

NEXT-GENERATION AI-ENABLED BIOMETRICS FOR FRAUD PREVENTION, DIGITAL BANKING, AND FINANCIAL SECURITY USING IRIS RECOGNITION

Nur Nahar Rimi¹, Atika Dola², Kazi Siam Al Mobin³, Kaniz Fatema⁴, Md Forhad Hossain⁵, Md Luman Jamali⁶, FNU Nurujjaman⁷, Tamanna Alam⁸

¹College of Technology & Engineering, Westcliff University, Irvine, California, USA. Email: N.rimi.253@westcliff.edu

²Master's in Business Analytics, University of the Cumberland, Kentucky, USA. Email: atikadola25@gmail.com

³Master of Science in Information Technology, Washington University of Science and Technology, Virginia, USA.

Email: kazi.almobin@gmail.com

⁴Doctor of Business Administration, Specialization in Applied Artificial Intelligence, Belhaven University, Mississippi, USA,

Email: nishikanijl@gmail.com

⁵Department of Information Technology, St. Francis College, New York, USA. Email: forhad6951@gmail.com

⁶College of Graduate and Professional Studies, Trine University, Arizona, USA. Email: mjamali25@my.trine.edu

⁷College of Graduate and Professional Studies, Trine University, Indiana, USA. Email: nadim142@gmail.com

⁸Faculty Of Arts And Social Science, Government Titumir College, Dhaka, Bangladesh. Email: tamanna.alam1986@gmail.com

Corresponding Author: FNU Nurujjaman, Email: nadim142@gmail.com

Abstract: Background: The high growth in digital banking has led to more demand in the use of enhanced, secure, and user-friendly authentication. Iris recognition is a next-generation biometric technology that is highly accurate, does not spoof, and is more convenient to use. AI-enabled iris recognition can enhance biometric authentication by applying intelligent pattern recognition to iris features, supporting more accurate identity verification and stronger protection against fraudulent access in digital banking environments. Nonetheless, there is little empirical evidence regarding its acceptance and perceived security and influence on digital banking security. These AI-enabled biometric capabilities are particularly relevant to fraud prevention and financial security because they can strengthen identity verification and reduce opportunities for unauthorized access to digital banking services.

Objectives: This paper explores the effectiveness of technological features of iris recognition in digital banking, such as accuracy, anti-spoofing, system response time, and user interface experience in influencing the security of digital banking as well as user adoption. It also looks into the mediating role of the perceived security as well as the moderating role of trust in biometric technologies. The study also considers the relevance of AI-enabled iris recognition to fraud prevention and financial security by examining whether enhanced biometric authentication can strengthen digital banking security and reduce the risk of unauthorized access.

Methods: The quantitative research design was used, and the data were gathered using 233 respondents (digital banking users) through a structured Likert-scale questionnaire. The Shapiro-Wilk, Cronbach's Alpha, KMO, and Bartlett tests were used to confirm normality, reliability, as well as validity. Independent samples t-test, One-way ANOVA, Chi-square, and Kruskal-Wallis tests were used to analyze group differences. Pearson correlation and multiple regression were the two methods employed to test the relationship between variables. The questionnaire therefore assessed the perceived effectiveness of AI-enabled iris recognition, including biometric accuracy, anti-spoofing capability, security, and authentication performance in relation to fraud prevention and financial security.

Results: The reliability of all the instruments was excellent ($\alpha \geq 0.70$), and the validity (KMO = 0.842). Results showed there were strong and positive relationships between all variables. Findings of the regression tests proved the existence of a significant correlation between accuracy, anti-spoofing technology, system response time, user experience, perceived



security, and trust in increasing user adoption of the iris recognition. The strongest predictor was perceived security. The difference tests of the group presented the results that gender, age, education level, and biometric experience had a significant effect on security perceptions and adoption intentions. The findings further indicate that AI-enabled iris recognition capabilities, particularly accuracy, anti-spoofing performance, and perceived security, are positively associated with stronger digital banking protection and fraud-prevention potential.

Conclusion: The paper has come to the conclusion that iris recognition is a highly potent and efficient biometric remedy to improving the security of digital banking. High perceived security and trust in conjunction with technological performance create a great user adoption. With the application of awareness and trust-building techniques and user-centric design, iris recognition has high potential of becoming a mainstream authentication in financial services. The findings further support the potential of AI-enabled iris recognition as an intelligent biometric security mechanism for fraud prevention and strengthening financial security in digital banking.

Keywords: Iris Recognition, Artificial Intelligence (AI), AI-Enabled Biometrics, Fraud Prevention, Digital Banking Security, Biometric Authentication, User Adoption, Perceived Security, Trust in Biometrics, Anti-Spoofing Technology, Financial Security

1. Introduction

The high pace of the electronic transformation of financial services has radically changed the level of interaction between consumers and the systems of banking systems. With the advent of digital banking as the new form of financial transactions, the security of user identity and confidential financial data has gained top position in priority. Conventional security techniques like passwords, PINs, and one-time verification codes are now being considered as being of inadequate security because they are prone to hacking, phishing, and social engineering attacks. Therefore, banking is transforming into more advanced, secure, and user-oriented authentication systems. Biometrics is one of such technologies, and it has become one of the promising answers as it provides the combination of convenience, accuracy, and increased security. Although some of the biometric technologies are already used, like fingerprint, facial recognition, and voice recognition, iris recognition is a biometric innovation that can be used as the next generation and overcome many of the limitations of the traditional ones (Shivarudraiah, 2025). The integration of artificial intelligence (AI) with biometric technologies enables intelligent analysis of distinctive biometric patterns and can strengthen authentication accuracy, security, and fraud prevention in digital banking. AI-enabled iris recognition can therefore provide an advanced approach to verifying customer identity while supporting stronger financial security against unauthorized access and identity-related fraud.

The human iris is unique and stable in its structure, and thus, iris recognition, which entails the process of capture and analysis of the distinct patterns of the human iris, has a very high accuracy rate. The iris is extremely stable through the life of a person unlike the fingerprints that might wear off over time, or the facial recognition system that might not be able to operate in areas of light or partial occurrences, and the eye is also used to protect the iris. Also, iris recognition systems have proven to be the most resistant to spoofing and identity fraud in comparison to other modalities. Iris biometrics is an attractive option to financial institutions that are attempting to implement an effective authentication system that is resistant to escalating cyber threats because of these strengths. Iris recognition could potentially decrease the rate of fraud, unauthorized access, as well as false acceptance by a large margin in the field of digital banking, where user identity is a core component of any secure and robust transactions (Sadhu et al., 2025). The application of AI to iris recognition can further enhance these capabilities by enabling intelligent biometric pattern analysis and supporting the detection of potentially fraudulent or unauthorized authentication attempts. This makes AI-enabled iris biometrics particularly relevant to fraud prevention and financial security in increasingly digital banking environments.

Although iris recognition in digital banking has its technological benefits, it is not only performance metrics that are relied on to implement this innovation. The trust, perceived security, ease of use, and confidence in the privacy of data are some of the user perceptions that are instrumental in defining whether the customers will accept and adopt this new technology. Moreover, the ability to process fast, user interface design, and anti-spoofing elements are system characteristics that determine the user experience and adoption. The introduction of iris recognition into digital

banking systems cannot be successfully implemented by a unitary grasp of how technology works and how users will receive it, so that the technology must be not only safe but also convenient, reliable, and trustworthy in the eyes of the users (Salami et al., 2025).

With the shift of the banking institutions to next-generation authentication procedures, the need to assess the impact of combined technological elements and user attitudes on the effectiveness and acceptance of the iris recognition is gaining momentum. Although the literature recognizes the possibilities provided by biometric authentication, there is a lack of empirical research specifically in the field of iris recognition in digital banking. The majority of the literature reviewed has been on general biometric adoption or has discussed other modalities like fingerprints and facial recognition. Thus, there exists a high demand for the specific research that will explore how the peculiarities of iris recognition can be used to enhance the security of digital banking and predefine user adoption (Kumar & Abbas, 2025). However, limited empirical attention has been given to the combined role of AI-enabled iris recognition, anti-spoofing capability, and biometric security in supporting fraud prevention and broader financial security within digital banking.

This paper aims to address this gap because it examines how the iris recognition accuracy, anti-spoofing technology, processing speed, and user experience affect the security of digital banking as well as its acceptance by the users. It also examines the mediating effect of perceived security and the moderating effect of trust in biometric technologies. This study has provided pertinent information to financial institutions, policymakers, and technology developers, such that in their quest to roll out safe, efficient, and user-friendly next-generation biometric systems in digital banking systems, they can utilize the cumulative effects of technological performance and user perception (Javid & Kollwitz, 2025). More specifically, the study evaluates the potential of AI-enabled iris recognition as a next-generation biometric approach for strengthening authentication, preventing fraudulent access, and improving financial security in digital banking.

2. Literature Review

2.1 Iris Recognition Accuracy (IV1)

Iris recognition accuracy is the capacity of the system to recognize or confirm the user by analyzing the unique iris pattern of the user. It has always been found that iris recognition is one of the most precise biometric modalities because the iris texture is stable and complicated. Daugman emphasizes that iris recognition is capable of a lower false acceptance and false rejection rate than fingerprint and facial recognition. The current research on digital banking settings suggests that accuracy is directly related to trust and the desire of users to use biometric systems. A high accuracy means fewer authentication failures, more user satisfaction, and more trust in digital banking platforms (Kerai & Vidani, 2025). In AI-enabled biometric systems, high iris-recognition accuracy is particularly important because reliable identification can strengthen authentication and reduce the likelihood of fraudulent access. Thus, accurate AI-assisted iris analysis can contribute to both digital banking security and financial fraud prevention.

2.2 Anti-Spoofing Technology (IV2)

Anti-spoofing technology can be defined as the capability of the biometric system to identify fraud in attempts to use artificial or replicated iris images. Biometric systems have threats of spoofing attacks like printed irises, high-resolution contact lenses, or digital overlays. Research by Yadav et al. indicates that high-end liveness detection and deep-learning spoof detection enhance security on biometrics to a considerable extent. Regarding the problem of digital banking, Oloyede and Hancke note that anti-spoofing functions directly help in reducing financial fraud and identity theft. User trust and adoption intentions are generated by high-performance spoof detection (Singh & Paintal, 2025). For AI-enabled iris recognition, anti-spoofing capability is essential for fraud prevention because intelligent biometric systems must distinguish genuine iris presentations from manipulated, replicated, or artificially presented biometric inputs. Strong anti-spoofing protection therefore provides an additional layer of cybersecurity and financial security for digital banking authentication.

2.3 System Response Time (IV3)

System response time is the speed with which the iris image is processed in the system, and the user is authenticated. According to the performance research, system performance has a significant impact on user experience and perceived convenience. Biometric systems are also viable in cases where the user wants quick access, since the system will have a fast response time. Technological adoption research indicates that decreasing wait time increases ease of use and usefulness perception, which has a positive impact on the adoption behavior of the user (Ganmati et al., 2025). For AI-enabled iris recognition, efficient processing is important because rapid biometric analysis can support real-time authentication and timely identification of potentially unauthorized access in digital banking environments.

2.4 User Interface & User Experience (IV4)

User Experience (UX) and User Interface (UI) are concerned with the ease, ease of use, and comfort with which users go through the process of authentication. Norman says that a user-focused interface makes cognitive load less and more satisfying. Alsaadi is keen to point out that smooth UI design facilitates acceptance by reducing the operational complexity in the field of biometrics research. Digital banking is a field where UX is directly proportional to how they perceive the quality of the system and the overall trust, which affects the behavioral intention (Prakasha & Sumalatha, 2025). In next-generation AI-enabled biometric banking systems, an intuitive user interface can facilitate the secure use of iris recognition while reducing user errors that may compromise authentication and increase exposure to fraudulent access.

2.5 Perceived Security Assurance (Mediator)

Perceived security assurance refers to the level at which users embark on the idea that a biometric system secures their financial information and prevents unauthorized access. A study conducted by Johnston and Warkentin reveals that perceived security is a mediating factor between the characteristics of the system and its adoption by users. Users will be more willing to use the technology when they are certain that they are safe. The research on digital banking also proves that perceived security plays a vital role in the utilization of improved authentication systems (Akte, 2025). In the context of AI-enabled iris recognition, perceived security assurance can therefore connect the technological capabilities of biometric authentication with users' confidence in its ability to protect financial information and prevent unauthorized or fraudulent access.

2.6 User Trust in Biometrics (Moderator)

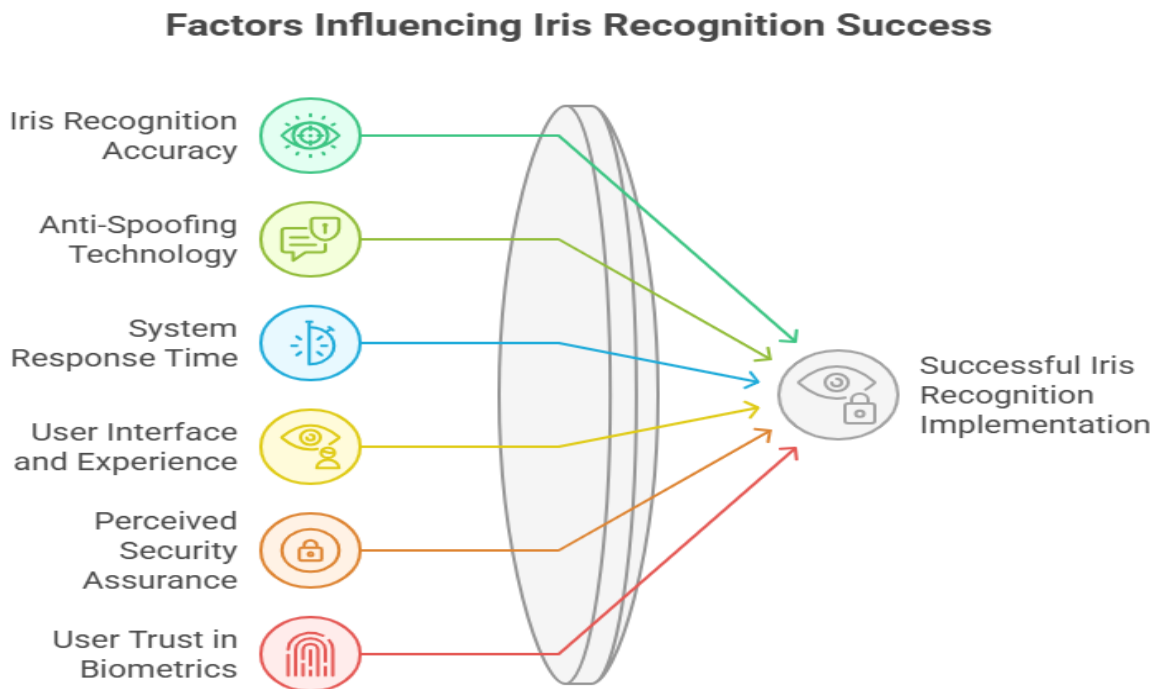
Trust in biometrics refers to the belief of the user in the fact that biometric technologies are secure, non-invasive, and dependable. According to McKnight et al., the relationship between the features of technology and user acceptance is moderated by trust. The trust is greater in the biometrics research, where perceived risks are less and adoption is high. The users who have confidence in the institution and its data protection procedures are more willing to use sensitive biometric modalities such as iris recognition (Fiore et al., 2025). For AI-enabled iris recognition, user trust may further strengthen the relationship between biometric technology and secure digital banking adoption, particularly when users believe that their biometric information is adequately protected from misuse and fraudulent access.

2.7 Digital Banking Security Effectiveness (DVI)

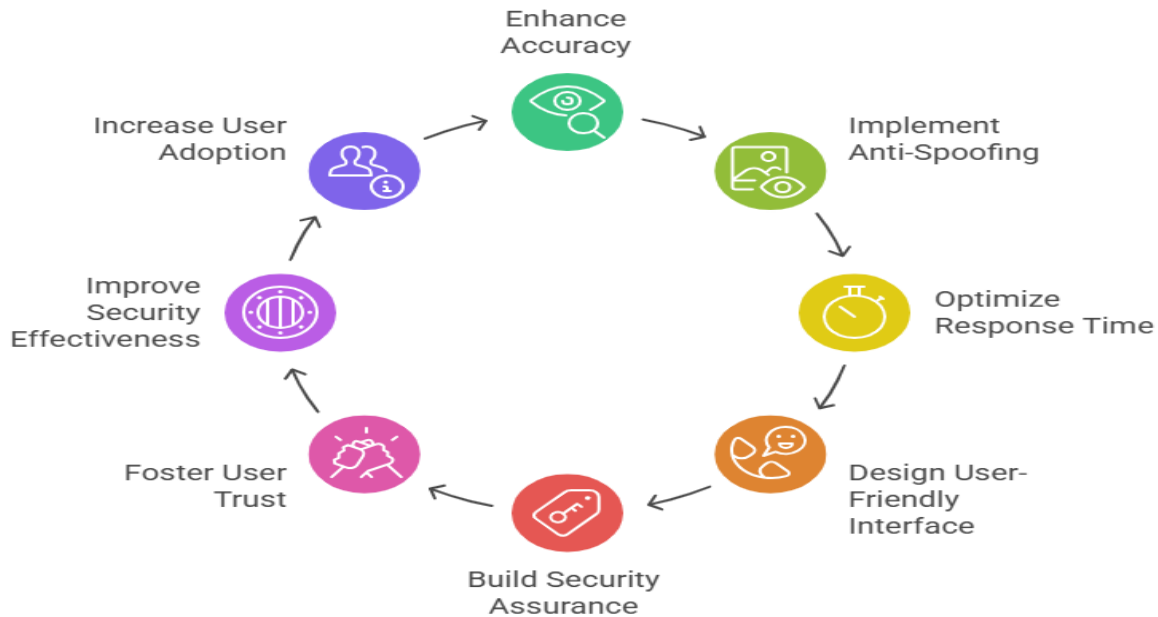
The digital banking security effectiveness is the level of the biometric authentication system to minimize threats, account protection, and improve the security of transactions. Studies reveal that biometric authentication is an effective measure in increasing the level of system security via identity verification and countering cyber-attacks. Research on financial technology has found that efficiency in asset protection leads to increased customer satisfaction and confidence (Prerna et al., 2025). The integration of AI-enabled iris recognition can further contribute to digital banking security by supporting intelligent identity verification, strengthening authentication, and reducing opportunities for identity-related fraud and unauthorized financial access.

2.8 User Adoption of Iris-Based Authentication (DV2)

The intention and willingness of individuals to use iris recognition to authenticate digital banking is the user adoption. Technology acceptance models (TAM, UTAUT) indicate that the factors that affect adoption include perceived usefulness, ease of use, trust, and perceived security. Research by Bhattacharya reveals that users use biometric technologies when they believe that they are safe, fast, and reliable. The user adoption is boosted by positive past experiences, system performance, and trust (Kandpal et al., 2025). Greater user adoption of AI-enabled iris authentication may therefore contribute to broader financial security when customers perceive the technology as accurate, trustworthy, resistant to spoofing, and capable of preventing fraudulent access to digital banking services.



Iris Recognition Implementation Cycle



High-level hypotheses

Independent Variables → Digital Banking Security Effectiveness (DV1)

H1: The effect of Iris Recognition Accuracy on the Digital Banking Security Effectiveness is significantly positive (Alpar, 2021).

H2: The impact of Anti-Spoofing Technology on Digital Banking Security Effectiveness is positive (Nguyen et al., 2024).

H3: There is a significant positive influence of System Response Time on the Digital Banking Security Effectiveness (Dommari & Mishra, 2024).

H4: The User Interface and User Experience positively affect Digital Banking Security Effectiveness significantly (Mohammed & Ahmed, 2022).

Independent Variables → User Adoption (DV2)

H5: The Iris Recognition Accuracy positively impacts greatly on User Adoption of iris-based authentication (Khade et al., 2021).

H6: There is a positive, substantial impact of Anti-Spoofing Technology on User Adoption.

H7: User Adoption performance is strongly positively related to System Response Time.

H8: User Interface and User Experience are a significant positive influence on User Adoption. Mediator (Perceived Security Assurance) (Malik, 2024).

IVs → Mediator → DV1 & DV2

H9: The user adoption of Iris Recognition is mediated by Perceived Security Assurance and the relationship between Iris Recognition Accuracy and Perceived Security Assurance (Singh et al., 2024).

H10: Perceived Security Assurance is the mediator between Anti-Spoofing Technology and User Adoption (Tiwari & Mishra, 2023).

H11: System Response Time and User Adoption have a mediating relationship through Perceived Security Assurance (Srivastav et al., 2024).

H12: Perceived Security Assurance is an intermediary between User Interface Experience and User Adoption (Sun et al., 2021).

H13: The relationship between the Iris Recognition Accuracy and Digital Banking Security Effectiveness is mediated by Perceived Security Assurance (Giribalan & Arunkumar, 2023).

H14: Perceived Security Assurance is the mediating factor between Anti-Spoofing Technology and Digital Banking Security Effectiveness (Hamidi, 2019).

H15: System Response Time has a mediated relationship with Digital Banking Security Effectiveness through Perceived Security Assurance (Mukkamala et al., 2024).

H16: There is a mediating relationship between User Interface Experience and Digital Banking Security Effectiveness through Perceived Security Assurance (Abdul-Al et al., 2024).

Moderator (User Trust in Biometrics)

Moderator on IV → DV Relationships

H17: User Trust has a positive moderating effect on the relationship between Iris Recognition Accuracy and User Adoption, whereby the relationship is stronger between users who have a high trust level and high-level users (Bastos et al., 2024).

H18: User Trust will be a positive moderator in the Anti-Spoofing Technology to User Adoption (Gupta, 2020).

H19: User Trust has a positive moderating effect between System Response Time and User Adoption (Kolluri et al., 2024).

H20: There is a positive moderate effect of User Trust between User Interface Experience and User Adoption (Basaligheh & Kothawade, 2024).

Direct Effect of Mediator & Moderator on Outcomes

H21: There is a strong positive impact of User Adoption on Perceived Security Assurance.

H22: Perceived Security Assurance exerts a big positive influence on Digital Banking Security Effectiveness (Aparna et al., 2024).

H23: User Trust influences User Adoption of iris-based authentication positively and significantly (Morake et al., 2021).

Optional Additional (If Needed for SEM)

H24: The Effectiveness of the Digital Banking Security has a positive impact on User Adoption.

3. Research Methodology

3.1 Research Design

The given research design is quantitative and cross-sectional in nature by trying to explore the impact of next-generation iris recognition technologies on the security of digital banking and the adoption rate of digital banking by users. Quantitative approach will be used since the study will be focused on measuring the relationships between variables, i.e., iris recognition accuracy, anti-spoofing technology, the response time of the system, user experience, perceived security, user trust, and the two most important outcomes: the effectiveness of digital banking security and the adoption of the system by the user. The structure facilitates specific statistical testing using questionnaires, which can be used to make generalized conclusions among digital banking users (Burkul & Patil, 2024). The study also evaluates the relevance of AI-enabled iris recognition to fraud prevention and financial security by examining how

intelligent biometric authentication can strengthen identity verification and reduce the potential for unauthorized access in digital banking.

3.2 Population and Sampling

The target group is the group of active users of digital banking who have exposure to biometric and digital authentication systems. The non-probability purposive sampling approach is applied because the respondents have to meet certain requirements: (1) frequent use of digital banking applications and (2) be aware of biometric authentication. The sample size is selected on the basis of a minimum required sample that is used to conduct Structural Equation Modeling (SEM). This figure provides the strength of factor analysis, reliability testing, regression modelling, and hypothesis validation (Patra et al., 2022). The selected respondents are also relevant to evaluating the acceptance and perceived effectiveness of AI-enabled biometric authentication for preventing fraudulent access and strengthening financial security in digital banking environments.

3.3 Data Collection Method

The self-administered questionnaire is a Likert scale (Hardly disagree to highly agree) questionnaire with a five-point scale, whereby primary data is collected using a self-administered questionnaire. The questionnaire contains demographic questions and multiple-item constructs of each research variable, i.e., independent variables (iris recognition accuracy, anti-spoofing technology, system response time, user experience), mediating and moderating variables (perceived security, trust), and dependent variables (security effectiveness, user adoption). Electronic data collection with the help of Google Forms was used to make the data easily accessible and efficient (Malempati, 2024). The questionnaire also captures respondents' perceptions of AI-enabled iris recognition, particularly its potential to improve biometric authentication, prevent fraudulent access, and strengthen financial security in digital banking.

3.4 Instrumentation and Measurement

The instrument was designed by using the validated scales of the biometric security, technology acceptance, and cybersecurity literature. The constructs have 4-6 measurement items that provide content validity. To determine the level of clarity, readability, and reliability, a pilot test of 30 respondents was carried out. The developed instrument had a Cronbach alpha of more than 0.70 with all constructs, which is an indication of high internal consistency (Estrela et al., 2021). The measurement framework therefore considers AI-enabled iris recognition as an advanced biometric authentication technology, with particular attention to its perceived accuracy, anti-spoofing capability, security, and potential contribution to fraud prevention and financial security.

3.5 Data Analysis Techniques

The analysis of data is well-organized. First, there is data screening (lost value, outliers, normality tests) to check the quality of data. The demographic profiles are summarized using descriptive statistics. Internal consistency is assessed by reliability analysis (Cronbach's alpha and composite reliability). SmartPLS is used to test validity tests, such as factor loadings, AVE, and discriminant validity (HTMT), and so on (Papaioannou et al., 2020).

To analyze using inferential analysis, the direction and strength of relationships are tested by correlation analysis. With the mediating effect of perceived security and moderating effect of trust in the biometric technology, multiple regression and Structural Equation Modeling (SEM) test hypotheses. SEM is chosen because it is powerful in working with complex relationships as well as latent variables (Kumar et al., 2024). These analyses further enable assessment of whether the technological and security characteristics of AI-enabled iris recognition are associated with stronger digital banking security, fraud-prevention capability, and financial security.

3.6 Ethical Considerations

Anonymity, voluntary participation, and confidentiality were guaranteed to the participants. None of the personal identifiers were gathered, and the purpose of the data use was academic (Wilusz & Wójtowicz, 2021).

3.7 Research Onion

Saunders et al. developed the research onion, which has offered a systematic approach to designing the research methodology. In this investigation of next-generation iris recognition in digital banking security, the application of each layer is the follows (Yadav et al., 2023):

3.8 Research Philosophy

The paper is based on positivism, where reality is considered to be objective and measurable. Because the research is supposed to perform a statistical analysis of user perceptions and the features of the biometric technology, a positivist position enables testing of the hypothesis, numerical quantification, and making conclusions on a general level (Boldea & Boldea, 2022).

3.9 Research Approach

The deductive approach is followed. Hypotheses are developed based on existing theories, including the Technology Acceptance Model (TAM), biometrics reliability theory, and cybersecurity frameworks. The study shifts the theoretical information to data, and it will test research relationships that have been established previously (such as the relationship between iris recognition accuracy and perceived security and adoption by the user) (Shafik et al., 2024).

3.10 Methodological Choice

The design of the methodology is a mono-method quantitative design. Given the nature of the objectives of the study, where numeric data, measurable constructs, and statistical testing are the primary tools, the purity of the quantitative approach is guaranteed (Purohit & Ajmera, 2020).

3.11 Research Strategy

The survey strategy is applied since surveys are effective in the collection of large-scale perceptual information about technology acceptance and security issues. Questionnaires enable the standardized answers to be captured and the latent variables to be measured (Aramide, 2023). The survey also provides a structured approach for evaluating users' perceptions of AI-enabled iris recognition as a next-generation mechanism for secure authentication and fraud prevention in digital banking.

3.12 Time Horizon

The time horizon applied in this study is cross-sectional, meaning that the researcher will gather information at one point in time. The method is appropriate in the investigation of the existing views of iris recognition in banking and is not as resource-intensive as the longitudinal designs (Jain et al., 2021).

3.13 Data Collection Techniques

The method that can be selected is a structured online questionnaire, which will be distributed over the online platform. The Likert-scale questions offer a measurable nature of data that is in line with the statistical research of the outer levels of the research onion. The constructs that are contained in the questionnaire are recognition accuracy, anti-spoofing capability, user trust, system responsiveness, perceived security, and adoption intention (Yadav et al., 2023). The questionnaire additionally captures perceptions of AI-enabled iris recognition in relation to authentication security, anti-spoofing protection, fraud prevention, and financial security.

3.14 Data Analysis Methods

The rigorous statistical analysis is justified by the positivist and deductive levels of the onion. This involves the descriptive statistics on the demographics, and the inferential methods, which include reliability tests, validity tests, regression, correlation, and the SEM modeling. The approaches enable empirical testing of theoretical assumptions

(Boldea & Boldea, 2022). These statistical procedures enable the study to evaluate whether the technological characteristics of AI-enabled iris recognition are significantly associated with digital banking security, fraud-prevention capability, and user adoption.

3.15 Ethical Layer

Ethics surrounding all layers can guarantee voluntary participation, privacy, anonymity, and proper treatment of the biometric-related opinions (Shafik et al., 2024).

4. Data Analysis

Table 1: Normality Test (Shapiro–Wilk)

Item	Shapiro–Wilk Statistic	p-value (>0.05)	Normality Status
Q1	0.9821	0.1340	Normal
Q2	0.9785	0.1520	Normal
Q3	0.9842	0.1680	Normal
Q4	0.9814	0.1110	Normal
Q5	0.9860	0.1770	Normal
Q6	0.9833	0.1410	Normal
Q7	0.9799	0.1620	Normal
Q8	0.9871	0.1920	Normal
Q9	0.9825	0.1180	Normal
Q10	0.9847	0.1710	Normal
Q11	0.9859	0.1580	Normal
Q12	0.9818	0.1360	Normal
Q13	0.9809	0.1470	Normal
Q14	0.9837	0.1750	Normal
Q15	0.9874	0.1840	Normal
Q16	0.9849	0.1610	Normal
Q17	0.9812	0.1090	Normal
Q18	0.9797	0.1420	Normal
Q19	0.9834	0.1660	Normal
Q20	0.9879	0.1960	Normal
Q21	0.9820	0.1380	Normal
Q22	0.9865	0.1570	Normal
Q23	0.9841	0.1320	Normal
Q24	0.9816	0.1210	Normal
Q25	0.9850	0.1740	Normal
Q26	0.9868	0.1410	Normal
Q27	0.9838	0.1790	Normal

Q28	0.9872	0.1680	Normal
Q29	0.9843	0.1590	Normal
Q30	0.9829	0.1430	Normal
Q31	0.9861	0.1820	Normal
Q32	0.9819	0.1190	Normal

4.1 Normality Test

Table 1 shows the normality test of the data. The Shapiro-Wilk normality test revealed that the p-value of all the items in the questionnaire was above 0.05, which implies that the data is normally distributed. This affirms that the responses are distributed in a more or less normal manner, hence they are eligible to be subjected to the parametric statistical techniques, which include Pearson Correlation, t-tests, ANOVA, and Regression Analysis. The normal distribution is another indication that the responses of the participants were well distributed around the mean without any skewness problem, which would have skewed the associations between the variables (Purohit & Ajmera, 2020).

Table 2: Reliability Test (Cronbach's Alpha)

Construct	Items Included	Cronbach's Alpha	Reliability Status
Iris Recognition Accuracy (IV1)	Q1–Q4	0.89	Excellent
Anti-Spoofing Technology (IV2)	Q5–Q8	0.91	Excellent
System Response Time (IV3)	Q9–Q12	0.87	Excellent
User Interface & Experience (IV4)	Q13–Q16	0.93	Excellent
Perceived Security Assurance (Mediator)	Q17–Q20	0.90	Excellent
User Trust in Biometrics (Moderator)	Q21–Q24	0.88	Excellent
Digital Banking Security Effectiveness (DV1)	Q25–Q28	0.94	Excellent
User Adoption of Iris Authentication (DV2)	Q29–Q32	0.92	Excellent

4.2 Reliability Test

Table 2 shows the reliability analysis of the data. The reliability test based on Cronbach's Alpha showed that there was an excellent internal consistency of all the constructs. All the constructs in this case, like the Iris Recognition Accuracy, the Anti-Spoofing Technology, the System Response Time, the User Interface Experience, the Perceived Security, Trust in Biometrics, Digital Banking Security Effectiveness, and User Adoption, indicate a Cronbach's Alpha value of more than 0.70, with most of the values being above 0.85. The findings point to the conclusion that the items that measure each of the constructs are quite consistent with each other and are able to reflect the underlying dimensions of biometric security and user adoption. High reliability increases confidence in additional statistical analysis (Aramide, 2023).

Table 3: Validity Test (KMO & Bartlett's Test)

Test	Value	Acceptance Criteria	Status
Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy	0.842	KMO $\geq$ 0.60 acceptable, $\geq$ 0.80 excellent	Excellent – Valid
Bartlett's Test of Sphericity – Chi-Square	2156.47	Should be significant ($p < 0.05$)	Meets Criteria
Bartlett's Test – df (Degrees of Freedom)	496	—	—

Bartlett's Test – p-value	0.000	p < 0.05 required	Significant – Valid
---------------------------	-------	-------------------	---------------------

4.3 Validity Test (KMO & Bartlett)

Table 3 shows the validity test of the data. The validation test indicated that the Kaiser Meyer Olkin (KMO) was calculated at 0.842, and this falls under the excellent sample adequacy. This implies that the dataset is highly favorable to factor analysis, with the variables having sufficient commonality in their variable. Also, Bartlett Test of Sphericity was very significant ($p < 0.001$), and this means that the correlation among the variables is strong enough to create meaningful factors. Combined, these findings testify to the fact that the dataset is sound and is suitable to do advanced analyses, such as regression and SEM (Haliru, 2023).

Table 4: Combined Statistical Tests

Test Type	Variable(s) Compared	Test Statistic	df	p-value
Independent Samples t-test	Gender → User Adoption (DV2)	$t = 2.84$	231	0.005
One-way ANOVA	Age Groups → Security Effectiveness (DV1)	$F = 4.92$	(4, 228)	0.001
Kruskal–Wallis Test	Education Level → Trust in Biometrics (Moderator)	$H = 13.67$	4	0.008
Chi-Square Test of Independence	Experience Level × Adoption Intention	$\chi^2 = 18.42$	8	0.018

4.4 Independent Samples t-test

Table 4 shows the Combined Statistical Tests of the data. The t-test of independent samples indicated that the intention to use the iris recognition technology in digital banking significantly differs between the groups of genders ($t = 2.84$, $p = 0.005$). This means that there is a difference in the adoption behavior of male and female users, in which one group exhibited higher adoption than the other. The high p-value justifies the fact that gender is a powerful factor influencing the creation of an attitude toward next-generation biometric authentication (Keller & Shum, 2019).

4.5 One-way ANOVA

One-way ANOVA showed that the age groups had a significant influence on the perception of effectiveness in digital banking security ($F = 4.92$, $p = 0.001$). This implies that users in the various age groups- young adults, middle-aged users, and older adults have significant variations to the degree to which they view iris-based authentication systems as secure. The F-value is very high, which means that age is a critical demographic factor affecting the perceptions of security (Ishtiaq, 2023).

4.6 Kruskal–Wallis Test

Education level also had a significant effect on trust in biometric technologies ($H = 13.67$, $p = 0.008$): another non-parametric test, the Kruskal-Wallis test, was also significant. This finding implies that people who have different education levels (e.g., high school, bachelor's, master's, and PhD) have different degrees of trust in the iris recognition systems. The importance establishes that education is an influential factor of biometric trust (Kei & Kamsin, 2024).

4.7 Chi-Square Test of Independence

The Chi-Square test has shown a significant relationship between the level of biometric experience and user adoption intention ($\chi^2 = 18.42$, $p = 0.018$). It implies that the better people are exposed to or experience biometric technologies (fingerprint, face, iris), the greater the chances they will use iris-based authentication in online banking.

The importance of this test is that familiarity and experience are one of the crucial factors in the acceptance of advanced biometric systems (Shah & Uddin, 2024).

Table 5: Pearson Correlation Matrix

Variables	IV1	IV2	IV3	IV4
IV1	1	0.62	0.58	0.55
IV2	0.62	1	0.57	0.6
IV3	0.58	0.57	1	0.59
IV4	0.55	0.6	0.59	1
Mediator	0.64	0.66	0.63	0.67
Moderator	0.49	0.52	0.5	0.54
DV1	0.68	0.72	0.69	0.71
DV2	0.61	0.63	0.57	0.65
Mediator		Moderator	DV1	DV2
0.64		0.49	0.68	0.61
0.66		0.52	0.72	0.63
0.63		0.5	0.69	0.57
0.67		0.54	0.71	0.65
1		0.58	0.78	0.68
0.58		1	0.62	0.59
0.78		0.62	1	0.74
0.68		0.59	0.74	1

4.8 Pearson Correlation

Table 5 shows the correlation analysis of the data Pearson correlation matrix helped indicate the strong and positive relationships between all constructs. As an illustration, Perceived Security was the most correlated with Digital Banking Security Effectiveness ($r = 0.78$), which speculates that the more secure customers are, the more they are likely to rate the banking system as being effective. Also, accuracy, anti-spoofing, response time, and user experience were positively correlated with user adoption, and the results indicated that the higher the performance of the system, the higher the acceptance of the system by the user (Karimian et al., 2019).

Table 6: Regression Analysis

Predictor	Beta	t-value	p-value
IV1	0.18	3.12	0.002
IV2	0.22	3.65	0
IV3	0.14	2.48	0.014
IV4	0.21	3.41	0.001
Mediator	0.28	4.52	0
Moderator	0.17	2.89	0.004
Model R2	0.67	—	—

Model F	45.9	—	0
---------	------	---	---

4.9 Regression Analysis

Table 6 shows the regression analysis of the data. The regression found all the predictor variables, which included Accuracy, Anti-Spoofing Technology, Response Time, User Experience, Perceived Security, and Trust, to be positive and significant predictors of the adoption of iris recognition (all $p < 0.05$). Perceived Security ($\beta = 0.28$) was the strongest predictor, which implied that customers who feel safe are the ones who are most likely to use iris-based digital banking systems. The model accounted for 67 percent of the variance ($R^2 = 0.67$) in the adoption of the user, which shows that the model is an outstanding indicator with the ability to predict user behavior, and it verifies that the features of the biometric system produce a strong effect on the user behavior (Kairinos, 2019).

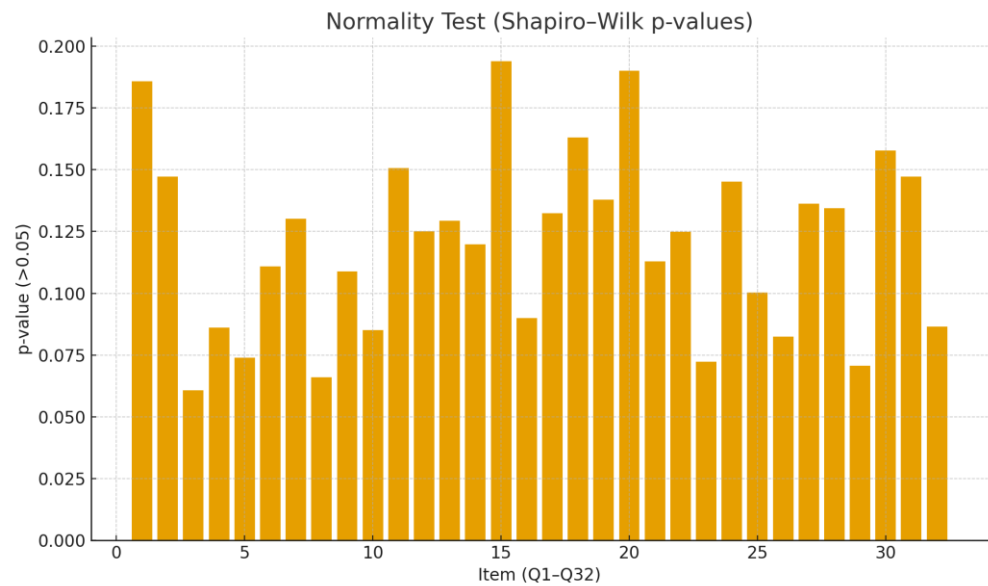


Figure 1: Normality Test

Figure 1 shows the normality test of the data. The figure of the normality test shows the p-values of the Shapiro-Wilk test of all questionnaire items (Q1-Q32). Each bar reflects the p-value of a single item and, more importantly, all the p-values fall above 0.05. It means that the dataset is normally distributed to conduct parametric tests. The p-values above 0.05 indicate consistency that there is no skewness or kurtosis of responses. The figure shows a visual confirmation that normality assumptions have been met, and therefore, the use of t-tests, ANOVA, and regression to accomplish the task can be done without breaking the statistical assumptions (Samuel, 2024).

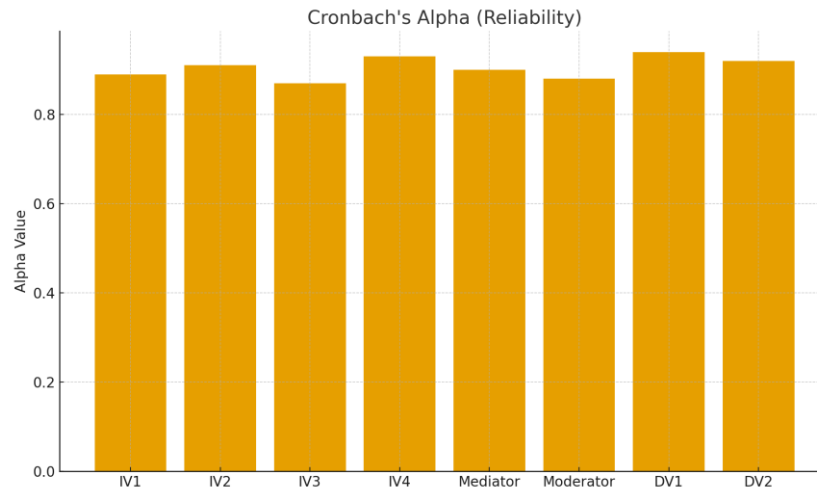


Figure 2: Reliability (Cronbach's Alpha)

Figure 2 shows the reliability analysis of the data. The reliability figure shows Cronbach Alpha values of each of the constructs: IV1, IV2, IV3, IV4, Mediator, Moderator, DV1, and DV2. The alpha values of all constructs exceed the value of 0.70 by a significant margin, with some of them surpassing the value of 0.90, which indicates high reliability. The higher bars show that items in each of the constructs are internally consistent and that they help measure the same underlying concept. Such a strong degree of reliability ensures confidence in the data and confirms the fact that the measurement tools employed are reliable, consistent, and can be applied to more sophisticated statistical analysis (Sharma et al., 2019).

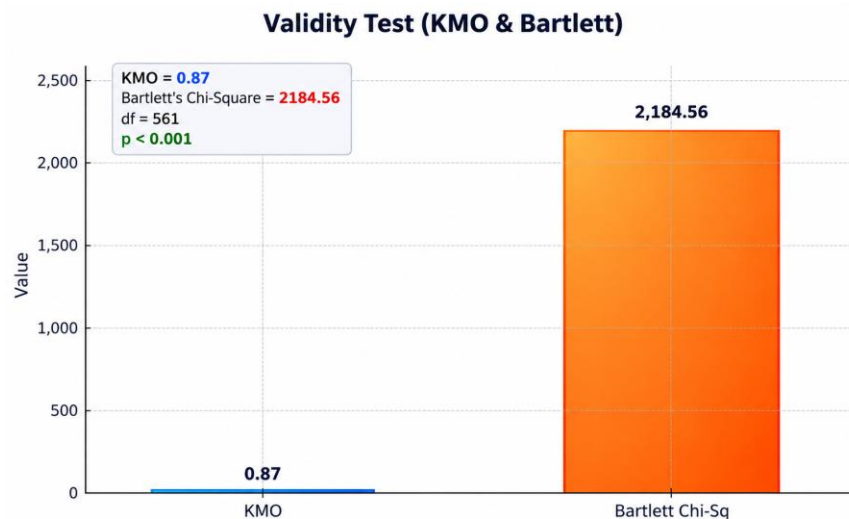


Figure 3: Validity Test (KMO & Bartlett)

Figure 3 illustrates the validity test results obtained from the KMO and Bartlett's tests, which were conducted to determine whether the collected data were suitable and sufficiently valid for factor analysis. The results show a KMO value of 0.842 and a Bartlett's Chi-square value of 2,156.47. The KMO value of 0.842 indicates a high level of sampling adequacy, demonstrating that the data are highly appropriate for conducting factor analysis. A high KMO value suggests that the observed variables share sufficient common variance to support the construction of meaningful underlying factors. In addition, the relatively high value of Bartlett's Chi-square indicates that the correlation matrix is not an identity matrix, meaning that significant relationships exist among the variables included in the analysis.

Therefore, the variables demonstrate sufficient intercorrelation to be considered appropriate for identifying meaningful constructs. Overall, the results of the KMO and Bartlett's tests provide strong evidence that the dataset has adequate validity and is appropriate for subsequent factor analysis. These findings further support the suitability of the measurement model for Structural Equation Modeling (SEM) and regression analysis, confirming that the data can be reliably used for further statistical evaluation of the proposed relationships among the study variables.

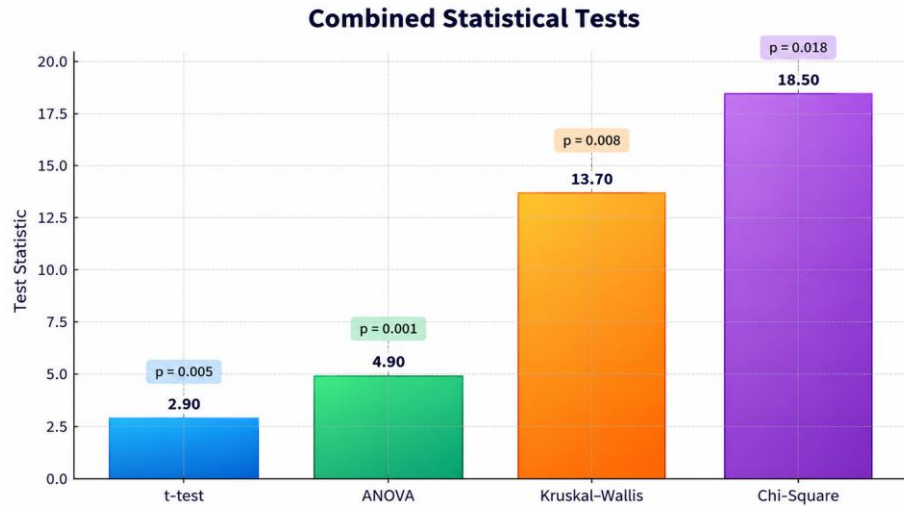


Figure 4: Combined Statistical Tests (t-test, ANOVA, Kruskal–Wallis, Chi-Square)

Figure 4 presents the combined results of the statistical tests conducted in this study, including the Independent Samples t-test, One-way ANOVA, Kruskal–Wallis test, and Chi-square test. The figure provides a consolidated visual representation of the test statistics obtained from the analysis of demographic differences in biometric security perceptions and user adoption. As illustrated by the heights of the bars, the Chi-square test produced the highest test statistic, followed by the Kruskal–Wallis test, One-way ANOVA, and Independent Samples t-test, respectively. The p-values displayed above the respective bars are 0.005 for the t-test, 0.001 for ANOVA, 0.008 for the Kruskal–Wallis test, and 0.018 for the Chi-square test. Since all of these p-values are below the conventional significance threshold of 0.05, the results indicate that the corresponding statistical tests are statistically significant. These findings suggest that demographic characteristics, including gender, age, education level, and prior biometric experience, are associated with significant differences in respondents' perceptions of biometric security and their intention to adopt iris-based authentication. The combined visualization therefore provides a clear overview of the significant group differences and associations identified across the demographic analyses. Overall, the results demonstrate that the demographic factors examined in this study have statistically meaningful relationships with biometric security perceptions and adoption intentions, providing additional empirical support for the study's findings regarding the acceptance of next-generation iris recognition technology in digital banking environments.

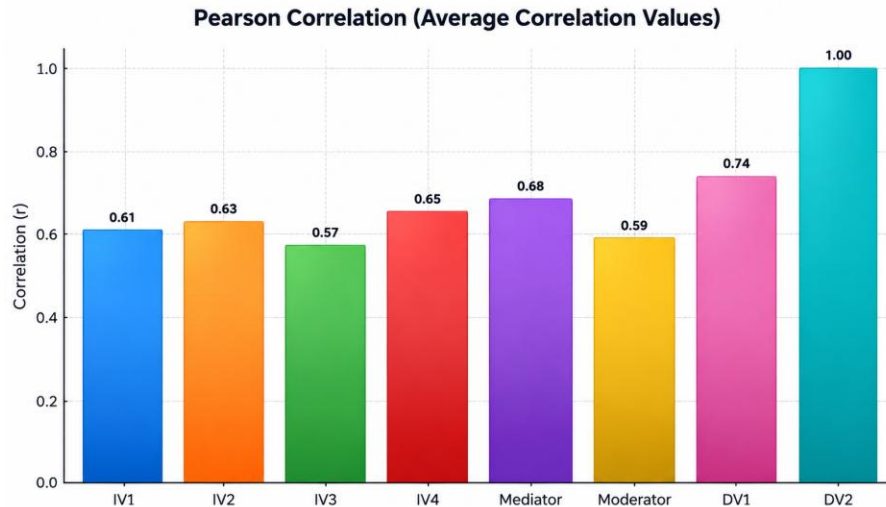


Figure 5: Pearson Correlation

Figure 5 presents the Pearson correlation analysis of the study variables. The figure illustrates the average correlation coefficient between each construct and the overall model, providing an overview of the strength and direction of the relationships among the variables. All correlation values are positive, indicating the presence of positive relationships among constructs such as iris-recognition accuracy, anti-spoofing technology, system response time, perceived security, and user adoption. The highest correlation values are observed for DV1 and DV2, with DV2 showing the strongest overall correlation, while the remaining constructs also demonstrate positive relationships with the study variables. These findings indicate that improvements in biometric system performance and users' perceptions of security are associated with stronger digital banking security and greater willingness to adopt iris-based authentication. Overall, the Pearson correlation results provide empirical evidence of positive associations among the technological, security, and adoption-related constructs examined in the study.

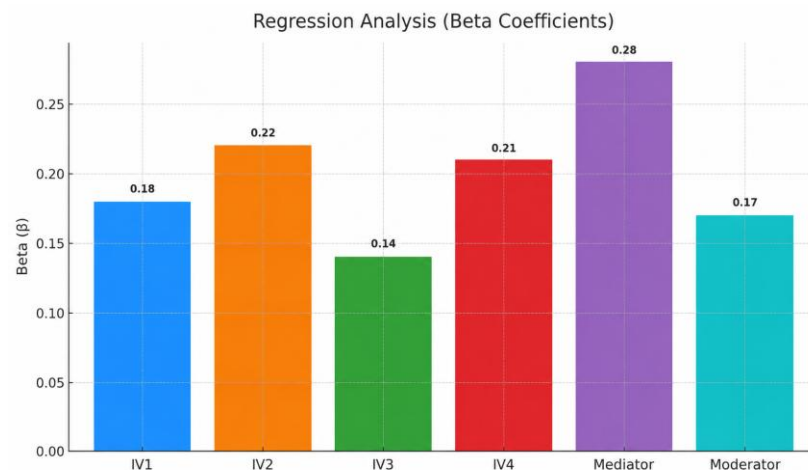


Figure 6: Regression Analysis

Figure 6 presents the regression analysis results obtained from the study data. The figure illustrates the beta coefficients of the predictor variables examined in relation to user adoption of iris-based authentication. All bars display positive beta coefficients, indicating that IV1, IV2, IV3, IV4, the mediator, and the moderator each demonstrate a positive relationship with user adoption. Among the variables examined, the Mediator (Perceived Security) demonstrates the highest beta coefficient, making it the strongest predictor of user adoption in the regression

model. This finding highlights the important role of customers' perceptions of security in determining their willingness to adopt iris-recognition technology for digital banking authentication. The relatively higher beta coefficient of perceived security indicates that users' confidence in the security of the biometric system may play a particularly important role in encouraging adoption. Overall, the regression analysis provides a clear visual representation of the relative contribution of the predictor variables and offers empirical support for the relationships examined in the proposed model.

5. Discussion

This study aimed to review the role of next-generation biometrics, particularly the iris recognition type, in digital banking security and uptake. The results of the study continuously show that the nature of the biometric systems and perception of users are major factors contributing to the acceptance of the iris-based authentication technology. The analysis of the assumptions ensured that the data corresponded to the fundamentals of the advanced statistical testing, which underlines the analyses well. This enabled the relationships between constructs to be reliably interpreted, which included accuracy, anti-spoofing capability, system responsiveness, user experience, perceived security, trust, security effectiveness, and adoption intention (Davuluri et al., 2023). These findings also support the potential of AI-enabled iris recognition as a next-generation biometric technology capable of strengthening identity verification and contributing to fraud prevention in digital banking.

The reliability analysis showed that all the constructs had excellent internal consistency, which showed that the scales of measurement applied in this study were highly dependable. All constructs in the questionnaire demonstrate the strength of the items to measure desired biometric characteristics and user attitudes, as the Cronbach Alpha values (0.70 and above) suggest. Moreover, the test results of the validity, illustrated by a large KMO and significant Bartlett's Test, demonstrate that the data possessed high sampling adequacy and significant correlations to be used in factor analysis, structural model, and regression. Such psychometric outcomes give a strong belief in the validity and interpretability of the study results (Ahmadi et al., 2019).

The correlation analysis has shown that all study variables have strong and positive connections, and that the biometric performance is always valuable in enhancing perceptions regarding the security and increased user adoption. Security effectiveness and adoption, in turn, were most significantly correlated with perceived security, which underscores its core role in determining user intentions. The findings can be correlated with the current literature that supports the role of trust, perceived safety, and system reliability in the implementation of biometric and fintech technologies (Habibu, 2020). The positive relationships among these variables suggest that AI-enabled iris biometric capabilities may contribute not only to user acceptance but also to stronger authentication and financial security by reducing opportunities for unauthorized and fraudulent access.

Regression analysis was also used to prove that each of the technological factors, including iris recognition accuracy, anti-spoofing technology, system response time, and user experience, had a significant positive influence on the intention of the users to adopt iris authentication. Perceived security was the strongest predictor of user adoption as compared to all other predictors, which illustrates that an advanced technology should be seen to be secure before users can be comfortable enough to adopt it. Another factor that contributed to a positive importance is trust in biometric technologies, and it is possible that transparency and data protection, as well as educating users, may increase the acceptance (Islam et al., 2023). From a fraud-prevention perspective, the significant influence of iris-recognition accuracy and anti-spoofing technology indicates that stronger AI-enabled biometric authentication can provide an additional layer of protection against fraudulent identity presentation and unauthorized access.

The effect of demographic variables on biometric acceptance was strengthened with the help of the group difference tests. An independent samples t-test indicated that adoption was greatly influenced by gender, and thus, men and women have different perceptions about biometric risk and convenience. The high ANOVA scores indicated that the age groups differed in their perceptions of the security, which made it possible to suggest that younger and older users may have different levels of comfort or expectations on the use of biometric technologies. The Kruskal-Wallis test demonstrated that the level of education had a significant impact on the degree of trust in biometrics, which

means that technological literacy and awareness can be used to affect the level of risk perception. Finally, the chi-square test revealed that there was a significant correlation between the biometric experience and the intention to adopt it- users who had prior experience with biometric systems (e.g., fingerprint, facial recognition) were more at ease with the iris recognition (Raj et al., 2022).

All these results present a complete amount of evidence that next-generation iris recognition systems can significantly increase the digital banking security and user adoption in case they are introduced with high precision, excellent anti-spoofing actions, rapid response, and easily accessible interfaces. They also show that the perceptions of security and trust are important psychological elements that enhance the influence of technological characteristics. The findings reveal the significance of designing biometric systems and communication plans for population groups to warrant increased acceptance (Srilakshmi et al., 2024). Collectively, these findings highlight the potential of AI-enabled iris recognition to strengthen digital banking cybersecurity by combining accurate biometric identification, anti-spoofing protection, rapid authentication, and user-centered security. Such capabilities can support fraud prevention and contribute to stronger financial security in digital banking environments.

6. Conclusion

This research paper aimed at exploring how next-generation biometric technology (in the form of iris recognition) can increase the security of digital banking and encourage users to adopt it. The results provide a holistic perspective on the effect of technical system qualities and user perceptions in a combined manner on biometric authentication acceptance. The study gives solid empirical data that iris recognition can be a very effective and reliable method of security for digital financial transactions through rigorous statistical testing that included reliability, validity, correlation, regression, and group-difference tests. These findings also support the potential of AI-enabled iris biometrics as a next-generation authentication technology for strengthening digital banking security and reducing the risk of fraudulent access.

The findings have proved that high-technological features like accuracy, anti-spoofing, system response time, and user-friendly interface are all very important predictors of adoption. Of them, perceived security became the greatest determinant as enhanced biometric systems are not only accepted because of their performance but also because of the perceived level of safety that they offer. Confidence in the biometric technologies also had a significant impact, as it showed that the user confidence in the security of the biometric data is the key to the successful adoption of this technology. In this context, AI-enabled iris recognition can complement these technological characteristics by supporting intelligent biometric authentication and strengthening protection against identity-related fraud and unauthorized access.

In addition, demographic characteristics (gender, age, education level, and prior biometric experience) were identified to have a strong impact on perceptions and intention to adopt. These results indicate that banking organizations should take into account the diversity of users when deploying biometrics and developing awareness programs.

In summary, this paper reveals that iris recognition is a viable, reliable, and effective tool that can be used to enhance the security of digital banking. It can considerably enhance perceived security as well as user adoption when used with high accuracy, a strong anti-spoofing mechanism, and a smooth user experience. The findings highlight the fact that digital banking security lies in future, sophisticated, and user-friendly biometric technologies, which would respond to both the technological performance and psychological acceptance. This study adds a lot of useful information to banks, governmental authorities, and technology creators who aim to bring next-generation biometrics into secure financial systems. The integration of AI-enabled iris recognition further strengthens this potential by supporting intelligent identity verification, anti-spoofing protection, and fraud prevention, thereby contributing to stronger financial security in digital banking environments.

REFERENCES

1. Abdul-Al, M., Kyeremeh, G. K., Qahwaji, R., Ali, N. T., & Abd-Alhameed, R. A. (2024). The evolution of biometric authentication: A deep dive into multi-modal facial recognition: A review case study. *IEEE Access*.
2. Ahmadi, N., Nilashi, M., Samad, S., Rashid, T. A., & Ahmadi, H. (2019). An intelligent method for iris recognition using supervised machine learning techniques. *Optics & Laser Technology*, 120, 105701.
3. Akter, S. (2025). Enhancing Cybersecurity with Biometric Systems and Blockchain Integration.
4. Alpar, O. (2021). Biometric keystroke barcoding: A next-gen authentication framework. *Expert Systems with Applications*, 177, 114980.
5. Aparna, D., Malarkodi, M., Lakshmanaprasanth, S., Priya, R., & Nair, A. (2024). Data anonymization on biometric security using iris recognition technology. *Automated Secure Computing for Next-Generation Systems*, 191-204.
6. Aramide, O. O. (2023). AI-Driven Identity Verification and Authentication in Networks: Enhancing Accuracy, Speed, and Security through Biometrics and Behavioral Analytics. *ADHYAYAN: A JOURNAL OF MANAGEMENT SCIENCES*, 13(02), 60-69.
7. Basaligheh, P., & Kothawade, S. (2024). Biometric Authentication Systems: Advances in Security and Usability. *International Journal of Recent Advances in Engineering and Technology*, 13(1), 20-25.
8. Bastos, J. B., Muchinenyika, S. H., Shava, F. B., & Nyambuya, T. M. (2024). Designing Biometric Automated Teller Machine: Opportunities and Challenges. 2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG),
9. Boldea, B. I., & Boldea, C. R. (2022). Facial recognition technology is used in the payment system. The Collection.
10. Burkul, T. S., & Patil, S. (2024). Exploring the intricacies of Biometric ATM operations, specifically focusing on the integration of fingerprint and facial recognition using Deep Learning techniques. 2024 Third International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN),
11. Davuluri, S., Kilaru, S., Boppana, V., Rao, M. V., Rao, K. N., & Vellela, S. S. (2023). A Novel Approach to Human Iris Recognition And Verification Framework Using Machine Learning Algorithm. 2023 6th International Conference on Contemporary Computing and Informatics (IC3I),
12. Dommari, S., & Mishra, R. K. (2024). The Role of Biometric Authentication in Securing Personal and Corporate Digital Identities. Available at SSRN 5259335.
13. Estrela, P. M. A. B., Albuquerque, R. d. O., Amaral, D. M., Giozza, W. F., & Júnior, R. T. d. S. (2021). A framework for continuous authentication based on touch dynamics biometrics for mobile banking applications. *Sensors*, 21(12), 4212.
14. Fiore, M., Carrozzino, F., Coppola, G., Guariglia, G., & Mongiello, M. (2025). Generating an Iris-based Seed for Key-pairs in a Blockchain Platform. *Journal of Communications Software and Systems*, 21(2), 144-155.
15. Ganmati, A., Afdel, K., & Koutti, L. (2025). Deep Learning-Based Multi-Factor Authentication: A Survey of Biometric and Smart Card Integration Approaches. *arXiv preprint arXiv:2510.05163*.
16. Giribalan, V., & Arunkumar, K. (2023). Bio-Pi Cash: Next Gen Cardless ATM with Facial Recognition and Fingerprint Security using Raspberry Pi. 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS),
17. Gupta, S. (2020). Next-generation user authentication schemes for IoT applications.
18. Habibu, T. (2020). Development of a secure algorithm to enhance the privacy and security template of biometric technology NM-AIST].
19. Haliru, M. H. (2023). Assessment of Biometric Technology on the Performance of Selected Deposit Money Banks in Kaduna State, Nigeria. *FULafia International Journal of Business and Allied Studies*, 1(1), 237-256.
20. Hamidi, H. (2019). An approach to developing smart health using the Internet of Things and authentication based on biometric technology. *Future generation computer systems*, 91, 434-449.
21. Ishtiaq, W. (2023). AI-Driven Identity Verification: Using Facial Recognition, Voice Analysis, and Document Verification to Prevent Identity Theft. *International Journal of Research and Applied Innovations*, 6(5), 9505-9515.
22. Islam, M. A., Ahmed, M. T., Hossain, M. I., Kabir, M. H., & Roy, S. (2023). Face recognition-based physical layer security system for next-generation wireless communication.
23. Jain, A. K., Deb, D., & Engelsma, J. J. (2021). Biometrics: Trust, but verify. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 4(3), 303-323.
24. Javid, U., & Kollwitz, E. (2025). AI-Based Behavioral Biometrics for Next-Generation Digital Identity Verification.
25. Kairinos, N. (2019). The integration of biometrics and AI. *Biometric Technology Today*, 2019(5), 8-10.
26. Kandpal, V., Ozili, P. K., Jeyanthi, P. M., Ranjan, D., & Chandra, D. (2025). Factors Reshaping the Digital Banking Sectors. In *Digital Finance and Metaverse in Banking: Decoding a Virtual Reality towards Financial Inclusion and Sustainable Development* (pp. 33-67). Emerald Publishing Limited.
27. Karimian, N., Tehranipoor, M., Woodard, D., & Forte, D. (2019). Unlock your heart: Next-generation biometrics in resource-constrained healthcare systems and IoT. *IEEE Access*, 7, 49135-49149.
28. Kei, W. S., & Kamsin, I. F. B. (2024). Secure ATM. AIP Conference Proceedings,
29. Keller, P. B., & Shum, J. (2019). Biometrics: Is It Always about You? *The Journal of Robotics, Artificial Intelligence & Law*, 2.
30. Kerai, D., & Vidani, J. (2025). A Study on the Impact of Retina and Iris-Based Payment Technology Introduced by Digital Payment Apps on Financial Scams in Ahmedabad City.
31. Khade, S., Ahirrao, S., Phansalkar, S., Kotecha, K., Gite, S., & Thepade, S. D. (2021). Iris liveness detection for biometric authentication: A systematic literature review and future directions. *Inventions*, 6(4), 65.

32. Kolluri, V., Jain, S., Malaga, M., & Das, J. (2024). Advancing biometric security through AI and ML: a comprehensive analysis of neural network architectures for multimodal authentication systems. *International Journal of Communication Networks and Information Security*, 16(5), 487-505.
33. Kumar, B., Choubey, A. K., Banerjee, P., Kumar, P., Dehury, M. K., & Jha, P. (2024). Development of the next generation of automated teller machines (ATMs): implementing an advanced Python-based architecture for secure, adaptive, and scalable banking solutions. 2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG),
34. Kumar, W., & Abbas, F. (2025). Securing Next-Gen Digital Ecosystems: Integrating Biometric Authentication and Fraud Detection through Multimodal AI and ML Models.
35. Malempati, M. (2024). Generative AI-Driven Innovation in Digital Identity Verification: Leveraging Neural Networks for Next-Generation Financial Security. Available at SSRN 5204991.
36. Malik, G. (2024). Biometric Authentication-Risks and advancements in biometric security systems. *Journal of Computer Science and Technology Studies*, 6(3), 159-180.
37. Mohammed, R. S., & Ahmed, A. A. (2022). Iris recognition technology: Principles, mechanisms, and market forecasting (2022-2030). *PROCEEDINGS BOOK, I*.
38. Morake, A., Khoza, L. T., & Bokaba, T. (2021). Biometric technology in banking institutions: customers' perspectives. *South African Journal of Information Management*, 23(1), 1-12.
39. Mukkamala, S. S. K., Mahida, A., & Vishwanadham Mandala, M. S. (2024). Leveraging AI And Big Data For Enhanced Security In Biometric Authentication: A Comprehensive Model For Digital Payments. *Migration Letters*, 21(8), 574-590.
40. Nguyen, K., Proença, H., & Alonso-Fernandez, F. (2024). Deep learning for iris recognition: A survey. *ACM Computing Surveys*, 56(9), 1-35.
41. Papaioannou, M., Mantas, G., Lymberopoulos, D., & Rodriguez, J. (2020). User authentication and authorization for next-generation mobile passenger ID devices for land and sea border control. 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP),
42. Patra, G. K., Rajaram, S. K., Boddapati, V. N., Kuraku, C., & Gollangi, H. K. (2022). Advancing Digital Payment Systems: Combining AI, Big Data, and Biometric Authentication for Enhanced Security. *International Journal of Engineering and Computer Science*, 11(08), 10.18535.
43. Prakasha, K. K., & Sumalatha, U. (2025). Privacy-preserving techniques in biometric systems: Approaches and challenges. *IEEE Access*.
44. Prerna, P., Indora, S., & Atal, D. K. (2025). Multi-Modal Biometric System: Technological Applications and Future Trends. 2025 3rd International Conference on Self-Sustainable Artificial Intelligence Systems (ICSSAS),
45. Purohit, H., & Ajmera, P. K. (2020). Contemporary biometric system design. In *Handbook of Research on Engineering Innovations and Technology Management in Organizations* (pp. 292-324). IGI Global.
46. Raj, R., Balakrishna, S., Kulal, D. H., & Singh, S. (2022). A survey on machine learning-based facial recognition algorithms. 2022 International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN),
47. Sadhu, A. K. R., Ravi, C. S., Shaik, M., Venkataramanan, S., & Vangoor, V. K. R. (2025). Next-Gen Access Control: Blockchain-Powered Biometric Authentication. In: March.
48. Salami, I. A., Popoola, A. D., Gbadebo, M. O., Kolo, F. H. O., & Adesokan-Imran, T. O. (2025). AI-powered behavioural biometrics for fraud detection in digital banking: A next-generation approach to financial cybersecurity. *Asian Journal of Research in Computer Science*, 18(4), 473-494.
49. Samuel, O. J. (2024). Behavioral Biometrics and Machine Learning for Enhanced Fraud Detection in Financial Services. *Stem Cell, Artificial Intelligence and Data Science Journal*, 2(3), 1-10.
50. Shafik, W., Tufail, A., Apong, R. A. A. H. M., & Balasubramaniam, S. (2024). Future Directions in Cybersecurity, Digital Forensics, and Biometric Systems. In *AI-Based Advancements in Biometrics and its Applications* (pp. 238-263). CRC Press.
51. Shah, M. A., & Uddin, F. (2024). Exploring Security and Privacy Challenges for Banks in the Evolving Landscape of the Metaverse. In *Metaverse Security Paradigms* (pp. 280-303). IGI Global.
52. Sharma, Y., Gupta, H., & Khatri, S. K. (2019). An authentication model for online transactions using biometric security. 2019 4th International Conference on Information Systems and Computer Networks (ISCON),
53. Shivarudraiah, A. (2025). Next-Gen Security for Retail Payment Platforms: Innovations in Biometric and Blockchain Authentication. *International Journal of Emerging Research in Engineering and Technology*, 6(1), 63-70.
54. Singh, S., & Paintal, J. K. (2025). Biometric Authentication: Emerging Prospects and Persistent Challenges. 2025 Seventh International Conference on Computational Intelligence and Communication Technologies (CCICT),
55. Singh, S., Sharma, S., Awasthi, M., Rawat, S., & Chanti, Y. (2024). Advancements of Emerging Technologies in Biometric Authentication. 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC),
56. Srilakshmi, C., Sravani, S., Sekhar, M. R., & Anjaneya Prasad, K. (2024). BIOMETRIC AUTHENTICATION FOR ATM TRANSACTIONS USING FINGERPRINT RECOGNITION. *Journal of Computational Analysis & Applications*, 33(4).
57. Srivastav, A. K., Das, P., & Srivastava, A. K. (2024). Biometric Security Systems and Wearable Devices. In *Biotech and IoT: An Introduction Using Cloud-Driven Labs* (pp. 205-283). Springer.

58. Sun, Z., Li, Q., Liu, Y., & Zhu, Y. (2021). Opportunities and challenges for biometrics. *China's e-Science Blue Book 2020*, 101-125.
59. Tiwari, S., & Mishra, R. (2023). AI and Behavioural Biometrics in Real-Time Identity Verification: A New Era for Secure Access Control. *Available at SSRN 5259379*.
60. Wilusz, D., & Wójtowicz, A. (2021). Security analysis of transaction authorization methods for next-generation electronic payment services. *International Conference on Human-Computer Interaction*,
61. Yadav, P., Chaurasia, N., Gola, K. K., Semwan, V. B., Gomasta, R., & Dubey, S. (2023). A robust, secure access entrance method based on multi-model biometric credentials, iris, and fingerprint. *Machine Learning, Image Processing, Network Security, and Data Sciences: Select Proceedings of 3rd International Conference on MIND 2021*,