access control in public spaces. In the financial sector, major international banks have implemented FR to authenticate customers across digital platforms, modern ATMs, and virtual branches, aiming to enhance both security and user convenience (Deloitte, 2021). However, the deployment of FR technology has also sparked significant controversy. In the United States, concerns center around privacy violations and racial bias due to misidentification of minority groups (Hill, 2020; Conger et al., 2020). In China, its extensive use in state surveillance, particularly targeting ethnic minorities, has raised human rights concerns (Mozur, 2019). In Europe, strict data protection regulations under the GDPR continue to limit the use of FR in public spaces (Kantorkita, 2024). Meanwhile, in Asian countries, public concerns focus on the risks of biometric data breaches and potential misuse by third parties (Lim et al., 2024).

Despite the growing adoption of FR technology in Indonesian banking, comprehensive studies analyzing the impact of data privacy concerns, biometric information misuse, and data breaches on user resistance remain limited. This study aims to evaluate how these factors influence user resistance to FR technology, examine the role of trust in technology and service providers in alleviating concerns, and assess how technological readiness and regulatory frameworks affect user acceptance or rejection of

FR authentication in mobile banking. Technological readiness, encompassing digital literacy, personal innovativeness, and prior experience, plays a crucial role in shaping users' attitudes toward new technologies. Digital literacy refers to an individual's ability to understand and effectively use digital technologies, while personal innovativeness reflects an individual's openness to adopting new technologies. Prior experience with similar technologies can also influence the level of comfort and trust users have toward FR technology.

In this study, *Facial Recognition* (FR) refers broadly to biometric authentication methods utilizing facial recognition technology, including its specific application in payment authentication (*Face Recognition Payment*, FRP). Recent studies highlight the strong influence of perceived risks on user trust and adoption of FRP systems. Zhang and Zhang (2024) found that technology anxiety and security concerns heighten privacy fears, increasing resistance to FRP. Similarly, Lim et al. (2024) reported that privacy and financial risks deter adoption in Malaysia due to fears of biometric data misuse. Trust in service providers and personal innovativeness have been shown to reduce this resistance. Users who trust FRP providers and are open to new technologies are more likely to adopt FRP, even when aware of its risks (Lim et al., 2025; Zhang & Zhang, 2024). While FRP offers convenience, perceived benefits alone do not guarantee adoption. Factors such as information transparency and positive prior experiences are also crucial in lowering technology anxiety and building user trust (Lim et al., 2024).

In Indonesia, foundational challenges persist in the adoption of FR technology within the banking sector. Low levels of digital literacy and uneven digital infrastructure across regions contribute to heightened technology-related anxiety and a sense of information vulnerability among users. Although the *Personal Data Protection Law* (UU PDP) was enacted in 2022 and became fully enforceable in October 2024, its practical implementation is ongoing, with certain regulatory aspects still being developed. These factors collectively influence public trust and acceptance of FR technology in banking services. This study aims to analyze the impact of perceived risks, specifically concerning privacy, security, and financial aspects, on user resistance to FR technology. It examines how Individual Technology Readiness (ITR), encompassing digital literacy, personal innovativeness, and prior experience, along with Regulation & Compliance (RC), influence user acceptance of biometric authentication methods in Indonesian mobile banking. Furthermore, the study explores the moderating roles of ITR and RC on the relationship between perceived risks and user resistance, as well as the mediating roles of Perceived Risk (PR) and Perceived Trust (PT) in this context. Additionally, the potential of *Facial Recognition-based Payment* (FRP) systems in future financial transactions is considered. However, if user resistance remains high, the effectiveness of FR as a fraud mitigation tool may be significantly limited. By addressing these factors, the research seeks to provide insights that can inform strategies to enhance user trust and acceptance of FR technology in Indonesia's banking sector.

This study explores the factors influencing user resistance to *Facial Recognition* (FR) technology in Indonesia's banking sector, specifically within mobile banking. By analyzing factors like individual technology readiness (digital literacy, personal innovativeness, and prior experience) and the role of regulation and compliance, the study examines how these elements affect perceived risk, perceived trust, and resistance to FR adoption. Additionally, it investigates the mediating effects of perceived risk and trust, as well as the moderating roles of technology readiness and regulatory frameworks. Previous research has identified the importance of privacy concerns and security risks in user resistance to FR technology, with studies by Zhang & Zhang (2024) and Lim et al. (2024) highlighting the impact of these factors in Malaysia. However, these studies did not address how regulatory frameworks and technology readiness can mitigate resistance, particularly in Indonesia.

Therefore, this study aims to examine the key factors influencing user resistance to *facial recognition* (FR) technology in Indonesia's digital banking sector. Specifically, it investigates how individual technology readiness encompassing personal innovativeness, prior experience, and digital literacy—affects perceived risk, perceived trust, and resistance. It further evaluates the roles of regulation and compliance in shaping user trust and risk perceptions. Additionally, the study explores the mediating effects of perceived risk and trust, and the moderating roles of technology readiness and regulatory frameworks, in the relationship between perceived risk, trust, and user resistance. Through this framework, the research seeks to offer both theoretical insights and practical implications for enhancing secure, user-accepted biometric authentication in mobile banking.

RESEARCH METHOD

This study employed a quantitative survey approach and was analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). This method is well-suited for models involving latent variables, moderation effects, and non-normal data distributions, and has been widely applied in research on biometric technology adoption in payment systems (Lim et al., 2024; Hair et al., 2019).

The questionnaire included demographic questions, screening criteria, and items measuring study constructs. A total of 200 valid responses were collected from Indonesian participants through purposive sampling. The target population comprised Indonesian mobile banking users with experience or awareness of facial recognition technology. Convenience sampling was used due to ease of access and suitability for digital research, despite the potential for selection bias toward more digitally literate users (Etikan et al., 2016). As such, findings reflect the perceptions of exposed users rather than the broader population

Data were gathered through an online questionnaire distributed via messaging apps, digital communities, and banking networks to reach active mobile banking users. A pilot test with 30 participants was first carried out to ensure the reliability of the questionnaire. This was followed by a main online survey, distributed via WhatsApp to various community groups across Indonesia. Participation was voluntary, with no incentives provided.

Based on Table 1, the valid responses consisted of 52% of females and 48% of males. 49% of them were aged 30–39 years old. Most respondents, 66%, had a bachelor's degree. A total of 157 respondents reported frequent use of mobile banking, either daily or several times a week. For payment methods that respondents currently use, Bank Transfer have the highest frequency, with 185 respondents using this as their payment method currently.

Table 1. Demographic profile of respondents

Total Number of respondents (N=200)	Description	Frequency	Percentage (%)
Gender	Female	104	52%

Total Number of respondents (N=200)	**Description**	**Frequency**	**Percentage (%)**
	Male	96	48%
Age (Years)	<20	3	2%
	20-29	56	28%
	30-39	97	49%
	40-49	23	12%
	Above 50	21	11%
Education level	High School	23	12%
	Diploma	7	4%
	Bachelor's degree	132	66%
	Master's degree or above	38	19%
Mobile banking usage frequency	Everyday	78	39%
	Several times a week	79	40%
	Several times a month	23	12%
	Rarely	20	10%
Payment method you are using currently	Bank Transfer	185	93%
	QR Payment	175	88%
	Credit/Debit Cards	169	85%
	Digital e-wallets	160	80%
	Cash	157	79%

Source(s): Created by authors

This study is based on four previous studies, each highlighting key aspects of risk perception, trust, technology readiness, and regulatory compliance in the adoption of Facial Recognition Payment (FRP). Zhang & Zhang (2024) found that privacy concerns have a significant impact on user resistance, while Lim et al. (2024) emphasized that trust plays a more crucial role than perceived benefits in driving FRP adoption. Furthermore, Zarco et al. (2024) demonstrated that trust in technology and service providers is a primary determinant of adoption decisions, whereas Gao et al. (2023) highlighted that regulatory frameworks and transparency in data policies enhance trust and reduce user resistance.

This research framework (Figure 1) illustrates the factors influencing resistance to Face Recognition Technology (RFR), focusing on how users' perceptions of risk and trust shape their attitudes toward adoption.

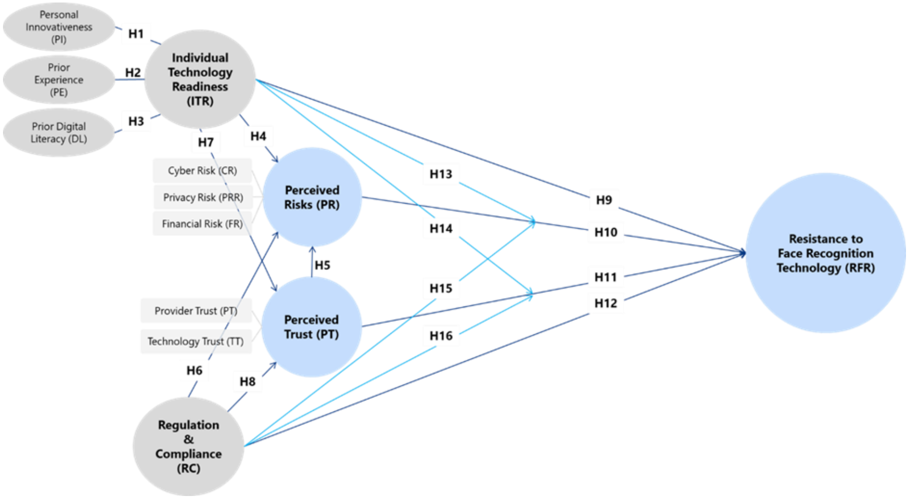

Figure 1. Research Framework

Role of Innovativeness, Experience, and Digital Literacy in Technology Readiness

Individual Technology Readiness (ITR) plays a critical role in shaping user acceptance of new technologies, such as facial recognition (FR) in digital banking. ITR is influenced by three key factors: Personal Innovativeness (PI) – the individual's tendency to try new technologies. Those with higher innovativeness are typically more open to adopting emerging technologies like FR, even when they are aware of potential risks (Lim et al., 2024). This openness drives early adoption and reduces resistance. Second, Prior Experience (PE) – users with greater exposure to digital technologies are generally more comfortable embracing FR, as past experience helps them better understand its benefits and functionality (Venkatesh et al., 2012). In contrast, limited experience often leads to anxiety and hesitancy. Third, Digital Literacy (DL) – the ability to effectively understand and use digital tools significantly affects readiness. Digitally literate users are more confident in assessing both the benefits and risks of FR and are thus more likely to adopt it (Featherman & Pavlou, 2003).

H1: Personal Innovativeness positively influences ITR.
H2: Prior Experience positively influences ITR.
H3: Digital Literacy positively influences ITR.

ITR on Risk Perception, Trust and User Resistance to FR

Individual Technology Readiness (ITR) plays a pivotal role in how users perceive and interact with emerging technologies, such as facial recognition (FR) in digital banking. Users with higher levels of technology readiness—marked by digital confidence, prior experience, and openness to innovation—are generally more comfortable exploring new systems. This readiness helps reduce feelings of uncertainty and concern, leading to a lower perception of risk (Lim et al., 2025; Zarco et al., 2024). At the same time, individuals with strong technology readiness tend to exhibit greater trust in technology. Familiarity with how digital systems function enhances users' confidence in both the performance and the security of technologies like FR, especially those involving sensitive biometric data (Zarco et al., 2024). Importantly, higher ITR is also linked to lower resistance to technology adoption. When users feel prepared and informed, they are more open to adopting new

innovations and less likely to reject or avoid them. In the case of FR, this means users with high ITR are more likely to accept the technology, recognizing its benefits and understanding how it works (Zarco et al., 2024).
H4: ITR negatively influences Perceived Risk (PR).
H7: ITR positively influences Perceived Trust (PT).
H9: ITR negatively influences Resistance to Facial Recognition (RFR).

Perceived Risk (PR) and User Resistance to FR

Perceived risk plays a critical role in shaping user resistance to facial recognition (FR) technology in digital banking. When users feel uncertain or vulnerable, whether due to fears of cyberattacks, data misuse, or financial fraud, they are more likely to reject the technology. Cyber risks, such as hacking or identity theft, raise concerns about the security of biometric data, which, unlike passwords, cannot be changed once exposed. Privacy risks emerge when users fear that their facial data might be collected or used without their clear consent, particularly in contexts where transparency is lacking. Financial risks involve potential losses from unauthorized access or fraud, especially with growing threats like deepfakes or spoofing attacks. These perceived threats amplified by past incidents and lack of safeguards, can lead to strong resistance, even when the technology promises convenience and enhanced security. Understanding and addressing these concerns is key to improving user acceptance.
H10: PR positively influences Resistance to Facial Recognition (RFR).

Perceived Trust (PT) on Resistance to FR

Perceived Trust (PT) refers to users' confidence in both the technology and the service providers behind facial recognition (FR) systems. This trust can be divided into two dimensions: Provider Trust and Technology Trust (Gefen et al., 2003). Provider Trust reflects the belief that banks or financial institutions will protect biometric data responsibly and in compliance with data protection regulations, such as Indonesia's PDP Law or the EU's GDPR. Transparency, strong data governance, and a solid reputation all contribute to this trust (Gao et al., 2023; Zhang & Zhang, 2024). When users trust the provider, they are more likely to feel safe and less resistant to adopting FR. Technology Trust refers to confidence in the reliability, accuracy, and security of the FR system itself. Features like anti-spoofing, liveness detection, and encrypted biometric storage increase this trust. When users believe the technology is robust against threats like deepfakes or spoofing, their resistance tends to decrease (McKnight et al., 2002; Zhang & Zhang, 2024).
H11: PT negatively influences Resistance to Facial Recognition (RFR)

Perceived Trust (PT) on Risk Perception

Trust plays a pivotal role in shaping how users assess the risks associated with adopting new technologies, particularly those involving sensitive data, such as biometric systems. When users have greater trust in the technology—believing it is secure, reliable, and well-regulated—they are more likely to feel less at risk. This trust acts as a psychological buffer, reducing uncertainty and concerns over privacy or misuse of personal data (Gao et al., 2023; Lim et al., 2025; Zarco et al., 2024; Zhang & Zhang, 2024). In the context of facial recognition, trust can significantly lower perceived barriers to adoption by making users feel more in control and secure.

H5: PT negatively influences Perceived Risk (PR).

Regulation and Compliance (RC) on PR, PT and User Resistance to FR

In digital banking, Regulation and Compliance (RC) are critical in influencing how users perceive and respond to technologies like facial recognition (FR). Strong, transparent regulations such as Indonesia's Personal Data Protection Law (UU PDP) or the EU's GDPR, provide legal assurance that biometric data is handled with care, privacy, and accountability. This sense of protection can significantly reduce perceived risk and enhance user trust (Lim et al., 2024; Porfírio et al., 2024). On the other hand, weak or unclear regulatory frameworks often trigger user anxiety around data misuse, surveillance, or unauthorized access, which in turn increases resistance to adoption (Porfírio et al., 2024; Gao et al., 2023). To mitigate these concerns, financial institutions must be transparent about how facial data is collected, stored, and used. Practices such as regular third-party security audits and clear data protection policies help build user confidence and trust (Featherman & Pavlou, 2003; Zhang & Zhang, 2024).

H6: RC negatively influences Perceived Risk (PR).

H8: RC positively influences Perceived Trust (PT).

H12: RC negatively influences Resistance to Facial Recognition (RFR).

The Moderating Role of Individual Technology Readiness (ITR)

Individual Technology Readiness (ITR) moderates the impact of both perceived risk and perceived trust on user resistance to facial recognition (FR). Users with high ITR—those who are digitally literate, experienced, and open to innovation—are better equipped to assess and manage risks. As a result, perceived risks have less influence on their resistance. Conversely, users with low ITR are more likely to overestimate threats and resist adoption (Lim et al., 2024). At the same time, high ITR amplifies the positive effect of trust. Digitally confident users are more likely to believe in the security and reliability of FR systems and their providers, reducing resistance (Zarco et al., 2024).

H13: ITR weakens the effect of PR on Resistance to Facial Recognition (RFR).

H14: ITR strengthens the effect of PT on Resistance to Facial Recognition (RFR).

The Moderating Role of Regulation and Compliance

Regulation and Compliance (RC) help reduce user resistance to facial recognition (FR) by moderating the effects of both Perceived Risk (PR) and Perceived Trust (PT). Strong data protection laws—such as the GDPR and Indonesia's PDP Law—reassure users that their biometric data is handled securely, reducing concerns over cyber threats, privacy breaches, and financial fraud (Lim et al., 2024; Porfírio et al., 2024). Clear consent rules, encryption, MFA, and AI-based fraud detection strengthen perceptions of safety (Zhang & Zhang, 2024). Likewise, RC enhances user trust by ensuring transparency, regular audits, and strict compliance, increasing confidence in both the provider and the technology (McKnight et al., 2002; Gao et al., 2023).

H15: RC moderates the relationship between PR and resistance to FR, weakening the effect of PR.

H16: RC moderates the relationship between PT and resistance to FR, strengthening the effect of PT.

RESULT AND DISCUSSION

This study was analyzed using the Partial Least Squares Structural Equation Modeling (PLS-SEM) approach, version 4.1.0.9. The analysis consisted of two primary stages: the evaluation of the Measurement Model (Outer Model) to assess the validity and reliability of each construct, and the Structural Model (Inner Model) to examine the strength of the relationships among latent variables and to evaluate the model's overall predictive capability regarding user behavior (Hair et al., 2022).

Measurement Model

The evaluation of the measurement model focused on three criteria: internal reliability, convergent validity, and discriminant validity, following guidelines from Hair et al. (2021). Internal reliability was assessed using Cronbach's Alpha and Composite Reliability (CR). As reported in Table 2, all constructs demonstrated CR values above 0.90 and Cronbach's Alpha values above 0.85, exceeding the minimum threshold of 0.70 (Nunnally and Bernstein, 1994; Hair et al., 2021). These results confirm that the constructs exhibit high internal consistency. Convergent validity was evaluated through indicator loadings and Average Variance Extracted (AVE). All item loadings exceeded 0.70 and AVE values ranged from 0.734 to 0.972, indicating that each construct captures more than 50% of the variance in its indicators (Fornell and Larcker, 1981). No items were removed during this process.

Table 2. Internal Reliability and Convergent Validity Results

Variables	Items	Loadings	Cronbach's alpha	CR	AVE
Personal Innovativeness (PI)	ITR1-PI	0.971	0.944	0.973	0.947
	ITR2-PI	0.975			
Prior Experience (PE)	ITR3-PE	0.953	0.891	0.948	0.901
	ITR4-PE	0.946			
Digital Literacy (DL)	ITR5-DL	0.985	0.971	0.986	0.972
	ITR6-DL	0.986			
Individual Technology Readiness (ITR)	ITR7	0.931	0.853	0.932	0.872
	ITR8	0.937			
Perceived Risk (PR)	PR1-CR	0.933	0.971	0.976	0.873
	PR2-CR	0.948			
	PR3-PRR	0.955			
	PR4-PRR	0.922			
	PR5-FR	0.949			
	PR6-FR	0.899			
Perceived Trust (PT)	PT1-PT	0.881	0.879	0.917	0.734
	PT2-PT	0.885			
	PT3-TT	0.793			
	PT4-TT	0.864			
Regulation & Compliance (RC)	RC1	0.846	0.901	0.931	0.771
	RC2	0.877			
	RC3	0.92			
	RC4	0.867			
Resistant to FR Technology (RFR)	RFR1	0.941	0.941	0.962	0.894
	RFR2	0.945			

Variables	Items	Loadings	Cronbach's alpha	CR	AVE
	RFR3	0.95			
Note(s): Composite Reliability (CR); Average Variance Extracted (AVE)					
Source(s): Created by authors					

Discriminant validity was verified using the Fornell–Larcker criterion. As shown in Table 3, the square root of each construct's AVE (diagonal values) is greater than its correlations with other constructs, indicating satisfactory discriminant validity and that all constructs are empirically distinct. These results confirm that the measurement model is both reliable and valid, thus appropriate for further structural model analysis.

Table 3. Discriminant Validity Results (Fornell-Larcker Criterion)

Variables	DL	ITR	PR	PT	PE	PI	RC	RFR
DL	0.986							
ITR	0.934	0.934						
PR	0.494	0.516	0.935					
PT	-0.198	-0.202	-0.509	0.857				
PE	0.497	0.558	0.170	0.079	0.949			
PI	0.676	0.834	0.365	-0.133	0.594	0.973		
RC	-0.144	-0.165	-0.412	0.757	0.030	-0.137	0.878	
RFR	0.397	0.413	0.639	-0.470	0.154	0.271	-0.481	0.946
Source(s): Created by authors								

Structural Model

The structural model was evaluated to test the hypothesized relationships and assess the model's predictive performance. Bootstrapping with 10,000 bias-corrected resamples was conducted using SmartPLS to obtain robust estimates of the path coefficients and significance levels (Hesterberg, 2015). Model strength was determined by examining the coefficient of determination (R^2) and predictive relevance (Q^2) as recommended by Hair et al. (2017).

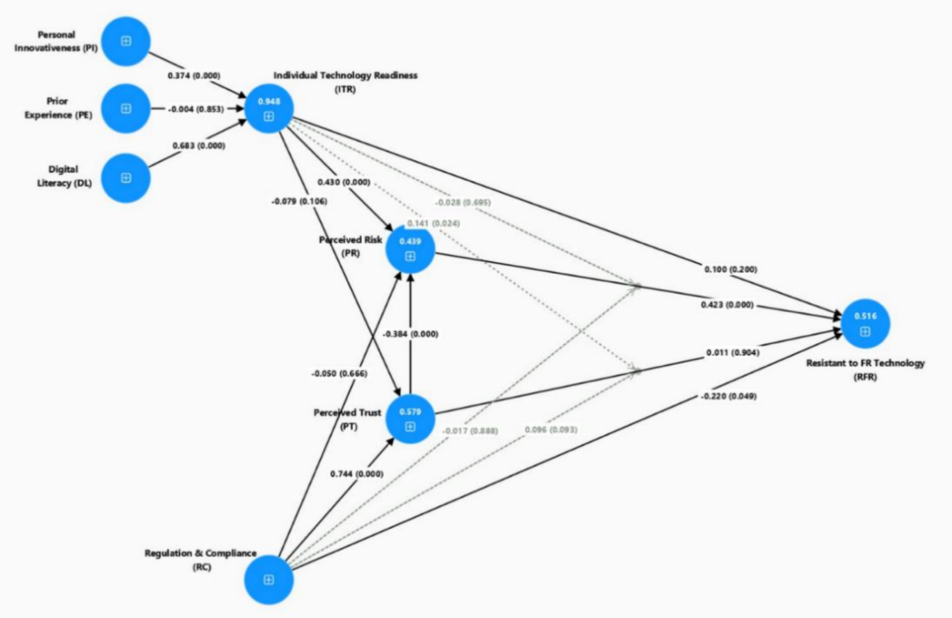

Figure 2. Results of the Conceptual Model (Path Coefficients and p-values)

As illustrated in Figure 2, the model shows strong explanatory power, with Individual Technology Readiness (ITR) achieving a high R² of 0.948, while Resistance to FR Technology (RFR) and Perceived Risk (PR) demonstrated moderate explanatory power, with R² values of 0.516 and 0.439, respectively. The Q² values, used to assess the model's predictive relevance via blindfolding, also indicated good predictive accuracy. ITR and Perceived Trust (PT) had high Q² values of 0.945 and 0.571, respectively, while other constructs remained within acceptable predictive relevance thresholds (Q² > 0).

To evaluate multicollinearity, the Variance Inflation Factor (VIF) was analyzed. All VIF values were below the conservative threshold of 5, suggesting that collinearity is not a concern in this model. The highest VIF value (2.758) was recorded for the path from ITR to RFR, which remains well within acceptable limits (Hair et al., 2017).

Further, PLS-Predict analysis was conducted to assess the model's out-of-sample predictive power. The Root Mean Square Error (RMSE) values for PLS-SEM were compared against linear model (LM) benchmarks. As reported in Table 4, most indicators showed PLS-SEM RMSE < LM RMSE, and all Q²_predict values were greater than 0, confirming moderate to high predictive validity at the indicator level (Shmueli et al., 2019).

Table 4. PLS Predict Results

Variables	Items	Q²predict	PLS-SEM RMSE	LM RMSE
Individual Technology Readiness	ITR7	0.761	0.554	0.421
	ITR8	0.883	0.413	0.157
Perceived Risk	PR1-CR	0.342	0.985	0.977
	PR2-CR	0.313	1,003	1,016
	PR3-PRR	0.303	1,019	1,010
	PR4-PRR	0.250	1,072	1,106
	PR5-FR	0.273	1,072	1,089
	PR6-FR	0.239	1,070	1,099

Variables	Items	Q^{2}predict	PLS-SEM RMSE	LM RMSE
Perceived Trust	PT1-PT	0.488	0.756	0.784
	PT2-PT	0.539	0.731	0.738
	PT3-TT	0.273	0.792	0.839
	PT4-TT	0.354	0.787	0.779
Resistant to FR Technology	RFR1	0.328	1,006	1,067
	RFR2	0.353	0.985	1,072
	RFR3	0.352	1,026	1,112

Source(s): Created by authors

Direct effects

As presented in Table 4, 7 of the 12 direct hypotheses were supported ($p < 0.05$), providing empirical insights into the determinants of user resistance to facial recognition (FR) technology in digital banking. Personal Innovativeness (PI) and Digital Literacy (DL) were found to significantly enhance Individual Technology Readiness (ITR), with DL exhibiting the strongest effect (H1: $\beta = 0.374$, $p < 0.001$; H3: $\beta = 0.683$, $p < 0.001$). These findings suggest that user readiness is driven more by digital capabilities than prior exposure. In contrast, Prior Experience (PE) had no significant influence on ITR (H2: $\beta = –0.004$, $p = 0.853$), indicating that familiarity alone does not ensure readiness unless it is accompanied by constructive digital engagement (Zarco et al., 2024; Lim et al., 2025).

Contrary to common assumptions, ITR demonstrated a positive association with Perceived Risk (PR) (H4: $\beta = 0.430$, $p < 0.001$), implying that higher technological competence may lead to increased risk sensitivity, perhaps due to greater awareness of biometric vulnerabilities (Gao et al., 2023). However, ITR did not significantly influence either Perceived Trust (PT) (H7: $\beta = –0.079$, $p = 0.106$) or Resistance to FR (RFR) (H9: $\beta = 0.100$, $p = 0.200$), suggesting a paradox wherein digitally literate users remain hesitant due to heightened privacy concerns.

Perceived Risk had a direct and significant effect on resistance (H10: $\beta = 0.423$, $p < 0.001$), confirming its role as a key barrier to adoption. While PT reduced risk perception (H5: $\beta = –0.384$, $p < 0.001$), it did not directly reduce user resistance (H11: $\beta = 0.011$, $p = 0.904$), supporting the notion that trust alone is insufficient when risk concerns are high (Zhang & Zhang, 2024; Featherman & Pavlou, 2003).

The role of Regulation & Compliance (RC) produced mixed results. Although RC had no significant effect on risk perception (H6: $\beta = –0.050$, $p = 0.666$), it positively affected trust (H8: $\beta = 0.744$, $p < 0.001$) and significantly reduced user resistance (H12: $\beta = –0.220$, $p = 0.049$). These findings underscore the importance of robust and transparent regulatory frameworks in promoting user acceptance (Porfírio et al., 2024).

In summary, the direct effects analysis highlights the centrality of Perceived Risk as a barrier and reinforces the role of Digital Literacy and Regulatory Confidence in shaping user responses to biometric technologies. However, it also reveals nuanced dynamics,particularly the awareness *risk paradox* suggesting that technologically prepared users may still resist adoption if risks are perceived to be unresolved.

Moderating effects

This study additionally explored the moderating roles of Individual Technology Readiness (ITR) and Regulation & Compliance (RC) on the relationships between

Perceived Risk (PR), Perceived Trust (PT), and user resistance to facial recognition (FR) technology.

The interaction between ITR and PR (H13) was not significant ($\beta = -0.028$, $p = 0.695$), indicating that even among tech-ready users, risk perception remains a dominant factor. Thus, readiness does not attenuate the influence of perceived risk (Lim et al., 2025; Zarco et al., 2024). Conversely, ITR significantly moderated the effect of PT on resistance (H14: $\beta = 0.141$, $p = 0.024$), suggesting that trust exerts a stronger influence in reducing resistance when users exhibit high technological readiness.

The moderating effects of RC on both PR (H15) and PT (H16) were not supported, with non-significant path coefficients and low effect sizes. While RC demonstrated direct effects on trust and resistance, it did not significantly alter the impact of either PR or PT on resistance.

Overall, the findings suggest that technological readiness amplifies the influence of trust, but not of perceived risk, on user resistance. Meanwhile, regulatory support, although beneficial in direct pathways, does not significantly moderate user responses to risk or trust.

Mediating effects

Mediation analysis revealed that Perceived Risk (PR) fully mediates the relationship between Individual Technology Readiness (ITR) and Resistance to FR Technology (RFR) ($\beta = 0.423$, $p < 0.05$). This finding suggests that while tech-ready users do not resist facial recognition directly, their heightened awareness may increase perceived risks, which subsequently drive resistance—challenging the conventional assumption that readiness reduces risk perception (Gao et al., 2023).

In contrast, PR did not mediate the effect of Regulation & Compliance (RC) on resistance, and Perceived Trust (PT) did not mediate the effects of either ITR or RC. These results imply that trust does not emerge automatically from technological readiness or regulatory presence, but is likely shaped by user experience, transparency, and confidence in data security (McKnight et al., 2002; Featherman & Pavlou, 2003; Zhang & Zhang, 2024). Overall, PR was the only significant mediator, emphasizing that mitigating perceived risk is critical in reducing user resistance. Readiness and regulation alone are insufficient without targeted efforts to address users' underlying concerns.

Table 5. Hypothesis Testing Results

Hypothesis relationship	Path coefficient (β)	Std.dev (σ)	t-value	p-value	95% Confidence interval		Q^2	R^2	f^2	Effectsize	VIF	Supported
					LL	UL						
H1 PI → ITR	0.374	0.037	10,000	0.000	0.301	0.45	0.945	0.948	1,222	Large	2,200	Yes
H2 PE → ITR	-0.004	0.023	0.185	0.853	-0.051	0.041			0.000	No Effect	1,586	No
H3 DL → ITR	0.683	0.036	19,103	0.000	0.609	0.751			4,732	Large	1,893	Yes
H4 ITR → PR	0.430	0.065	6,666	0.000	0.302	0.553	0.331	0.439	0.317	Moderate	1,043	Yes
H5 PT → PR	-0.384	0.101	3,807	0.000	-0.576	-0.182			0.110	Small	2,378	Yes
H6 RC → PR	-0.050	0.117	0.431	0.666	-0.279	0.182			0.002	No Effect	2,345	No
H7 ITR → PT	-0.079	0.049	1,618	0.106	-0.177	0.014	0.571	0.579	0.014	No Effect	1,028	No
H8 RC → PT	0.744	0.042	17,665	0.000	0.655	0.819			1,281	Large	1,028	Yes
H9 ITR → RFR	0.100	0.078	1,283	0.200	-0.053	0.253	0.387	0.516	0.012	No Effect	1,699	No
H10 PR → RFR	0.423	0.106	3,999	0.000	0.175	0.585			0.193	Moderate	1,915	Yes
H11 PT → RFR	0.011	0.095	0.12	0.904	-0.183	0.183			0.000	No Effect	2,758	No
H12 RC → RFR	-0.220	0.112	1,965	0.049	-0.446	-0.009			0.037	Small	2,702	Yes
H13 ITR X PR → RFR	-0.028	0.071	0.392	0.695	-0.181	0.098			0.001	No Effect	2,253	No
H14 ITR X PT → RFR	0.141	0.063	2,254	0.024	0.01	0.258			0.031	Small	1,566	Yes
H15 RC X PR → RFR	-0.017	0.119	0.141	0.888	-0.187	0.265			0.000	No Effect	1,726	No
H16 RC X PT → RFR	0.096	0.057	1,682	0.093	-0.007	0.214			0.020	No Effect	1,579	No

Source(s): Created by authors

CONCLUSION

The findings reveal that PR is the most influential driver of resistance, fully mediating the relationship between ITR and user resistance. Surprisingly, greater technological readiness was associated with increased risk perception, suggesting that digitally literate users may be more aware of potential vulnerabilities in biometric systems. While ITR did not directly reduce resistance or enhance trust, it strengthened the effect of trust in reducing resistance, indicating an interaction between digital confidence and trust effectiveness. Conversely, RC had no moderating effect but exerted direct influence by increasing trust and decreasing resistance. These results highlight the need to address users' psychological concerns and risk perceptions directly, moving beyond technical readiness and regulatory presence. For banks and fintech providers, it's essential to invest in trust-building strategies, such as transparent data governance, user education, and visible security measures, while also enhancing digital onboarding and communication about biometric system safeguards. Policymakers must ensure effective implementation of the Personal Data Protection Law (UU PDP) alongside clear biometric governance, standardized audit protocols, and user-centric data protection practices. Future research should incorporate longitudinal or experimental designs, cross-country comparisons, and mixed-method approaches to better capture the dynamics influencing biometric technology adoption. In sum, the adoption of FR in digital banking depends not only on technical or regulatory readiness, but critically on efforts to reduce perceived risks and build trust in the technology and its custodians.

REFERENCES

Conger, K., Fausset, R., & Kovaleski, S. (2020, January 12). Facial recognition technology in policing: Dangerous and biased. The New York Times.

Deloitte. (2021). Biometric authentication: Enhancing digital identity in banking.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. American Journal of Theoretical and Applied Statistics, 5(1),1-4.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. International Journal of Human-Computer Studies, 59(4), 451–474.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1),39–50.

Gao, L., Waechter, K. A., & Bai, X. (2023). Understanding consumers' acceptance of facial recognition payment: The role of perceived risk and trust. Journal of Retailing and Consumer Services, 70, 103125.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2019). A primer on partial least squares structural equation modeling (PLS-SEM) (2nd ed.). SAGE Publications.

Hair, J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2022). PLS-SEM or CB-SEM: Updated guidelines on which method to use. International Journal of Multivariate Data Analysis, 1(1), 107–123.

Hesterberg, T. C. (2015). What teachers should know about the bootstrap: Resampling in the undergraduate statistics curriculum. The American Statistician, 69(4), 371–386.

Hill, K. (2020). Wrongfully accused by an algorithm. The New York Times.

Kantorkita. (2024). Kontroversi penggunaan teknologi pengenalan wajah di Eropa. KantorKita.id.

Lim, W. M., Lee, S. Y., & Hew, T. S. (2024). Trust or convenience? Investigating determinants of user resistance to facial recognition payments. Journal of Business Research, 168, 114045.

Lim, W. M., Hew, T. S., & Wong, L. W. (2025). Privacy and innovation concerns in biometric systems: The role of personal innovativeness. Information Technology & People, 38(1), 199–215.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3), 334–359.

Mozur, P. (2019). One month, 500,000 face scans: How China is using AI to profile a minority. The New York Times.

Porfírio, J. A., Carrilho, T., & Felício, J. A. (2024). The impact of data protection laws on trust in digital platforms. Government Information Quarterly, 41(1), 101810.

Ringle, C. M., Sarstedt, M., Mitchell, R., & Gudergan, S. (2022). Partial least squares structural equation modeling in HRM research. The International Journal of Human Resource Management, 33(1), 23–42.

Shmueli, G., Ray, S., Velasquez Estrada, J. M., & Chatla, S. B. (2019). The elephant in the room: Evaluating the predictive performance of PLS models. Journal of Business Research, 104, 632–643.

Sugihyanto, T., & Arsjah, R. J. (2023). The effect of digital banking, digital transformation on the efficiency of commercial banks in Indonesia. *International Journal of Islamic Education, Research and Multiculturalism (IJIERM)*, *5*(2), 387–408.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. MIS Quarterly, 36(1), 157–178.

Zarco, F., Fernández, J., & Herrero, A. (2024). User readiness and resistance to biometric systems: An empirical investigation. Technological Forecasting and Social Change, 198, 122912.

Zhang, Y., & Zhang, J. (2024). Facial recognition payments and user adoption: A risk-trust perspective. Information & Management, 61(1), 103741.